Utrecht Law Review published by igitur

Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11

Paul De Hert*

Post-September 11 changes in the public discourse and policy making on security

After the events of September 11 the US government immediately took steps to strengthen security through a range of ambitious intelligence-gathering programmes using mass surveillance systems, such as the Terrorism Information Awareness Network, which employs data search and recognition pattern technologies within joined-up databases to uncover terrorist and other threats to the infrastructure, and the Computer Assisted Passenger Pre-Screening System (CAPPS II). Most EU countries also responded to the events of September 11 by implementing a variety of operational and legislative measures aimed at raising their levels of security. Legislative measures were taken with a view to strengthening judicial mechanisms and (special) investigative powers in the Member States and harmonizing anti-terrorism policing procedures across Member States.[1] Needless to say, this evolution gained a new impetus after the March 11, 2004 terrorist attacks in Madrid.

It is important to note however that many of the intrusive security measures were already under discussion prior to September 11. Hence, the terrorist attacks should be regarded as a catalyst rather than as a trigger[2] in the still ongoing shift from a *reactive*

* P.J.A. De Hert, associate-Professor at Leiden University; Professor at the Free University of Brussels and Fellow to the research groups 'Securing the Rule of Law in a World of Multilevel Jurisdiction' and 'Trias Europa' at the Faculty of Law, Leiden, e-mail: p.j.a.dehert@law.leidenuniv.nl

[1] This description of post 9/11 is based on a report, in which the author participated, of the Institute for Prospective Technological Studies - Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*. *Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs* (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN, particularly pages 8-9 and 94-98. See also: <ftp://ftp.jrc.es/pub/EURdoc/eur20823en.pdf>. See also the contributions in Emmanuelle Bribosia & Anne Weyembergh (eds.), *Lutte contre le terrorisme et droits fondamentaux*, Brussels, Bruylant, 2002, 305p.

[2] Institute for Prospective Technological Studies - Joint Research Centre, *o.c.*, 95-96 : "September 11 both accelerated the rate of existing change processes and also created the opportunity for a changed security agenda: a) *it brought about a more supportive public mandate for security* - In addition to 'real time' information flow analysis and security hardening to increase protection against attack, public reaction also became more supportive of a range of pan-European 'policing' initiatives planned before September 11 in response to pre-existing concerns over threats to security, e.g. the Council of Europe's Cybercrime Convention was signed by EU and G8 countries; the European arrest warrant replaces in 2004 the current system of extradition; Eurojust, set up to assist the co-ordination, investigation and prosecution of serious cross-border crime and improve judicial co-operation; and the cross-border Joint Investigation Teams. The willingness to co-operate within the EU and with the US over terrorist finance (including regulation of professionals), extradition and intelligence sharing was facilitated by sympathetic EU reactions to

to a *pro-active* security and crime policy. September 11 indeed accelerated and deepened this process, notwithstanding the vehement and worldwide resistance of pro-privacy groups like Electronic Privacy Information Centre (EPIC), Privacy International (PI) and Statewatch. In short, the result has been a widening of the use of data mining and post-hoc behavioural pattern analysis systems, whereby the use of ICT-based systems facilitates data collection and sharing between multiple sources in support of intelligence gathering. In addition, the measures taken have also reinforced the powers of governments and law enforcement bodies to access individuals' personal data for purposes different from those for which the data were originally gathered, supplied and processed.[3] Of course, such forms of permanent and automated surveillance are also affecting the power economy of our societies for they shape and steer the behavior of individuals: under surveillance an individual will act differently than without, even if he/she does not act or intend to act illegitimately. This evolution seems to turn into hard reality what the American sociologist Gary Marx in 1988 already called the *maximum security society*.[4] This 'maximum security society' relies on a refined technological framework to influence and even 'programme' the daily lives of citizens.[5] Harsh investigation techniques are replaced by softer versions that can be applied without knowledge of the persons observed. Large databases are established and linked containing data on the people at large, suspect or not. The data is gathered not occasionally, but via routinized discovery systems.[6] Actions are taken on the basis of concrete information *and* profiles. Data collecting and surveillance methods are entrusted to various public and private actors. Recent studies confirm Marx's critical analysis of contemporary law enforcement and surveillance methods. Robert O'Harrow's *No Place to Hide* actually supplements some of Marx's theses, by emphasizing the more aggressive and dominant role of private data hunters in America's security policy today.[7] Also, older technologies, such as national ID cards,

