The fight against crime and/or the protection of privacy

Poullet, Yves

Published in:
International Review of Law Computers & Technology

Publication date:
2004

Document Version
Publisher's PDF, also known as Version of record

International Review of Law Computers & Technology, Volume 18, No. 2, Pages 251–273, July 2004

Carfax Publishing
Taylor & Francis Group

The Fight against Crime and/or the Protection of Privacy: A Thorny Debate![1]

YVES POULLET

ABSTRACT *This article analyses a recent legislative provision adopted by the Belgian legislator imposing on all communication service providers the requirement that they retain traffic data for a minimum period of 12 months, in addition to the recent European debates about Echelon and traffic data retention in the light of the requirements of Article 8 of the Council of Europe Convention on Human Rights and Fundamental Freedoms. The equilibrium between state security requirements and privacy protection imperatives leads the proposal of a certain number of limitations, as regards to cyber-surveillance by governmental authorities in order to maintain the efficient functioning of our democracies.*

> Those prepared to sacrifice a little liberty for the sake of security, deserve neither the one nor the other.
>
> BENJAMIN FRANKLIN

The history of Article 109b, E, of the law of 11 March 1991, intended to reform certain public entities, testifies to the fear of Belgian society with regard to attacks on personal or material security, attacks made that much easier by the spread of new communication and information technologies. This law, which was inserted into the recent law on cybercrime in response to the current desire for a more secure world, imposes the collaboration of information society providers with the police. In the context of the aftermath of the attack on the twin towers of the World Trade Centre, this particular Belgian legislation is being cited within the European debate as a model.

Our intention is to offer a brief commentary of the provision, while simultaneously taking a position in the 'data protection versus privacy' debate. To this end, our reflections will

Correspondence: Yves Poullet, Centre de Recherches Informatique et Droit, 5 Rempart de la Vierge, 5000 Namur, Belgium. E-mail: yves.poullet@fundp.ac.be.

The author is Dean of the Faculty of Law of the FUNDP, Namur, Belgium and Director of the Centre for Research into Computing and Law (CRID), Namur (http://www.crid.ac.be).

ISSN 1360-0869 print/ISSN 1364-6885 online/04/020251-23 © 2004 Taylor & Francis Ltd
DOI: 10.1080/1360086042000223535

draw on numerous sources within the reports and judgements issued by the Commission on recent legislation targeting cyber-criminality or bearing on the interception or tapping of telephones.[2]

The new provision requires, under threat of sanctions, that network operators and telecommunications service providers conserve call and caller data from within the frontiers of the European Union (EU) for a minimum period of 12 months.

In addition to this, a Royal decree on the protection of privacy, consulted upon within the Council of Ministers following an opinion delivered by the Commission, and setting down the time limit and type of data that may be conserved, has never been enacted.

Our examination of this provision takes the following course:

- Section 1 engenders an analytical description of the implications of the text: what do we understand by 'operators' or 'service providers'? What 'data' may or must be conserved?
- Section 2 touches on the current European debate concerning the fight against cybercrime, a debate that the fall-out from the events of 11 September 2001 has revived. In particular, it deals with the discussions held throughout the process leading to the adoption of the *privacy and the electronic communications sector* directive[3], and the debates regarding the provisions adopted in this regard by the European Convention on Cybercrime.[4]
- Finally, Section 3 is a critique of the legal provision itself, the object of this study, from the point of view of the principles of privacy enunciated in both Belgian and international European texts.

1. The Significance of the Provision

The legal provision[5] completes a recently introduced text. The law of 11 June 1998 modifying the law of 30 June 1994 relative to the protection of privacy from wire-tapping, examination and recording of private communications and telecommunications, had in fact already introduced the obligation of certain communications service providers to collaborate with judicial authorities. Under that law, the King determines, in accordance with the opinion given by the Commission for the Protection of Privacy, transmitted in a post-deliberation judgement issued by the Council of Ministers, 'the technical means whereby network operators and service providers must permit the detection, localisation, tapping, examination and recording of private telecommunications'.[6]

The main fear[7] expressed by the Commission for the Protection of Privacy with regard to this law was the risk of the introduction of a general regime of exploratory surveillance: contingent upon the limits that might be introduced under the Royal decree, the judicial authorities are in effect granted the right to extract information enabling general exploratory surveillance from data banks maintained by operators and service providers. Such a regime of general exploratory surveillance is forbidden under the principles established by the European Court of Human Rights on the basis of Article 8 of the European Convention.[8]

The addition introduced by the law of 28 November 2000 to section 1 §2 article 109b, E considerably amplifies the means granted to police authorities inasmuch as it allows them not only to access real-time, but also pre-recorded communications data. Indeed, telecommunications service providers are obliged, under threat of penal sanction,[9] to make data conserved within EU frontiers[10] available to the authorities for a 'minimum' of 12 months.[11]

The provision targets all 'telecommunications operators and service providers'. The term 'network operators', implies all providers of traditional transport and routing message services, whether public or private networks, such as intranets owned by particular administrations or organizations, regardless of whether these involve mobile telephony, radio broadcast, satellite, cable or other media.

The term 'communications service providers[12] 'further enlarges the provision's frame of application, implying as it does those myriad of providers offering internet services (access providers, message services, search engines, internet portals, discussion forums, etc.) or those who offer added value services, such as cryptography, trusted third parties or online banking. Even the owners of 'cyber cafés' and anonymization servers, etc., are included.

It is up to the Royal decree[13] envisaged by the law to determine, from within this list, those categories of services genuinely targeted by the legal provision. We may observe that the greater part of these 'operators' or 'providers' have no *a priori* reason whatsoever to conserve this data beyond termination of the actual connection.[14] Indeed, a good number of these services are free of charge. In other words, the only finality for the conservation of such data is in the context of a need to bring evidence in the event of an infraction being pursued. Such a conclusion has a bearing, both on the foundation for the legitimacy of such processes, as well as on the statute of those persons expected to carry out such conservation.

The data to be conserved will also be fixed by Royal decree. These will be, depending on the terms of enactment, telecommunications media[15] call data and service user identification data.

The list of such data is infinite.[16] The 'Discussion Paper' prepared by the Commission services for the meeting of experts, called on the 6 November 2002 to consider the question of data retention, lists more than 60 types of data that might thus be considered for collection and conservation.[17] We may note, as has Dinant,[18] that these traces are currently multiplying thanks to the increasingly generalized use of communication services in all sectors of professional and non-professional life. Furthermore, the identity of those conserving the information, as well as the nature, purpose and location of their archives, is becoming increasingly opaque to those individual citizens who are leaving their coordinates in the tender hands of networks, as often as not without their knowledge or permission.

Thus, when navigating via a search engine such as Lycos Altavista and visiting a site hosted by any given server, without even considering the numerous invisible operations possible, the typical internaut leaves a trail—with the operators of networks his trajectory follows, with access providers and with the various servers hosting the sites visited. The type of traces left within the given sample are varied. While the network operator conserves traces of network traffic (the number calling or rather the address of the message recipient), the access provider may be logging a trace of the various applications called on by the internaut's information system: the different sites visited, the pages called-up and the route taken, the length of each visit and, of course, the characteristics of the internaut's configuration. A similar wealth of information will be found with the search engine operator and with the cyber-marketing company with which that search engine is connected by invisible hyperlink.

The European texts, the Directive itself and the European Convention of the Council of Europe, marks out certain categories from within this data. The Council of Europe distinguishes between 'traffic-related data' and 'subscriber-related data', and the EU between traffic and location data. We shall return later to the importance of such distinctions.[19]

2. The European Debate on the Obligation to Conserve Traffic-related Data

Two European bodies are either currently discussing, or have finished their discussions on the obligation to conserve communication data and its corollary, the obligation laid upon private bodies, required to conserve data, to collaborate with public bodies such as the police and judicial authorities.

(a) The Council of Europe

On 8 November 2001, the Council of Europe adopted the first international treaty on 'cybercrime'.[20] It was presented for signing by the other Member or non-Member[21] States on 23 November that same year at the Conference of Budapest.

The text is based on Recommendation No. R(95)13 from the Ministers' committee regarding problems of penal procedure relative to information technology.[22] It is the fruit of work carried out by a committee created in 1997, which was given the task of drawing up a convention on cybercrime in cyberspace designed to reinforce international cooperation.