---

'September 11'. b) *it increased intelligence gathering through ICTs* - The changing public discourse towards securitization has also increased the use of surveillance to gather intelligence to forewarn against attacks and continuous threats from traffickers in arms, drugs and people (many of the latter being economic migrants), plus the money laundering that is a routine component of all major crimes involving financial gain. Schemes that seek to generate trust through the application of advanced technologies are being introduced. Increased threat has been used to justify reliance upon ICT-based systems to facilitate data collection and sharing, authentication and identity."

[3] *Ibid.*, 9 : "In fact, normal access to many commercial and governmental services is now conditional upon the citizen's providing more comprehensive personal data than would have been the case previously. There can be little doubt therefore that the combined effect of the operational and legislative measures described has been to tip the security/privacy balance in favor of security interests. That they are principally based on the massive application of different technologies leads us to raise the question of how efficient and effective these technologies are in achieving their aims."

[4] Gary T. Marx., 'La société de sécurité maximale', *Déviance et société*, 1988, 147-166. For a discussion of this concept and similar concepts by Michel Foucault, Stanley Cohen and Gilles Deleuze: see Serge Gutwirth, *Privacy and the information age*, Lanham, Rowman & Littlefield Publ., 2002, 71-78 ("Controlling societies").

[5] "Dans la société de sécurité maximale, il n'y a pas de distinction entre public et privé: nous sommes sous observation permanente, tout est transcrit dans un dossier définitif, et beaucoup de ce que nous disons, faisons et même pensons est connu et enregistré par d'autres que nous ne connaissons pas, que nous le voulions ou non, et même que nous le sachions ou non. On peut grouper et analyser des informations receuillies de régions, d'organismes et d'époques chronologiques trés éloignés les uns des autres. Le contröle préventif est imprégné d'un systþme où les informateurs, les dossiers et la classification prédominent. En même temps qu'elle pénétre comme un laser, la surveillance absorbe comme une éponge. On regroupe et on entend à la société en général la surveillance intensive qui normalement ne s'applique qu' à l'investigation des suspects criminels, des cas d'espionnage ou des prisoniers" (Gary T. Marx., 'La société de sécurité maximale', *Déviance et société*, 1988, 150).

[6] G.T. Marx & N. Reichman, 'Routinizing the Discovery of Secrets', *American Behavioral Scientist*, 1984, 423-452.

[7] Robert O'Harrow jr., *No Place to Hide. Behind the Scenes of of our Emerging Surveillance Society*, Free Press, 2005, 368p. Compare with 'Your Identity, Open to All', *Wired*, consulted May 2005, http://www.wired.com/news/privacy/0,1848,67407,00.html: "A search for personal data on ZabaSearch.com - one of the most comprehensive personal-data search engines on the net - tends to elicit one of two reactions from first-timers: terror or curiosity. Which reaction often depends on whether you are searching for someone else's data, or your own. ZabaSearch queries return a

now under vote in the last Western countries that have refrained from introducing them, combined with newer technologies such as biometrics and facial recognition by CCTV software, allow for massive identification schemes.[8] The combination of these technological measures threatens people's ability to remain 'anonymous' and enable tracking people where they are, where they've been and where they are going. To believe O'Harrow this was exactly what admiral John Poindexter, father of the US Total Information Awareness project, had in mind, but the admiral's dream plan was subsequently modified (though not abandoned) because of public upheaval. The negative reactions were based on the feeling that this use of surveillance technology has implications for human rights in general, and privacy in particular, as its potential to exploit people or exert social control is unregulated.