The Recommendation limited itself to prescribing 'specific obligations … for service providers offering telecommunications services to the public at large, via public or private communication networks, to deliver information necessary to the identification of a user, when required by the competent authorities charged with an inquiry'. In other words, it essentially involves permitting police authorities, within the context of an inquiry, to demand the identity of a client on the basis of a TCP/IP address, a mobile phone or fixed-line telephone number. The 2001 Convention contains various obligations for the signatory States, assuming, as Article 15 reminds us, that the installation of the intended measures is made subject to the 'conditions and safeguards envisaged by their internal laws which must assure an adequate protection of Human Rights and Liberties'. This general principle clearly involves the respect of Article 8 of the European Convention on Human Rights and of any jurisprudence based upon or interpreting that Article.

The first obligation concerns the 'rapid' conservation of specific data, including traffic data stored by computer systems. It is incumbent upon those people in control or possession of such data, and Article 16 envisages this rapid conservation as being for a maximum, though renewable, term of 90 days.[23] This provision is far from having the general range of its Belgian counterpart. It arrogates, within the framework of a specific infraction, the right to the relevant authorities to order a person already in possession of certain data to conserve it against the possibility of it otherwise disappearing. It does not authorize the State to impose supplementary data conservation obligations upon operators or providers and certainly not to operate such conservation as a general regime for all uses of their services.[24]

Article 17 makes plain that the conservation and divulgence of data on the basis of Article 16 concerns a quantity of traffic-related data sufficient to permit the 'identification of service providers and the route by which the communication was transmitted'.

Alongside this first prescription, Article 18 of the Convention obliges the Member States to introduce such measures as enable the competent authorities to order a service provider to 'communicate subscriber-related data' in their possession or under their control. Article 18 envisages that by 'subscriber-related data' it should be exclusively understood as data 'bearing on the identification of persons using the services supplied by operators and on the technical characteristics of the communications assured by these latter. On no account may

such data bear upon the content of correspondence exchanged nor of information consultable, in whatever form that may be, within the context of these communications.'

One may note that the obligation to divulge thus envisaged only concerns data already treated by providers in the normal course of their activities and only targets so-called connection data, that is to say data relative to the identity of persons connected to the service, to the exclusion of so-called traffic data, such as the list of sites visited, the length of the connection, etc.

This exclusion of data relating to the use made of a service is the fruit of long debates and, in particular, the marked opposition of a series of American and European associations for the defence of civil liberties[25] as well as a European group for the protection of persons with regard to the processing of data of a personal character, known as the Article 29 Group.[26]

(b) The European Union

The EU position, which has always privileged a 'protection of civil liberties' approach, has found itself considerably called into question in the aftermath of the events of 11 September 2001 on American soil.

As a particularly apt illustration of the initial EU approach, we may cite the reaction of numerous European instances upon discovering the existence of the satellite-tapping network known as ECHELON.[27] This network, for the most part managed by the USA, enables their intelligence services to intercept and analyse all or certain communications transiting via satellite, whether telephonic or electronic. Certainly, reactions to the STOA report of 1998[28] were slow to come at first, owing in part to the participation of the UK in the Echelon network, the presence of listening posts in Germany and England and, finally, the existence of a competing network run by the French. However, thanks mainly to the intervention of the European data protection group,[29] a rising wave of reactions would lead in time to a resolution voted by the European Parliament on 5 September 2001, in the wake of the Schmidt report. Here we may notably remark, among their considerations, the inclusion of a condemnation of interception practices not in conformity with the principles of the European Convention on Human Rights.

The European concern to protect the private lives of citizens in cyberspace is based on the recognition, within Europe, of data protection as a fundamental right[30] as much as, outside Europe, it is based on a modern vision of the principle of sovereignty.[31] However, it must take into account the imperatives of security and, in particular, the imperatives of the war on cybercrime. Since the treaty of Amsterdam, initiatives founded on the so-called 3rd Pillar,[32] that of intergovernmental cooperation in the fields of justice, both civil and penal, as well as internal affairs, are possible at the European level. This necessity for equilibrium is affirmed by a communiqué of the Commission Communication dated 26 January 2001:[33] 'The present communication questions the need of an initiative in order to define a global policy, and analyses the different ways to achieve it in the context of broader objectives. These are Information Society and the notion of a common space of liberty, security and justice in order to better the necessity of information infrastructures and the fight against computer viruses, in full respect of fundamental rights, according to E.U. commitments'.

Applying the principle of a counterweight to the 'obligation to conserve' certain traffic-related data, the communiqué distinguishes those processed by service operators and providers in the context of their normal activities of invoicing[34] and data whose processing is solely for the purposes of a criminal inquiry. With regard to the first category, the Commission considers that the Member States may adopt legal measures aimed at limiting

the range of an obligation to erase traffic-related data whenever such a limitation constitutes a necessary measure for the prevention, investigation, detection and pursuit either of criminal infractions or of the unauthorized use of telecommunications systems.[35]

With regard to the second category of data, the Commission considers that their recording and conservation cannot be justified other than for exceptional reasons and for a very limited period.

To this end, the Commission cites a resolution of the European Parliament that in a specific instance, namely the fight against child pornography, permits the conservation of traffic-related data for a period of 3 months as a quite exceptional case.[36]

The 11 September attacks and the American government's insistence that the European States improve their collaboration in the fight against terrorism and in particular review their mechanisms for the protection of electronic data in order to ensure a more effective front against terrorist organizations operating notably with the help of modern communication networks.[37] We observe that 'with all the urgency of a notion at war' and in record time, the White House has driven through Congress a number of legislative texts paving the way for an effective campaign against terrorism, in particular the Patriot Act,[38] of which certain provisions concern phone tapping.[39] With regard to these, we may note: that the US provisions do not involve any obligation upon communications service providers to conserve traffic-related data for any period longer than that necessitated by the normal requirements of the service they offer;[40] that the communication of such stored data is not imposed but is made voluntarily in the framework of 'codes of conduct' drawn-up between these providers and the security or judicial authorities and, finally; that the obligation to communicate traffic-related data is surrounded by procedural guarantees, criminal law and civil law sanctions that can be levied in the case of non-respect of the legal conditions imposed by the text[41] and may under no pretence give access to a communications' content.[42] Finally, pressured by the civil liberties defence lobby, the law envisages a 'Sunset'[43] clause, limiting the validity of its legal provisions to a term of four years.

The discussion underway since 2000 on a revision of the 97/66 directive on the processing of personal data and data protection in the telecommunications sector[44] should provide the principle framework for the European reply to this American request. This directive proposal was originally embedded within a series of proposals aimed at reforming the European telecommunications regulation[45] in order to adapt it to developments both in technology and in the telecommunications service market. The proposal, on reaching the draft stage, became the object of a 'Common Position decreed by the Council with a view to adopting the directive'.[46] This directive regarding the processing of data of a personal nature and the protection of privacy in the telecommunications sector was finally adopted on 12 July 2002.[47]

The initial proposal enunciated the principles under which traffic- and location-related data could not be conserved or used, other than for the purposes of invoicing and interconnection, without the express consent of the client within the framework of a value-added service offer. This initial proposal reiterated the solution already affirmed by the 97/66 directive. During the discussions which preceded the dramatic events of 11 September, the Council of Ministers telecommunications meeting of 27 June was already sympathetic[48] to the calls emanating from various police authorities, and accepted the addition of a phrase to section 10 of the preamble:[49] 'this directive does not affect the right of Member States to carry out legitimate interceptions of electronic communications or to take other measures such as ordering the conservation of traffic-related or localisation data for a limited period if such conservation is necessary and justified for reasons in conformity with the general principles of Community law.'