European feelings concerning the superior legal protection

Some commentators argue that these 'American stories' do not apply to decision making in Europe. Apart from differences in temper and approaches towards violence, eloquently but controversially identified by Robert Kagan,[9] there are differences in constitutionalism that suggest superior legal and judicial protection in Europe. Authors such as Schulhofer, Poullet and Goemans and Dumortier argue convincingly that unchecked law enforcement powers will not pass the Convention test.[10] One of the arguments by some of these authors is the existence of a solid framework for privacy protection in Europe. The protection of individual privacy at the EU level is mainly governed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and Article 7 of the Charter of Fundamental Rights of the European Union. In parallel, data protection in the EU is governed by Directive 95/46/EC (24 October 1995) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2002/58/EC (12 July 2002) on privacy and electronic communications, by Article 8 of the Charter of Fundamental Rights of the European Union[11] and by the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. In the United States there is no express right to privacy guaranteed by the Constitution and no specific act exists that regulates the protection of personal data. Although in certain situations the US Supreme Court has interpreted the Constitution to protect the privacy of individuals, and several highly specific regulations have been introduced, there is still no general recognized right to

---

wealth of info sometimes dating back more than 10 years: residential addresses, phone numbers both listed and unlisted, birth year, even satellite photos of people's homes".

[8] P. De Hert, *Biometrics: legal issues and implications,* Background paper for the Institute of Prospective Technological Studies, DG JRC – Sevilla, European Commission, January 2005, 39p. via http://cybersecurity.jrc.es/pages/ProjectlibestudyBiometrics.htm

[9] R. Kagan, *Of Paradise and Power: America and Europe in the New World Order*, Alfred a Knopf Inc, February 2003. Dutch translation: Robert Kagan, *Balans van de Macht. De kloof tussen Amerika en Europa*, Bezige Bij, 2003.

[10] See the references to their work *below*. The arguments of Schulhofer based on the regulations with regard to emergency situations such as terrorism will be discussed below.

[11] "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority".

privacy. Some even hold that it is precisely this patchwork of court rulings and regulations that poses threats to privacy.[12]

The basic document of the European human rights framework is undeniably the European Convention for the Protection of Human Rights. Concluded in 1950 within the framework of the Council of Europe,[13] it was designed to protect individuals' fundamental rights and freedoms in a novel way. The Preamble to the Convention reflects the determination of its drafters "to take the first steps for the collective enforcement of certain of the rights stated in the Universal Declaration". The Council of Europe therefore instituted a judicial procedure allowing individuals to bring actions against governments, if they consider that they are the victims of a violation of the Convention. After the exhaustion of national remedies, individual complainants have direct access to an international court, the European Court of Human Rights in Strasbourg. Before discussing the status and the interpretative work of this Court, it is worthwhile to recall some of the basic features of the European Convention.[14]
Firstly, the Convention is not a Constitution but a Treaty. After ratification it does not automatically form part of the domestic legal orders of a Member State. Countries such as the United Kingdom have ratified the Convention, but the Convention does not form part of the law of the land. Although the Court has referred to the Convention as "a constitutional instrument of European public order (*ordre public*)",[15] it has accepted this treaty-like status of the Convention.[16] It has also held that domestic courts are not obliged, as far as the Convention is concerned, to apply the Convention *ex officio*, i.e. when the applicant himself has not relied on the Convention in order to substantiate its claims.[17]
Secondly, unlike the US courts, the Court is not a constitutional court empowered to check on the 'constitutionality' or 'human rights compatibility' of new legislation. The Court does not have the power to annul national measures, nor does it have the capacity to consider that it can order a State to change its legislation.[18] Also, individuals are not permitted to complain against a law *in abstracto* simply because they feel that it contravenes the Convention. In principle, an individual applicant must be able to show that a law has been applied to his detriment. In *Klass*[19] the Court lowered the strict

[12] For a defence of the American approach: Joseph I. Rosenbaum, 'Privacy on the Internet: Whose Information is it Anyway?'; *Jurimetrics*, 1998, Vol. 38, 565-573.
[13] On the Council: A. Tomkins, 'Civil Liberties in the Council of Europe: A Critical Survey' in: C. Gearty (ed.), *European Civil Liberties and the European Convention on Human Rights. A Comparative Study*, The Hague, Martinus Nijhoff Publishers, 1997, 2-4
[14] We rely on R.A. Lawson & H. Schermers, 'A Bird's-Eye View of the European Convention**Fout! Bladwijzer niet gedefinieerd.**' in R.A. Lawson & H. Schermers (eds.), *Leading Cases of the European Court of Human Rights*, Nijmegen, Ars Aequi Libri; Second Edition, 1999, x-xii.
[15] ECHR, *Loizidou v. Turkey*, judgment of 23 March 1995, § 75. See more in detail on this: R.A. Lawson & H. Schermers, *l.c.*, xi. *Note about our references to the judgments of the European Court of Human Rights*: in a first reference to such a judgment we will mention the name of the applicant and the respondent state, as well as the date of the judgment. With these data the judgments can easily be found at: http://www.dhcour.coe.fr/eng/. After the first reference that we will only use the name of the applicant (ex. *Malone*). For precise references and quotes we will refer to the relevant paragraphs of the judgments.
[16] See for a discussion of dualist systems and the position of the Court: R.A. Lawson & H. Schermers, 'Comment to ECHR, Lawless v. Ireland, judgment of 1 July 1961', in R.A. Lawson & H. Schermers (eds.), *Leading Cases of the European Court of Human Rights*, Nijmegen, Ars Aequi Libri; Second Edition, 1999, 13-14.
[17] ECHR, judgment of 15 November 1996, *Ahmet Sadik,* § 33.
[18] However, Member States often amend their legislation in response to a judgment, if only to prevent identical violations in the future. Similarly, national judiciaries are increasingly prepared to apply the Strasbourg case law (R.A. Lawson & H. Schermers, *l.c.*, xi).
[19] ECHR, *Klass v. Germany*, judgment of 6 September 1978, § 33.

victim requirement in the Convention allowing the applicant to pursue his complaint concerning new German legislation containing wire-tapping powers and other powers to put persons and communications under surveillance, but this important hurdle was erected again in later cases without proper reasoning.[20]

Finally, the machinery of protection established by the Convention is subsidiary to the national systems safeguarding human rights.[21] Whereas the law of the European Communities generally seeks to harmonize the legal practice in the Member States, the European Convention on Human Rights only prescribes minimum standards.[22] From the 1970s onwards the Court has elaborated and refined a theory of the necessity of leaving Member States a 'margin of appreciation' when applying the Convention, judging that Member States and their competent national courts are in a better position to judge the necessity of measures that infringe on Convention rights.[23] The role of the Court is (only) to supervise this process and to give the final ruling on whether national measures are reconcilable with the Convention.[24] Interesting for our topic is the relevant nature of this European supervision. Different standards of scrutiny exist. In some cases more freedom is left to the Member States, in others there is a stricter standard of scrutiny. Several factors, identified by the Court in successive cases, account for these differences.[25] A bit contrary to the idea that all human rights are equally necessary, the Court has identified factors such as the nature of the Convention right in issue, its importance for the individual and the nature of the activities concerned.[26] It has been rightly observed that state activities such as the fight against serious forms of criminality or terrorism, are usually not subjected to the most strict standards of scrutiny.[27] In this area states enjoy a margin of appreciation. It is for them to make the

[20] See on the victim requirement and on the burden this imposes on the applicant to prove beyond doubt that a concrete violation has occurred in his or her case P. De Hert & O. De Schutter, 'Straatsburg, videosurveillance en het vorderingsrecht van verenigingen', *Algemeen Juridisch Tijdschrift* (*A.J.T.*), 1998, 504-511 (annotation of ECRM, *Pierre Herbecq & Ligue des droits de l'homme v. Belgium*); I. Cameron, *National Security And The European Convention On Human Rights*, The Hague/London/Boston, Kluwer Law International, 2000, (479p.), 97-101

[21] See on the importance of value pluralism and the position of the ECHR: Y. Arai-Takahashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Antwerp, Intersentia, 2002, 300.

[22] R.A. Lawson & H. Schermers, *l.c.*, xi with ref. to ECHR, *Richard Handyside v. United Kingdom*, judgment of 7 December 1976, § 49 (the Convention leaves to each Contracting Party, in the first place, the task of securing the rights and liberties it enshrines) and to ECHR, *Vermeire v. Belgium*, judgment of 29 November 1991, § 26 (States have a freedom of choice when deciding on measures to comply with their obligations under the Convention).