The aftermath of the attacks provoked vital discussions on this issue. On 20 September the meeting of European Justice and Internal Affairs Ministers adopted conclusions requiring all telecommunications providers to conserve data, grant police authorities access to it 'for the purposes of criminal investigation' and calling on the European Commission (EC) to revise European legislation in such a way as to guarantee a contribution to the efforts of authorities engaged in the application of criminal law.[50]

In response to this demand raised by the police, the Commission organized a 'cybercrime hearing' in Brussels on 27 November 2001.[51] This meeting was preceded by a meeting of experts, bringing together representatives of data protection authorities, the police and the communications industry on 6 November. The single stated object of this assemblage was the issue of the conservation of traffic-related data.[52] What emerged from these discussions, both the expert meeting and the cybercrime hearing of 27 November was:

- from the side of the industry, a dual point of view: that of the telecommunications service providers,[53] seeking to operate a regime of data conservation for the purposes of their own information systems security and uneasy at having to cooperate 'free of charge' with the frequently vague and poorly worded requirements of the authorities; versus the interests of those bearers of copyright, who might like to make use of police capabilities to better track down the sort of cyber-criminality which affects them, namely the illegal pirating of copyrighted works on the web;
- that of data protection authorities,[54] opposed to any conservation beyond the strict necessities of invoicing and, in a more general sense, desirous of defining any procedural measures in such a way as to ensure that they remain in perfect conformity with the fundamental rights and liberties of citizens and with data protection law: to this end the commissioners for data protection recalled the prohibition against any general measures of surveillance and the necessity of providing a concrete justification for the retention even of specific traffic-related data. Further, 'the period of data retention and the quantity of data conserved must be in proportion to the gravity of the criminal infraction'. Finally, the data protection authorities underlined the sensitive nature of traffic-related data inasmuch as they reveal the behaviour of an individual in an era of ever more pervasive use of telecommunications media in daily life;
- that of the police, who consider it vitally important that they be able to resolve cases thanks to the conservation of traffic- and location-related data and the cooperation, willing or imposed by law, of telecommunications service providers. The authorities stressed the absolute necessity of such cooperation for certain types of infraction,[55] inasmuch as its absence in these cases would make it absolutely impossible for them to detect the criminals. Finally, the police authorities justified the long list of traffic-related data to be conserved as well as the period (between 6 months and 2 years).

The European authorities. The European authorities had to draw conclusions from these debates by slightly modifying the text of the draft directive. Thus the final text expanded those legitimate finalities for which network providers or telecommunications services may process traffic- or location-related data. Article 6.5 adds the finality of fraud detection and stipulates that the permission of the person concerned is no longer required before data is processed with a view to commercialization through value added services, although the text specifies that such processing must be limited to that which is essential to such activities. Above all, Article 15 authorizes Member States to

> … adopt legislative measures aimed at limiting the rights and obligations envisaged under Articles 5 and 6, Article 8 paragraphs 1, 2, 3, and 4, and Article 9 of the present

> directive, whenever such a limitation constitutes a necessary measure for the safeguarding of national security—that is to say, the security of the State—as well as public defence and safety, or to assure the prevention, research, detection and pursuit of criminal infractions or unauthorized use of electronic communications systems, such as those envisaged under Article 13, paragraph 1 of the 95/46/CE directive.

To this end, the text adds

> Member States may, among other things, envisage the conservation of data for a limited period, when such conservation is justified by any of the motives included in the present paragraph, within the respect of the general principles of Community law.[56]

This revised text leaves each Member State free to proceed as it wishes, while nonetheless imposing observance of that which, according to Article 6 of the European Union Treaty of 7 February 1992,[57] constitutes a general principle of the European Union: the respect of Human Rights and fundamental liberties

> … such as they are guaranteed by the European Convention on Human Rights and Fundamental Liberties, signed in Rome on the 4 November 1950 and such as they are to be found expressed in the constitutional traditions of the Member States.

In other words, the text returns us to the obligation of Member States to respect Article 8 of the Convention and, according to the authors,[58] the jurisprudence of the Strasbourg Court taken in application of this same Article 8 as the privileged source of inspiration for Community law.

However, the obligation to respect the Convention does not forbid divergence of interpretation among the Member States with regard to the precise import to be given to this reference. In this sense, it does not meet the objections of the service providers, uneasy at the differences of interpretations that may be given by the governments of Member States to a provision that is as vague as this one, as much with regard to the period of conservation as with regard to the kind of data to be conserved or the modalities of that conservation. The text also transgresses the principles of data protection as they are interpreted by the data protection authorities and, finally, while agreeing with them as regards the principle of data conservation, the text sends the judges and politicians back to their national governments to obtain a national legalization of the obligations to conserve and to cooperate on the part of infrastructure and service providers. Thus we note that, in the context of a law on daily security measures[59] from the 31 October, the French legislator is expected to make use of the competences granted to national legislators within those texts whose tenor we shall be subjecting to critical examination under Section 3. It suffices to note here that the European Directive text confers upon the so-called 'Group of Article 29', composed of the representatives of the various data protection authorities, an important role in the interpretation to be given to the Community text, a role that may prevent national divergences or over-lax interpretations.[60]

3. Critical Analysis—Possible Follow-up Paths Regarding the Legal Obligation to Conserve Data and the Obligation upon Telecommunications Service Providers to Cooperate with Authorities

The complements brought to paragraph 2 of Article 109bE by the cybercrime law resemble an anticipatory transcription of a directive that is currently being approved. Our intention

in this last section is to suggest certain pathways for reflection that may serve as regulatory guidelines, with the aim of ensuring the law its full effect, while at the same time offering a review of the choices taken by our legislators.

Our first reflection is a preliminary one. It underlines the importance of the information that is actually at issue when one speaks of localization-related or traffic-related data. The notion of traffic-related data is defined by the European legislator as: 'all data treated in the course either of routing a communication via an electronic communications network or of invoicing it', and defines localization-related data as: 'all the data carried in an electronic communications network indicating the geographic position of the terminal equipment of the user of a publicly accessible electronic communications service'.

Such data is infinite: it includes, beyond simple connection information, the duration of our communications, the persons they are sent to, the sites we visit, the length of messages exchanged, the technical characteristics of the message and of the user's information system. Meanwhile localization data can be used to reveal the exact position of the owner of a cell-phone or GPS, even when it is not in use. Our increasingly intensive use of information technologies, together with the expansion of value-added services that grow up alongside them, betray the relationships we have with others, our movements, our tastes, our convictions, our illnesses … leaving a vast web of traces with a diversity of actors in a diversity of locations. Diverse, yes, but nonetheless vulnerable to being gathered and reconnected, thanks to the inherent characteristics of increasingly powerful information processing programmes, networks and systems.

Basically, the possibility of such access to a multiplicity of files and the ability to interconnect the data content thus gathered creates very tempting opportunities to the police and judicial authorities. Beyond this, we may raise the question as to whether it is possible to maintain a distinction between traffic-related data and the actual content. This distinction, which was always perfectly clear in the days of conventional telephone communications, is no longer present in modern networks, where so-called traffic-related data in fact reveals the very content of the communication, as is the case when accessing a web page or site.

Should limits be introduced to such conservation, particular modalities imposed on these operations and restrictions applied to the possible access of the authorities charged with the pursuit of infractions? We may recall in this context the fundamental verdict of the European Court of Human Rights, known as the Klass verdict of 6 September 1978, in which the Court recognized the discretionary powers of Member States with regard to the choice of surveillance systems to which they might have recourse, while underlining that such discretionary power was not to be used arbitrarily:

> Conscious of the danger inherent within such a law of undermining or even destroying the very democracy it seeks to defend, the Court affirms that they [*the Member States, trans.*] may not, in the name of the war against espionage and terrorism, simply introduce any measure they might deem appropriate … . The principle question which arises at this juncture, on the basis of Article 8, consists in knowing whether the terms of paragraph 2 are sufficient to justify the unwarrantable interference so far observed. By providing for an exception to a right that is guaranteed under the Convention, this paragraph calls for the very strictest of interpretations. The power to place citizens under secret surveillance, one so characteristic of the 'police state' is, according to the Convention, tolerable only with regard to such measures as are strictly necessary for the safeguarding of democratic institutions.[61]

In its recommendation number 2/99, concerning the respect of privacy in the context of telecommunications wiretapping,[62] the Group for the protection of persons with regard to the processing of data of a personal nature, summarized those guarantees deriving from the relevant Council of Europe jurisprudence[63] that are to be respected in surveillance situations.