[23] See on this theory, its origins and the 'better-position' argument: J. Schokkenbroeck, 'De margin of appreciation-doctrine in de jurisprudentie van het Europese Hof', in *Veertig jaar EVRM*, (*NJCM-special 1990*), 41-58; R. Macdonald, 'The margin of Appreciation', in R. Macdonald, F. Matscher & H. Petzold (eds.), *The European System for the Protection of Human Rights*, Dordrecht, Martinus Nijhoff Publishers, 1993, 83-124; J. Vande Lanotte & Y. Haeck e.a., *Het Europees verdrag tot bescherming van de rechten van de mens in hoofdlijnen*, Antwerp, Maklu, 1997, Deel 1, 187-188; E. Kastanas, *Unité et diversité: Notions autonomes et marge d'appréciation des Etats dans la jurisprudence de la Cour européenne des droits de l'homme*, Brussels, Bruylant, 1996, 480p.

[24] See e.g. ECHR, *Brannigan & McBride v. the United Kingdom*, judgment of 26 May 1993, § 43.

[25] 'The Court has pointed out in several judgments that the Contracting States enjoy a certain 'margin of appreciation' in assessing whether and to what extent differences in otherwise similar situations justify a different treatment in law (...). The scope of the margin of appreciation will vary according to the circumstances, the subject matter and its background; in this respect, one of the relevant factors may be the existence or non-existence of common ground between the laws of the Contracting States'; (ECHR, *Rasmussen v. Denmark*, judgment of 28 November 1984, §. 40).

[26] See in more detail: J.G.C. Schokkenbroek, *Toetsing aan de vrijheidsrechten van het Europees verdrag tot bescherming van de rechten van de mens*, Zwolle, W.E.J. Tjeenk Willink, 1996, (575p.), 206-208.

[27] "When the level of crime is perceived to threaten the *ordre public*, there may be pressure to take repressive measures at the expense of human rights. It appears from the case law that the Court is prepared to accept the legitimacy of the fight against crime and terrorism as well as to acknowledge the need to take effective measures, but obviously that does not mean that the authorities have *carte blanche*" (R.A. Lawson & H. Schermers, *l.c.*, xxi-xxii with ref. to ECHR, *Brogan and others v. the United Kingdom,* judgment of 29 November 1988, § 48; ECHR, *Kostovski v. the Netherlands*, judgment of 20 November 1989, § 44).

initial assessment as to whether a right balance is struck between the exercise by the individual of the rights guaranteed to him under the Convention and the necessity to protect the democratic society as a whole.

When considering these three basic features, one is inclined to wonder about the enthusiasm for and the moral authority of the European Court. In the following paragraphs we highlight some of the elements that have contributed to this success story, immediately followed by a more critical assessment of the strength of the European human rights framework.

The dynamic influence emanating from Article 8 of the Convention

Surveillance technologies in their contemporary sense (e.g. large scale applications of biometrics) were non-existent when French and American revolutionary spirits drafted the first Western constitutions at the end of the eighteenth century. These texts, and all the other texts that were inspired by them, simply did not envisage these techniques. Only rougher techniques such as torture were taken into consideration. Even in the European Convention there is no human right dealing explicitly with modern surveillance technology. There are however some human rights with a general scope that might be relevant for the issue. Of importance in the debate concerning contemporary strategies against terrorism is firstly Article 8 of the Convention stating that: "(1.) Everyone has the right to respect for his private and family life, his home and his correspondence. (2.) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".
The history of the case law with regard to Article 8 of the Convention is rich, complex and full of unexpected new developments that have contributed to a solid framework of privacy protection.[28] The first and foremost harmonizing influence emanating from Article 8 of the Convention is the requirement that any invasion of privacy for a legitimate reason (for purposes of criminal investigation, usually the prevention of crime) must have a basis in law, and that this law – be it case law or statute – must be of a certain quality: foreseeable (sufficiently detailed) and accessible and providing remedies for the citizen. While in continental "civil" legal systems and culture it is regarded as self evident that interference with the individual citizen by the state requires an explicit basis in law, common law systems take the opposite view: everything is allowed unless forbidden. Therefore, the full implementation of the Convention required of the United Kingdom a substantial cultural *volte face*,[29] at least as far as the rules governing police powers are concerned.[30]

[28] See P. De Hert, *Artikel 8 EVRM. De bescherming van privacy, gezin, woonst en communicatie*, Gent, Mys en Breesch Uitgeverij, 1998, 367p.
[29] The course of events from *Malone* to the Regulation of Investigatory Powers Act 2000 is a *locus classicus*. A violation was found of Article 8 ECHR in a case concerning interception and metering of telecommunication, on the grounds that a legal basis

The legality principle, meaning that interferences by the executive with the rights and freedoms of the individual should not be permitted unless there is a clear legal basis to do so and that individuals should be able to predict with reasonable certainty when and under what conditions such interferences may occur, is also expressly laid down in Articles 2, 5, 6, 7 and in the second paragraphs of Articles 9 to 11.