It is incumbent upon national legislations, via such legal instruments as are accessible to all citizens,[64] to lay down, in language both precise and vigorous, the obligation to respect all the following provisions:

- those authorities which are authorized to permit the legal interception of telecommunications, the services authorized to carry out such interceptions and the legal basis for their intervention,
- the finalities under which such interceptions may take place, which same should permit an appreciation of their proportionality with respect to the national interests at stake,[65]
- the prohibition of all exploratory or general telecommunications surveillance on a large scale,[66]
- the circumstances and precise conditions (such as factual elements justifying the measure and its duration) to which interceptions are submitted, within that respect of the principle of specificity to which all incursions into the private life of citizens are subject,[67]
- respect of the specificity principle, corollary of the prohibition of all exploratory and general surveillance, implies, more precisely with regard to traffic-related data, that the authorities may only have access to such information on a case by case basis, and in no way as a general or proactive measure,
- the security measures applied in the storage and processing of such data, as well as their period of conservation,
- with regard to those persons indirectly or randomly implicated in wiretapping measures,[68] the particular guarantees to be brought to the processing of data of a personal nature: notably the criteria justifying the conservation of data and the conditions governing its communication to third parties,[69]
- the informing of the person under surveillance as soon as possible,
- the types of recourse available to the person under surveillance,[70]
- the modalities of the monitoring of these services by an independent control authority,[71]
- the rendering public—for example in the form of regular statistical reports,[72] of telecommunications interception policy effectively taking place,
- the precise conditions under which data may be communicated to third parties in the framework of bilateral or multilateral accords.[73]

The application of these principles to measures that go beyond simple interception of electronic communications to extend to the analysis of communications data prior to an event raises a number of comments. The Belgian provision demands that all electronic communication providers and operators store certain communications data without differentiating between the persons concerned. It is difficult, in the light of such stipulations, not to speak of general surveillance. Indeed one may be justified in fearing, as does the European MP, Mr Cappato, reporting to the European parliament within the debate that currently occupies us, that the person under surveillance, the 'enemy', does not in fact turn out to be 'the simple citizen surfing the net or making a phone call'. This critical remark

on the legitimacy of such measures calls forth other reflections. One consists of distinguishing between processes, depending on the original finality; a second raises questions on the proportionality of the measures taken when compared to the dangers supposedly justifying them; yet another raises the question of risks actually created by the processing carried out under the stipulations at issue.

(a) Two Types of Processing

The general character of the Belgian text, in contrast to the French law,[74] does not distinguish data legitimately conserved by communications services operators and providers in the framework of their own business activities, from other data whose conservation does not fall *a priori* within this framework. As we have noticed, beyond the consent of the person concerned, the European directive[75] legitimizes data conservation for two finalities: (a) that of invoicing and payment, and (b) that of the security of a particular operator's or provider's own information system or network (hacker tracking, sabotage, viruses, etc).[76]

For data conserved and processed within the context of these finalities, its communication to the police authorities represents an ulterior process when viewed through the optic of data protection legislation, compatibility with which augments as a function of the following principles.

With regard to that data for which no legitimate conservation finality whatsoever exists either with the operator or with the provider, the only legitimate finality resides within the pursuit of infractions. In other words, in the second case, it is the public authority that is directly responsible for the processing, the task of which it confers either upon the operator or provider concerned, or upon another service, who will be charged with the collection of data from different operators and/or providers. These providers, operators or services are, in other words, only subcontractors to the public authority and, in accordance with Article 16 of the directive, are prohibited from making use of the data to any finality outside that of the mission they have had conferred upon them.

In this second case therefore, conservation may only be legitimized within the context of the objective imperatives of a police investigation.

We are States under the rule of law, and the Convention to which we adhere imposes that those who call for the conservation of data must show the imperative social interest of such a measure with regard to the rights and liberties thereby diminished. Where are such justifications? The police authorities seemed singularly mute when questioned on this issue at the meeting of experts convened by the EC to prepare this forum. They appeared incapable of presenting anything other than opinions and news clippings where statistical, social and psychological studies might have been able to demonstrate that the preparation of grievous crimes is genuinely taking place via electronic communications media, and that effective investigation of such crimes genuinely requires swift access to the data traces of such use. Rather to the contrary, the confrontation between police authorities and service providers revealed the lack of precision in the demands of the former, the tentative nature of their efforts and the rarity with which such measures achieve any real success.

(b) The Legitimacy of Investigative Police Processing

The legitimacy of data processing rests on an examination of proportionality: do the risks to the security of the State, or the protection of its citizens, justify an all-round regime of

data tracing? Is the suggested means, namely the obligation bearing on telecommunications operators and providers to conserve, necessary to the obtaining of such objectives?

In reply, the gravity of the crime is usually invoked as a justification for such incursions. We pose the question: is there a strong and necessary link between the granting of such means to the police authorities and the discovery of the criminals concerned?[77] The answer is no. Indeed, on the contrary, we may observe herein a means to facilitate detection of other far more minor crimes directly linked to the use of communication technologies, such as copyright violations of works available on the net,[78] attempts to hack into computer systems, fiscal fraud, etc. What should we think of an argument that rattles the skeleton of terrorism, while in reality hitting quite different targets, such as white-collar crime, the detection of whose authors hardly justifies recourse to such draconian measures as those envisaged. Should we not in any event—and the previously cited resolution of the European Parliament to combat child pornography[79] alludes to this—only reserve the use of such means as these for major infractions?

The rules of proportionality, necessity, foreseeability and legality of measures that restrict our fundamental rights and liberties lead us in any case to demand that the law be precise with regard to strict limits for the duration of such conservation, that it defines the identification data concerned (would not user connection data and the moment of 'transaction' alone be sufficient?)[80] as well as limiting the obligation to conserve to certain service providers only, those who actually grant access to the network. In particular, a distinction must be made between police operations involving data that is already conserved by telecom companies within their normal activities, and such operations as involve other data, such as is only gathered and conserved for police purposes.

The legislator is thus called upon to act here, as in other such situations, with 'trembling hands', all the more so since the consequences of the stipulations at issue engender such risks as those we shall go into below.

(c) The Risks of Such Processing

The first risk is that of regulatory deviation: even with the limits recalled above and clearly affirmed at the outset, we may fear nonetheless that the ink will hardly have dried on this law before its range begins to be progressively enlarged and those guarantees judged too 'awkward' begin to be ignored in the interest of increased effectiveness. Since the first Belgian law on communications tapping, five other laws have succeeded it, each slightly enlarging the scope of the police in the accessing of private communications. Thus tomorrow we will surely hear it said that, since such vast reservoirs of data exist, should they not be accessed more widely?[81] This tendency, once an exception has been introduced, to add some others, is most disquieting. How not to be struck by the wisdom of the American 'Patriot Act', limiting as it does the total duration of such exceptional measures to a period of 4 years, whereby we may note in addition that the obligation to conserve data does not even feature among them.

Among the first negative reactions to such measures, lawyers have highlighted the danger that, in their eyes, is represented by thus facilitating incursions on professional confidentiality. The police will indeed have some considerable difficulty sorting out, from among all the communications where they order intercepts, those covered by professional confidentiality from the others.

Furthermore, we should not forget that reinforcing the regulations on cyber-surveillance demands the existence of an independent monitoring authority. Yet are we sure that the

control of investigations carried out in the field by highly trained police teams will be effective, that the judicial authorities or specifically created monitoring bodies will always be able to grasp the significance of the use being made of such new investigative tools? Finally, does not the circulation of information within networks cooperating at an international level demand a reinforcement of the democratic and juridical controls of organizations such as Europol, Interpol, or of the future 'Eurojust' or Enfopol?[82]

Other deviatory risks were already underlined by the Belgian 'Privacy' Commission[83] during the debate prior to voting the cybercrime law. The simple existence of such files creates the risk of their abuse: providers and operators forced by law into such storage will be tempted to benefit in other ways from their labours. Beyond questions of the security of their own networks or services, we have reason to be nervous about the profiling of users either for their own internal ends or for commercial purposes. Of course one might want to consider confiding the management of such files to third parties specialized in conservation, or all the more so to police authorities, but this would be substituting, for the danger already described, that of the creation of gigantic mammoth files within which every kind of interconnection becomes possible.

If the European Court of Human Rights considers that even the simple storage of data for police finalities represents an attack on our liberties (see, for example, the Klaas, Lüdi, Rotaru and Ammann cases), the consequences of processes induced by the legislation we are dealing with here call for even more significant precautions. Indeed we have reason to fear that police forces might pull the initial elements of their enquiry out of such vast reserves of data, even prior to any other investigation (tracing of those persons close to the 'scene of the crime', list of their correspondents, last call in, last call out, etc.). Or even worse, they might even be tempted to find within such files the means of attempting an exploratory surveillance of so-called 'risk groups', those who frequent this or that website, those who log in from a particular 'hot' location, suspected 'terrorists' or 'hackers', etc.

Thus it is absolutely necessary to

> prohibit any setting-up by the security services of a general access to the information conserved: consulting the conserved data should take place as part of a precisely regulated procedure, on the basis of case-by-case requests. It should not be possible to install any kind of permanent access to this data, such as would enable the introduction of automated processes that could be used for general network surveillance. The physical conservation of the data should be the sole responsibility of the companies concerned by the obligation, who should strictly limit access.[84]

Conclusions[85]

The fight against cybercrime is affirmed as a priority without which society's very survival is at risk. Thus, in the name of security, and strengthened in an opinion that is constantly being relayed and amplified by the media, politicians at the National or European level are hurriedly preparing legislation to increase judicial and police powers in order to wage war on cybercrime. Do we dare to remind them that Bin Laden's cohorts, always assuming they were the ones responsible for the events of the 11 September, seem to have had no recourse whatsoever to the vaunted virtues of the Internet in the commission of their crimes?

What do these rapidly scribbled legislations envisage? They oblige the various electronic communications service providers, whether private or public, to archive the data resulting from our use of their services for a certain period, fixed by some at one year (Belgian

legislation even sets this as the minimum!).[86] This data archive is drawn up on the entire population as a preventative measure, without the slightest concrete suspicion.

Without doubt, some would reply to those defenders of civil liberties, that their vaunted freedoms are a luxury, one that we cannot afford when lives are in danger. They would add that the honest citizen has nothing to fear from this surveillance that gives assurance to their lives, unmasking the villain without frightening the good and the upright. Some would even go so far as to say that such surveillance forces us to adopt behaviour more in accordance with civil norms.

To those I would reply: there is no worse danger than this cyber-surveillance, which hunts a man down in his most intimate space and raises within him a perpetual and haunting fear of exposure.

> Through a perverse reversal, this obsessive pre-eminence of the gaze of authority[87] occurs in the very name of that which it destroys. For the values behind which it shelters are indeed of the highest order: justice, truth, liberty, democracy, due process of law, good citizenship, integrity. Who cannot fail to see that this all too abrasive vision, by wearing away all that it lingers upon, flays away to the bone certain principles that are among the foundations of our lives together? When that just proportionality which should reign, between the means made available to investigators and the actual goals of the investigation, is no longer respected, then a consecration of the process of investigation and exposure begins to assume 'method' rather than 'cause' as its sole legitimacy.[88]

Furthermore, by artificially creating a sense of security, such measures absolve those who employ them from questioning the rationale behind such crimes and from drawing up the instruments of prevention policy that may offer a response to this rising tide of violence. Everything is undertaken in the interest of criminalizing the act and defending society, and no further questions need be asked. Yet we know well that crime will always either migrate elsewhere, or become yet more violent, if its root causes are not genuinely addressed.

Notes and References

1 Concerning Section 1, §2, Article 109b of the Belgian law of 25 March 1991 as introduced by the Belgian law of 28 November 2000 on cyber-criminality.

2 In this connection, apart from the *opinion* delivered by the Commission for the protection of privacy regarding the law of 28 November 2000 quoted below in note 4, we draw attention to the following opinions: Opinion of the Commission on privacy of 20 March 2000 on the proposed law concerning the identification and the location of the postal numbers of communications or telecommunications and modifying Articles 90c, 90d, 90f and 90g of the Criminal Code; Opinion of the Commission on Privacy of 9 July 1997 on the application of Articles 202 and 203 of the law of 21 December 1994 containing social and other provisions (technical cooperation of the operators in carrying out judicial measures regarding wire-tapping); Opinion of the Commission on Privacy of 27 November 1994 on the amendments to the proposed law modifying the law of 30 June 1994 relating to the protection of privacy against wire-tapping, to obtaining cognizance of and recording private communications and telecommunications; Opinion of the Commission on Privacy of 23 March 1998 on the proposed organizational law for the intelligence and security services; Opinion of the Commission on Privacy of 24 March 24 1999 on the draft of the royal decree relating to the carrying out of the provisions of the law of 30 June 1994 relating to the protection of privacy against tapping, to obtaining cognizance of and recording private communications and telecommunications and of Article 109c E, §2 of the law of 21 March 1991 applying reforms to certain economic public enterprises, concerning the obligation for the operators of

networks of telecommunications and suppliers of telecommunications to lend their support; Opinion of the Commission on privacy of 28 February 2002 on the draft of a law modifying Article 44 of the organizational law of 30 November 1998 of the intelligence and security services.

3 Directive 2002/58/CE of the European Parliament and of the Council of 12 July 2002 concerning the treatment of personal data and the protection of privacy in the sector of electronic communications, J.O.L.202/37, 31 July 2002.

4 European convention on cyber crime, Council of Europe, European Treaty No. 185, open to the signature of the Member States, 23 November 2001, Budapest (available on the site of the Council of Europe: http://www.coe.int/treaty/fr/projets/cybercrime.htm).

5 For an analysis of this provision, the reader is referred to the articles published on the law of 28 November 2000 on computer crime; see C Meunier 'The law of November 28 2000 relating to computer crime, in current law relating to information technologies and communication' *CUP*, Actualites du Droit, Vol 30, February 2001, in particular p 151; Fl De Villenfagne and S Dusollier 'Belgium takes up arms against cyber crime' *Authors and Media*, 2001, p 77; Y Poullet 'Concerning the proposed law No. 214: the struggle against cyber crime in cyber space set against the principle of the regularity of evidence', in H Vuye and Y Poullet (eds) *Liber amicorum J. du Jardin*, Kluwer, Dordrecht, 2001, p 20. Compare also the writings of the author of the proposed law on the subject: P van Ecke *Criminaliteit en Cyberspace* Miys and Breesch, Gent, 1997, in particular, p 107; and P van Ecke 'Het voorontwerp van wet inzake informaticacriminaliteit', in *Recente ontwikkelingen in informatica- en telecommunicatie recht*, ICRI, Die Keure, Brugge, 1999, p 238.

6 A first draft of a royal decree determining these 'technical means' had been severely criticized by the Commission (opinion No 12/99 of 24 March 1999). A second draft of the royal decree is currently being examined. Compare in this connection, the opinion of the Commission for the protection of privacy No 09/97 of 20 March 1997 (Reporters B De Schutter and Y Poullet): 'With regard to such considerations and to the extent that Article 22 of the Constitution reminds us of the necessity for legislative measures for any authorization that goes against the principle of respect for privacy, the Commission cannot admit that the question be settled by a royal decree without strict limits being set on this royal intervention. The Commission further furnishes the reminder, in particular, that such technical measures cannot legitimize the practices of preventive localization or interception, that they cannot lead the authorities to have at their disposal information that is disproportionate to that needed for the investigation, and that they must respect the strictly exceptional nature of wire-tapping'.

7 Opinion No 33/99 of 13 December 1999 relating to the Bill relating to computer crime (reporters B De Schutter and Y Poullet), opinion available on the site of the Belgian Commission for the protection of privacy (http://www.privacy.fgov.be) and published in the parliamentary documents of the House of Representatives (Doc. Parl. Chambre, 0213/004). It should be noted that this opinion was initiated by the Commission, the latter not having been consulted by the Government. Compare also the very critical opinion of the State Council, published in Doc. Parl. 213/002).

8 We shall return below in No 21 to the provisions of the Convention of the European Council regarding cyber crime, in particular Article 17 which provides for a 'rapid display and disclosure of data relating to the traffic'. This convention, which was adopted on 8 November 2001, did not of course exist when the Commission gave its opinion on the law of 1998.

9 The new section 3 of Article 109c E in fact sanctions the supplier who does not fulfil his legal obligations with 3–6 months' imprisonment and/or a fine of 26–20,000 Bff.

10 The proposal mentioned the obligation to conserve the data on Belgian territory in order to avoid the procedural questions of international penal cooperation in the case where the request concerned data stored abroad (compare the arguments of the Minister, in Doc. Parl., Chambre, 0213/004, p 47). The EC (Opinion contained in Doc. Parl. Chamber, 0213/011, p 17) reacted strongly against a provision judged contrary to European principles of freedom to provide services and freely circulate them. The Belgian government gave in to these European arguments (Doc. Parl. Senate, 2-392/2, p 6).