Article 8 of the Convention has also benefited from a wild interpretative method used by the Court. The result is commonly known as 'the dynamic character of the Strasbourg case law'. This 'remarkable aspect' of the European human rights practice,[31] is no less than a straightforward departure from the traditional international public law principle of strict interpretation of treaties. On numerous occasions the Court emphasized that the Convention is "a living instrument which should be interpreted according to present-day conditions".[32] In a similar vein the Court has repeatedly stressed that the Convention is intended to guarantee "not rights that are theoretical or illusory but practical and effective".[33]
This unconventional, but effective method of interpretation that opens the way for expanding the protection offered by the Convention, is of course very promising when considering new technological developments that challenge human rights in a way that could not be foreseen when drafting the Convention. The telephone tapping case law of the European Court is traditionally hailed as a powerful demonstration of the strength of the Convention. Although the Convention does not speak to us about modern means of communication, the Court has successively brought telephone conversations (*Klass*),[34] telephone numbers (*Malone*), voice recording (*P.G. & J.H.*)[35] under the scope of Article 8. This "dynamic" interpretation of the Convention is believed to bring e-mails under the scope in due time.[36]

These examples show the wide interpretation given to Article 8 of the Convention.[37] The Court has been somewhat hesitant, however, in applying Article 8 to several forms of data processing (written data, biometrical data, visual data) in databases. Of course, it is precisely these practices that are central to most post-9/11 strategies.

---

as required by Article 8 was absent in English law. The Interception of Communications Act 1985 was an attempt to remedy this. Cf. ECHR, *Malone v. United Kingdom*, judgment of 2 August 1984.

[30] P. Alldrigde & Ch. Brants, 'Introduction' in P. Alldrigde & Ch. Brants (eds.), *Personal Autonomy, the Private Sphere and the Criminal Law. A Comparative Study*, Oxford, Hart Publishing, 2001, 13.

[31] R.A. Lawson & H. Schermers, *l.c.*, x.

[32] See R.A. Lawson & H. Schermers, *l.c.*, x with ref. to ECHR, *Tyrer v. the United Kingdom*, judgment of 25 April 1978,§ 31, ECHR, *Marckx v. Belgium*, 13 June 1979, § 41, ECRM, *Jeffrey Dudgeon v. Ireland*, judgment of 22 October 1981, § 60, ECHR, *Soering v. the United Kingdom*, judgment of 7 July 1989, § 102, ECHR, *B. v. France*, judgment of 25 March 1992, §§ 45-48) and ECHR, *Salesi v. Italy,* judgment of 26 February 1993, § 19. This culminated in 1995 when the Court held that the Convention "cannot be interpreted solely in accordance with the intentions of their authors as expressed more than forty years ago [...] at a time when a minority of the present Contracting Parties adopted the Convention" (ECHR, *Loizidou v. Turkey*, judgment of 23 March 1995, § 71).

[33] See R.A. Lawson & H. Schermers, *l.c.*, x with ref. to ECHR, *Airey v. Ireland*, judgment of 9 October 1979, § 24 and ECHR, *Soering v. the United Kingdom*, judgment of 7 July 1989, § 87.

[34] ECHR, *Klass v. Germany*, judgment of 6 September 1978.

[35] ECHR *P.G. and J.H. v. the United Kingdom* (Application n. 44787/98), judgment of 25 September 2001.

[36] Cf. H.H. De Vries, 'Vertrouwelijkheid van e-mail in arbeidsverhoudingen', in H.W.K Kaspersen & C. Stuurman, *Juridische aspecten van e-mail*, Deventer: Kluwer, 2001, 116-117; L. Ascher & W. Steenbruggen, 'Het Emailgeheim op de werkplek. Over de toelaatbaarheid van inbreuken op het communicatiegeheim van de werknemer in het digitale tijdperk', *Nederlands juristenblad*, 2001-37, 1788.