11 The time limit for conservation was fixed at 'a minimum of 12 months' at the last minute. The first proposal of law allowed the King to fix the time limit. In its opinion the Commission had considered that it was necessary for the legislator himself to pronounce on the time limit in view of the impact of this provision on our personal freedom. The Commission for the protection of privacy (opinion already given) had pleaded for a shorter time limit: 3 months as advocated by German law and Recommendation No 3/99 relating to the conservation of data relating to the communications for the offerers of Internet service with a view to ensuring respect for the law of the Group for the protection of data instituted by Article 29 of the Directive 95/46/CE, a text available on the site of the server of the European Union at the address: http://www.europa.eu.int/comm/dg15/fr/media/dataprot/wpdocs. There was a fierce parliamentary debate between the supporters of long conservation in response to the requirements of police enquiries and those who were concerned by the fact that a long wait would constitute a threat to freedom as well as being a financial burden to our business enterprises (also along these lines the opinion of the EC contained in Doc. Parl., Chambre, 0213/011, p 18). At the last minute the idea of fixing the time limit at 12 months was replaced by the current text which strongly favours those who uphold the protection of public order and investigatory requirements (concerning this debate, read Doc. Parl. Senate, 2-392/3, p 47: the hearing of a member of the National Computer Crime Unit and p 62: the way in which the balance between privacy and public order must be established according to the Senate).

12 The notion of 'communications service' refers to that defined by the law of 21 March 1991 on autonomous public enterprises: 'service consisting, in part or wholly, in the transmission and distribution of signals by telecommunications signals, with the exception of radio and television'. Compare with the notion of 'service provider' adopted by the Convention of the Council of Europe on cyber crime (Article 1). ' "Service provider" designates any public or private entity that offers among its services the possibility of communicating by means of a computer system; any other entity treating or stocking computer data for this communications service or its users'.

13 The Belgian commission criticized the royal delegation considering that Article 22 of the Constitution required a law (opinion published in Doc. Parl. Chambre 0213/004, p 30).

14 In this respect, see the remark by the Commission for the protection of privacy, p 9.

15 The account of the reasons (Doc. Parl., Chambre 0213/001, p 30) makes it clear that it is notably a question of data relating to the origin, destination, duration and localization of the calls. The Senate (Doc. Parl., 2-392/3, p 31) thus considers that the IP addresses of computers used for sending and receiving electronic telecommunications, the log-ins and log-outs, the time and beginning of the Internet addresses visited form part of the call data.

16 The EC (opinion published in the parliamentary documents of the Chamber (0213/011, p 18) strongly criticizes the absence of any definition of such notions. Similarly, the criticisms of the Commission for the protection of privacy, opinion published in the parliamentary documents of the Chamber (0213/004, p 30).

17 Annex 2 of the Discussion paper (29 October 2001) prepared by the services of the Commission in the framework of the EU Forum on Cyber crime of 27 November 2001 and of the preparatory meeting of experts of 6 November 2001 draws up the long list of types of data likely to be recorded and does so by type of Internet service: thus, for the e-mail server: SMTP log; date and time of connection of client to server; IP address of sending computer; message ID; sender e-mail address; receiver e-mail address; status indicator; POP log or IMAG log; date and time of connection of client connected to server; IP address; user ID; (in some cases) identifying information of e-mail retrieved; file upload and download servers; for the FTP(File Transfer Protocol) log, date and time of connection; IP source address; user ID; Path and filename of Data object uploaded or downloaded; for the web services: http log; date and time of connection; IP source address; operations (types of command); path of operation; last visited page; response codes; etc.

18 Y Poullet and J-M Dinant 'Le réseau Echelon existe-t'il? Que peut-il faire? Peut-on et doit-on s'en protéger?' Specialists' report drawn up for the attention of the Permanent Committee of Control

of the Intelligence Services, May 2000, confidential Doc., p 6; compare by the same author the excellent report drawn up on the European project ECLIP, available on: http://www.droit.fundp.ac.be/textes/privacy_law_tech_convergence.rtf.

19 See, note 21 below.

20 Concerning this convention, we pick out, among other commentaries, the following: E M Gning 'The proposed convention on crime in cyber space' *Lex Electronica*, Vol 6, No 2, 2001 available on: http://www.lex-electronica.org/Articles/v6-2/gning.htm; L Costes 'La Convention du Conseil de l' Europe du 8 novembre 2001: Premier traité international contre le "cyber crime" ' *Lamy, Cahiers droit de l'Informatique*, No 142, 1–9, December 2001.

21 Thus, the US, a non-member of the Council of Europe, signed the Convention the day it was open to signing by the States.

22 Available on http://www.coe.fr/cm/ta/rec/1995/f95r13.htm.

23 The conservation period of one year had been foreseen. It was considerably reduced following the pressure of the bodies controlling the protection of data and by associations concerned with the defence of civil liberties.

24 It should be noted that the European Parliament in its opinion of 6 September 2001 had insisted on the fact that 'a general principle of conservation should not be introduced'.

25 In this connection, we can stress the role played by EPIC (US), International Privacy (UK) and the Electronic Frontier Foundation.

26 This is shown very clearly by Recommendation 2/99 concerning the respect for privacy in the context of the interception of telecommunications, adopted 3 May 1999 (WP 18, 5005 99/final).

27 Read the specialist report on this network drawn up for the attention of the Belgian Committee for the surveillance of intelligence services by Poullet and Dinant, *op cit*, note 18, available at http://www.crid.ac.be: and especially the remarkable study by D Yernault 'De la fiction à la réalité: Echelon, le programme d'espionnage électronique global et la responsabilité des Etats en ce qui concern le respect de la Convention européenne des Droits de l'Homme' *Revue belge de droit international*, 2000, p 136.

28 Compare the report 'An evaluation of the techniques of political control (September 1998) and several studies (April and May 1999) published by the STOA (Scientific and Technological Options Assessment) of the European Parliament.

29 Compare in particular, the recommendation concerning the respect for privacy in the context of the interception of telecommunications (Recommendation 2/99 of 3 May 1999, Doc. 5005/99 final WP; 18, available at the address: http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs).

30 In this respect, we note that the Treaty of Nice, which fixes the European Charter of fundamental rights, clearly distinguishes the protection of a person's private and family life (traditional view of privacy) and the protection of privacy (a modern and enlarged view of privacy). Concerning this distinction, see our comments that will appear in 'For a justification of Articles 25, 26 and 4 of the directive 95/46 in respect of the protection of data', a paper presented at the International Conference organized by the European Commission on the transposition of the directive 95/46/CE (30 September to 1 October 2002).

31 On the evolution of this concept in the global information society, our remarks can be found in Poullet and Dinant, *op cit*, note 18, on the Echelon network.

32 On the characteristics of this third Pillar, its particular procedures and its merits, see D Vignes 'Plaidoyer pour le 3ème pilier' *Common Market Review*, 1996, p 273. Regarding computer crime, the Commission recently introduced in the context of this third pillar a proposal for a decision by the Council concerning attacks on information systems (Brussels, 19 April 2002, COM [2002°173 final]). This proposal seeks to harmonize the way criminal infractions are defined and to define the competence of each Member State in respect of the legal proceedings taken against such infractions, as well as the way they can collaborate.

33 Communication of the Commission to the Council, to the European Parliament, to the Economic and Social Committee and to the Regional Committee: 'Create a safer information society by

reinforcing the security of the information infrastructure and by fighting against cyber crime', Brussels, COM (2000) 890 final.

34 In conformity with the community directives on the protection of data of a personal nature, and more precisely with the general principle of limiting transfers to a specific purpose, a principle expressed in the directive 95/46/CE and with the particular provisions contained in the directive 97/66/CE, the traffic-related data must be erased or rendered anonymous as soon as the telecommunications service has been provided, except when the data are required for invoicing purposes. In the case of fixed or free access to the telecommunications services, the suppliers of the services are, in principle, not entitled to keep the data relating to the traffic.

35 The precise communication, echoing moreover the provisions of Article 14 of the directive 97/66/CE and of Article 13 of the directive 95/16.CE, is the following: 'However, any legislative measure taken on a national scale which would provide for the conservation of the data relating to the traffic in order to be able to implement the laws should fulfil certain conditions. The proposed measures should in fact be appropriate, necessary and proportionate to the goal being pursued, as provided by community law and international law, notably directive 97/66/CE and directive 95/16.CE, the Convention for safeguarding human rights and fundamental liberties of 4 November 1950 and the Convention of the Council of Europe of 28 January 1981 for the protection of persons in respect of the automated treatment of data of a personal nature. The respect for these conditions and principles is all the more important for the measures that involve the systematic conservation of data for a large portion of the population.