[37] For a detailed analysis of the case law, see P. De Hert, Article 8 ECHR and the Law in Belgium. Protection of Privacy, House, Family and Correspondence, *o.c.*, 367p. and P. De Hert, 'Artikel 8 EVRM. Recht op privacy' in J. Vande Lanotte & Y. Haeck (eds.), *Handboek EVRM. Deel 2 Artikelsgewijze Commentaar*, Antwerp-Oxford, Intersentia, 2004, 705-788.

Although the Strasbourg institutions have recalled on several occasions that data protection is an issue which falls within the scope of Article 8,[38] they have also held that not all aspects of the processing of personal data are protected by the ECHR. The Court has held that the rights in Article 8 ECHR do not imply a general right to access to personal data.[39] Also, the Court makes a distinction between personal data that fall within the scope of Article 8 and personal data that do not fall within its scope. In the eyes of the Court there is processing of personal data that affects private life and processing of personal data that does not affect the private life of individuals.[40] By contrast, in data protection, a general right to access is explicitly recognized. Also, data protection does not distinguish different kinds of personal data on the basis of such a thing as "intrinsic privacy relevance". The central notion of data protection is "personal data", meaning any information relating to an identified or identifiable individual.[41] In recent cases such as *Amann, Rotaru and P.G. and J.H. v. the United Kingdom*,[42] the European Court seems to remedy this by applying a very broad privacy definition, an uncritical reference to the Leander case, a generous reference to an older data protection treaty and a very loose scrutiny of the requirements of the first paragraph of Article 8 ECHR.[43] However, these cases should be carefully

[38] For instance: ECommissionHR, *Lundvall v. Sweden*, 11 December 1985, case 10473/83, *D.R.*, vol. 45, 130.

[39] ECHR, *Gaskin v. the United Kingdom*, judgment of 7 July 1989, § 37. In the *Leander* case the Court stated that the refusal to give Leander access to his personal data falls within the scope of Article 8 ECHR ((ECHR, *Leander v. Sweden*, judgment of 26 March 1987, § 48). A claim for access therefore can be based upon Article 8. Cf. *Antony and Margaret McMichael v. the United Kingdom*, judgment of 24 February 1995, § 91. In the case of McMichael the right to access is again recognized. Cf. *Antony and Margaret McMichael*, § 9. But, just as in the Leander case, a general right of access to personal data is not granted. In this case the Court does not explicitly deny such a right, but it 'simply' does not mention the issue.

[40] A good example is the 1998 case *Pierre Herbecq and the Association Ligue des droits de l 'homme v Belgium*. Cf. ECommHR, *Pierre Herbecq and the Association Ligue des droits de l 'homme v Belgium*, Decision of 14 January 1998 on the applicability of the applications No. 32200/96 and 32201/96 (joined), Decisions and Reports, 1999, 92-98; *Algemeen Juridisch Tijdschrift*, 1997-1998, Vol. 4, 504-508. In these two joint Belgium cases the applicants complained about the absence of legislation on filming for surveillance purposes where the data obtained is not recorded in Belgium. The application was held inadmissible on the following grounds: "In order to delimit the scope of the protection afforded by Article 8 against interference by public authorities in other similar cases, the Commission has examined whether the use of photographic equipment which does not record the visual data thus obtained amounts to an intrusion into the individual's privacy (for instance, when this occurs in his home), whether the visual data relates to private matters or public incidents and whether it was envisaged for a limited use or was likely to be made available to the general public. In the present case, the Commission notes that the photographic systems of which the applicant complains are likely to be used in public places or in premises lawfully occupied by the users of such systems in order to monitor those premises for security purposes. Given that nothing is recorded, it is difficult to see how the visual data obtained could be made available to the general public or used for purposes other than to keep a watch on places. The Commission also notes that the data available to a person looking at monitors is identical to that which he or she could have obtained by being on the spot in person. Therefore, all that can be observed is essentially public behavior. The applicants have also failed to demonstrate plausibly that private actions occurring in public could have been monitored in any way. Applying the above criteria, the Commission has reached the conclusion that there is, in the present case, no appearance of an interference with the first applicant's private life. It follows that this part of the application is manifestly ill-founded within the meaning of Article 27, § 2 of the Convention".