36 The legislative resolution containing the opinion of the European Parliament on the common action proposed has been adopted by the council on the basis of Article K.3 of the Treaty of the European Union—in respect of the fight against child pornography on the Internet, amendment 17 (JO, C219 of 30 July 1999, p 68).

37 Compare in particular the articles published by the newspapers in October following the discussions between President George Bush and the Belgian Prime Minister, Belgium then taking over the presidency of the EU; e.g. *la Libre Belgique* of 22 October 2001; *Gazet van Antwerpen* of 26 October 2001.

38 'Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism' (USA Patriot Act) Act of 2001, H.R. 3162, 1st Session, 107th Congress, available on site http://thomas.loc.goc, approved by the Senate 25 October 2001 and signed by President Bush 26 October 2001.

39 In this respect, we can note the declarations of Bush following the passing of this law, when he was putting the presidential signature to the law: 'This law will give intelligence and law enforcement officials new tools to fight a present danger to counter a threat like no other our nation has ever faced'.

40 Section 222: 'Nothing in this Act shall impose any additional technical obligation or requirement on a provider of a wire or electronic communication service or other person to furnish facilities or technical assistance …'.

41 Section 223: 'Civil Liability for certain unauthorized disclosure'.

42 Section 212 inserting notably a new §2703 'Required disclosure of customer communications or records': 'A provider of electronic communications service or remote computing service shall disclose a record or other information pertaining to a subscriber or to a customer of such service (not including the contents of communications covered …) to a governmental entity'.

43 Section 224. Concerning those measures which, according to Senator T Dashle, ensure 'an appropriate balance between protecting civil liberties, privacy and ensuring that law enforcement has the tools to do what it must': 'Negotiators have placed safeguards on the legislation, like a four-year expiration date on the wiretapping and electronic surveillance portion, court permission before snooping into suspects' formerly private educational records and court oversights over the FBI's use of a powerful e-mail wiretap system' (J J Holland 'Senate sends antiterrorism legislation to Bush' text available at: http://www.washingtonpost.com/wp-dyn/Articles/A51682-2001Oct25.html).

44 JO, L.24 of 1 January 1998, p 1.

45 On this common position, see Y Poullet, S Louveaux and M V Perez-Asinari 'Data protection and privacy in global networks: a European approach' *EDI (Electronic Data Interchange) Law Review*, 2001, p 147.

46 The common position was adopted by the Council on 21 January 2002 (Institutional Dossier 2000/0189 [COD], 15396/01).

47 Directive 2002/58/CE, JO. 31. 7. 2002, L.201/37.

48 Under pressure from the French and English governments.

49 The commission, through its commissioner E Likkanen, had insisted on the fact that such a phrase could not have the status of a 'Recital and could not be included in the text of the convention'.

50 'The Council requests the EC to submit proposals for ensuring that law enforcement authorities are able to investigate criminal acts involving the use of electronic communications systems and to take legal measures against their perpetrators. In this context, the Council will be making a particular effort to strike a balance between the protection of personal data and the law enforcement authorities' need to gain access to data for the purposes of criminal investigations.' (On these conclusions, see the report of the English association Statewatch, EU governments want the retention of all telecommunications data for general use by law enforcement agencies under terrorism plan, available at http://www.statewatch.org/news/2001/sep/20authoritarian.htm.)

51 A first hearing had been organized on 7 March 2001 regarding its communication on cyber crime in such a way as to allow the representatives of each category of interests (network operators; service providers; public bodies for the protection of data; associations for liberties) to put forward their point of view.

52 Regarding this meeting, compare the discussion paper prepared by the services of the Commission and available on the Commission's site at the address: http://europa.eu.int/information_society/topics/telecoms/internet/crime/wpapnov/index.htm.

53 Compare in particular the position of AOL: 'AOL retains only data that is necessary either for billing purposes, fraud prevention or security'. 'AOL cannot cost a potential data retention obligation without understanding fully what would be required from us. However, some costs consideration would be, not only the storing of data but more importantly the cost of keeping the integrity of the data and the costs associated with data retrieval.' Compare also the position of the European Association of Consumers and Electronic Manufacturers (EICTA) and of EACEM who consider that the obligation to conserve data imposes substantial financial costs on service providers and who oppose any compulsory conservation of traffic-related data except in the case of legal proceedings relating to specific infractions: 'Under a data preservation order, service providers store data related to a particular person, rather than store all users' data for potential future investigations. Because data preservation requirements are directed at a particular person or persons, they do not pose the same privacy concerns as general data retention.'

54 In this connection, see the speech by P Schaar at the meeting of experts on 6 November 2001 and that of D Smith at the hearing of 27 November 2001. Moreover, reference will be made to the 'opinions' expressed by the Group for the protection of data of Article 29, in particular, the last-mentioned (5074 final) adopted on 5 November 2001 concerning the Communication of the Commission: 'Creating a safer information Society by improving the security of information infrastructures and combating computer-related crime' (available on: http://europa.eu.int/commm/internal8market/en/dataprot/wpdocs/index.htm).

55 Compare in particular the hearing of the Norwegian police where attention was drawn to the following infringements: 'breaking into computer systems; theft of trade secrets; sabotage of critical IT systems; abuse of telephone systems; fraud; threats of life and death; blackmail; harassment and defamation …'.

56 Preamble No 11 notes: 'In line with directive 95/46/CE, the present directive does not deal with the questions of the protection of rights and fundamental liberties linked to activities which are not governed by community law. It does not therefore modify the existing balance between the rights of individuals to privacy and the possibility that the Member States have to take measures

such as those envisaged in Article 15, paragraph 1, of the present directive, that are necessary for the protection of public security, defence, the safety of the State (including the economic prosperity of the State when it is a question of activities linked to the safety of the State) and the application of criminal law. In consequence, the present directive does not affect the faculty of the Member States to legally intercept electronic communications or to employ other measures should this prove necessary to attain one of the above-mentioned goals, while respecting the European Convention on Human Rights and Fundamental Liberties, such as interpreted by the European Court on human rights in its rulings. These measures must be appropriate, strictly in proportion to the goal being pursued and necessary in a democratic society. They should also be subject to appropriate guarantees, in respect of the European convention for the safeguard of human rights and fundamental liberties'.

57 JOCE, C. 191, 29 July 1992 and M.B., 30 October 1993.

58 J Rideau and J F Renucci 'Dualité des protections juridictionnelle des droits fondamentaux: apport ou faiblesse dans la sauvegarde de ces droits?' *Justices*, No 6, 1997, p 95; F Picod 'The community judge and the European interpretation' in F Sudre (ed) *The Interpretation of the European Convention*, Brussels, Bruylant, 1998, p 289, which speaks of the 'phase of knowledge and exploitation' of the jurisprudence of Strasbourg by the CJCE. In this respect, the impressive list of rulings by the Court of Justice of the European Communities, cited by Renucci, *Droit européen des droits de l'Homme* 2nd edn, LGDG, 2001, p 339.

59 Law No 2001-1062 of 15 November 2001 relating to daily security, J.O. of 16 November 2001.

60 Article 15.3 expressly stipulates that: 'The group for the protection of individuals with respect to the treatment of data of a personal nature, instituted by Article 29 of the directive 95/46/CE, also fulfils the tasks envisaged in Article 30 of the said directive concerning the matters covered by the present directive, namely, the protection of rights and fundamental liberties as well as legitimate interests in the sector of electronic communications'. This explicit increase in the competence of group 29 is remarkable. It allows it notably, in conformity with Article 30.2 and 3 of directive 95/46 to make recommendations on the way the text should be interpreted and especially, if it finds divergences that are likely to affect the equivalence of the protection provided by the legislation or practices of the Member States, to inform the Commission which can then, in accordance with the mechanism foreseen in the text of directive 2002/58/CE, provide for a modification of the text of the directive.

61 Concerning this fundamental decree and its application regarding wiretapping by the State security services, read B Havelange and Y Poullet 'Sureté de l'Etat et protection des données: comment réconcilier l'irréconciliable?' in International Conference of 20 January 1999 organized by the Committee R, in 'Law of information and communication technologies' *Cahiers du Crid*, No 16, Brussels, Bruylant, 1999, p 235. On the notion of democracy stemming from this decree, see the article by F Ost 'Le concept de démocratie dans la jurisprudence de la Cour européenne des droits de l'Homme' *Journal des Procès*, No 124, 1998, p 13.

62 Recommendation adopted 3 May 1999 (Doc. 5005/99/final, WP 18, already cited). We remind the reader that this recommendation had been made in the context of the European reactions to the discovery of the Echelon network (compare above, No 15).

63 Sur cette jurisprudence, lire le remarquable article de (on that case law, read the noticeable article of) D Yernault 'Echelon' et l'Europe—La protection de la vie privée face à l'espionnage des télécommunications' *Journal des Tribunaux de Droit Européen* (*J.T.D.E.*), 2000, p 190.

64 In this respect, the *firm case law* of the Council of Europe, D Yernault 'From fiction to reality: the global electronic spying program; Echelon, and the international responsibility of the States with regard to the European Convention on Human Rights' *Belgian Review of International Law*, 2000, p 198. Recently concerning wiretapping, condemnation on the part of the UK, simple circulars from the Home Office clarifying the questions for wiretapping, the report of the Commission of 14 January 1998, Aff. *Govell* v. *The United Kingdom*, 6 62 and especially the Court ruling in the case *Khan* v. *The United Kingdom*, 12 May 2000, §27.

65 Concerning these first two conditions, we draw attention to the Malone ruling of 12 August 1984: 'The law must employ terms that are sufficiently clear to show everyone in a sufficient way and

under what conditions it authorizes the authorities to exercise such a secret infringement' and that of Leander of 26 March 1987: 'In a system applicable to all citizens, … the law must employ terms that are sufficiently clear to show them in an adequate way in what circumstances and under what conditions, it authorizes the authorities to interfere in this secret, and virtually dangerous way, in their private lives … . The law itself must define the extent of the power attributed to the competent authority with sufficient clarity—taking into account the legitimate goal being pursued—in order to provide the individual with adequate protection against arbitrary power'.

66 In this respect, note the ruling of the president of the Belgian Commission for the Protection of Privacy, Mr Thomas, during his hearing at the Justice Commission of the House when the proposed law on computer crime was being examined (Doc. Parl. Chambre, sess. 1999–2000, 50, 0213/004, p 32): 'We should not end up creating separate and supplementary data bases by imagining that they can always be useful'. This ban on exploratory and general surveillance is affirmed by the Klass ruling of the European Court on Human Rights already cited; it is also affirmed by the Committee on Human Rights of the United Nations, general observation, No 16.

67 On this condition, see the Huvig and Kruslin rulings of 24 April 24 1990 and the Valenzuela Contreras versus Spain ruling of 30 July 1998: the guarantees to figure in the law concern 'the definition of the categories of persons liable to be placed under wiretapping surveillance, the nature of the infractions, the fixing of a time limit for the duration of the surveillance; the conditions for making a synthesis of the transcripts of the conversations intercepted; the precautions to be taken to communicate the recordings to be checked by the judge and the defence; the circumstances under which the recordings can and must be erased'.

68 That is, the person connected with the person under surveillance and their localization in the case of contact by mobile phone.

69 Compare in this respect, the case of *Amann* v. *Switzerland* (16 February 2000) which questions the rules of criminal procedure adopted by Switzerland when they concern 'the third parties presumed to receive from or transmit information to the latter (the persons suspected or charged)', without regulating in detail the case of these interlocutors wiretapped 'by chance' as 'necessary participants' in a telephone conversation recorded by the authorities. 'In particular, the law does not state clearly the precautions to be taken with regard to them'.

70 Concerning these last two conditions, see the Buckley ruling of 25 September 1996 (§76) made by the European Court of Human Rights: 'According to the case law of the Court, even if Article 8 does not contain any procedural condition, the decision process that leads to measures of interference must be fair and show proper respect for the interests of the individual that are protected by Article 8'.

71 In the case *Rotaru* v. *Rumania* of 4 May 2000, the Court demands that as a last resort even in the case of administrative wiretapping, the last recourse should be the judiciary for 'it offers the best guarantees of independence, impartiality and regular procedure'.

72 It is a question of the requirement of which we are reminded by the Berlin Group (an international working group for the protection of data in the telecommunications sector) adopted during the meeting in Hong Kong on 15 April 1998, a recommendation on 'Public Accountability in relation to interception of private communications'.

73 In particular in the European networks of police and judiciary cooperation, like Europol and Infopol, and even, as the USA wanted, to the American defence authorities.

74 Compare above, No 18.

75 Compare above, No 19.

76 We remind the reader that the first proposition of the directive did not mention this finality, subsequently introduced at the request of the operators. The vague nature of this new finality for conserving data gives cause for concern even if it goes without saying that the principles of Article 6 of the so-called general directive for the protection of data apply and henceforth oblige the provider or operator of communications services to proceed to loyal treatment only for fixed and compatible finalities, only in respect of relevant data and in relation to those finalities and finally only for the strictly necessary period of time.

77 We can push this reasoning to the point of absurdity. Shall we draw from the fact that it seems that the accomplices of Bin Laden—insofar as he is guilty—made use of razor blades in their attack, the consequence that any individual buying such razor blades should have a file opened on them?

78 We should note in this connection the resolution adopted by the European Parliament on 4 May 2000 and the Communication of the European Commission of 30 November 2000 regarding the fight against forgery and pirating in the sole market that in fact encourages collaboration between the private sector and the police and judicial authorities in their fight for the protection of intellectual property. The proposal for a directive is expected on this point for October of this year.

79 Compare above, No 255 in fine.

80 It is a question of 'excluding, when drawing up the decree, the communication data that can be considered as indirect data of content or behaviour. Certain technical data can in fact provide knowledge of the content of the information transmitted (for example, the URL of the sites visited, the IP address of the server consulted or the heading of an e-mail), or on the behaviour of netsurfers (address of the addressee of an e-mail, for example). The Forum considers that this type of data must not be mentioned in the decree being drawn up. However, it considers that the IP address of the user certainly forms part of the data needed for establishing the communication and reveals nothing of the content of the information consulted or of the behaviour of the surfer'. (Forum of Internet rights, Recommendations to the authorities: conservation of data relating to an electronic communication, 18 December 2001, available at: http://www.foruminternet.org/recommandations/lire.phtml?id = 230).

81 Thus, the current debate in France regarding the interest shown by the Tax Administration in connection data. 'The Senate adopted, on 18 December, in the context of the proposed law of amended finance 2001, amendments giving access to customs officers and the investigating officers of the Commission for stock exchange dealings (COB) to the data conserved by access providers and telecommunications officers *under the Security Act provisions*. It profited from the occasion, however, by proposing a new amendment which extends this right of access to tax officers. By means of a new amendment, modifying Article L 32-3-1 of the Code for the Post and Telecommunications, it completes the operation by foreseeing that 'For the needs of *tracking down, sanctioning and identifying irregularities in accordance with the provisions of the customs code, the general tax code or the monetary and financial code*, the operators […] and service providers mentioned in Articles 43-7 and 43-8 of the law of 30 September 1986 […] must communicate [….] the data which they are asked for by the authorized agents in the customs and the services responsible for the recovery of taxes and dues […]'. The tax agents therefore obtain right of access to data conserved by the operators for invoicing purposes.

82 In this respect, read H Brulin and D Moreau 'Coopération policière internationale et autorités de contrôle: un mariage d'amour ou de raison?' in E Montero (ed) *Droit des technologies de l'information. Regards prospectifs*, Brussels, Bruylant, 1999, p 185.

83 Opinion of the Belgian Commission for the Protection of Privacy, already cited above, note 6.

84 Forum for Rights on Internet, Recommendations to the authorities; conservation of data relating to an electronic communication, 18.12.2001, available at: http://www.foruminternet.org/recommandations/lire.phtml?id = 230. No doubt it is also to be recommended that the conservation by the providers and operators as well as by the police is done with 'free software' allowing manipulations to be avoided that can take place without being detected by the controlling authorities.

85 Our conclusions take certain passages from the speech of the author during the hearing organized by the EC in Brussels on 27 November, a hearing relating to the fight against cyber crime. The speech was published at length under the title 'Sécurité ou Libertés? Ubiquité' *Revue de droit des technologies de l'information*, Brussels, Larcier, 2002, p 3.

86 Compare on this point, h. 252 above.

87 In this respect, see J Boyle 'Foucault in cyberspace: surveillance sovereignty and hard-wired censors' available at http://www.wel.american.edu/pub/faculty/boyle/fouc1.html. The author compares the police systems of electronic surveillance to a virtual 'Panopticon', which is much more effective than the real one proposed by J Bentham.

88 B Frappat 'La dictature de la transparence' *Etudes*, 58, 1999.