[41] Data protection - although it recognizes the existence of a special category of sensitive data - is built up upon the idea that *all* kinds of personal data can be abused, including the more ordinary ones, such as names and addresses: the basic idea of data protection is to offer protection to all personal data (and stronger protection to some types of sensitive data). This idea is without doubt based on common sense since the extent to which ordinary data should be protected may be debatable, but the idea that they should be is not. As an example consider the following: while prohibiting the processing of sensitive data concerning, for instance, Jewish people, is a good thing, it would be unwise to ignore that a simple list of names (ordinary data) can also convey the information required to target this group and ought therefore to be protected as well. Often, technical people favour an Internet without law and especially without data protection law which is considered as too bureaucratic or formal. It is amusing to note that those most familiar with the possibilities of ICT themselves oppose the idea that it can make sense to protect data such as names or data regarding consumer behaviour (e.g. clients of a Kosher e-market).

[42] *P.G. and J.H. v. the United Kingdom*.

[43] For instance in *Amann v. Switzerland*, judgment of 16 February 2000, § 65-57: "The Court reiterates that the storing of data relating to the "private life" of an individual falls within the application of Article 8 § 1 (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, 22, § 48). It points out in this connection that the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; there appears, furthermore, to be no reason in principle why this understanding of the notion of "private life" should be

interpreted. A closer reading shows that the old distinction between "data that merits protection" and "data that does not" is still operating. Also, the reference to existing data protection treaties is formulated in a way that leaves room for discretion. Moreover, even when these cases show a willingness to protect aspects of "public privacy" and the day may come that the Court will grant Article 8 ECHR protection to all personal data, there remain other questions to be answered, such as, just to mention one, the question of whether a right to access and correction can be considered as an integral part of rights contained in Article 8 ECHR.

Some may argue that beneath the sloppy textual (and historical) analysis of the Court lay genuine concerns to which the Court is responding. We leave this open for debate, but think the present is a particularly ripe moment for a fundamental rethinking of past privacy case law. From the start the Court (and the now abolished Strasbourg Commission on human rights) hesitated between a narrow and a broad concept of "privacy" or "private life".[44] Especially after *Niemietz* there can no longer be any discussion about the existence and use of a broader concept.[45] But often the Court has chosen to proceed by indirection. Judgments based on a narrow privacy concept are distinguished away rather than overruled.[46] Tricky criteria to define privacy, such as the *reasonable expectation of privacy* (*supra*) are introduced without justification or principled support (*Halford*) and whittled down (*P.G. & J.H.*).[47]

The result is not satisfactory. The *reasonable expectation of privacy* criterion seems to invite a Byzantium play of arguments about 'what privacy really is' and 'what really constitutes an infringement of our civil liberties'.[48] Take the example of camera

---

taken to exclude activities of a professional or business nature (see the *Niemietz*, § 29 and *Halford v. the United Kingdom,* judgment of 25 June 1997, § 42).

That broad interpretation tallies with that of the Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, which came into force on 1 October 1985, whose purpose is "to secure in the territory of each Party for every individual … respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him" (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual" (Article 2). In the present case the Court notes that a card was filled in on the applicant on which it was stated that he was a "contact with the Russian embassy" and did "business of various kinds with the company [A.]" (see paragraphs 15 and 18 above). The Court finds that those details undeniably amounted to data relating to the applicant's "private life" and that, accordingly, Article 8 is applicable to this complaint also".

[44] See in detail: P. De Hert, *o.c.*, 67-81.

[45] See *Niemietz*, § 29. "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings".

[46] This is not a typically European phenomenon. Comp. A.R. Amar, *The Constitution and Criminal Procedure. First Principles*, New Haven and London, Yale U.P., 1997, 147-148.

[47] See P. De Hert, 'L'article 8 CEDH', Chapitre 3, Titre I in P. De Hert (ed.), *Manuel sur la vie privée et la protection des données*, Bruxelles, Ed. Politéia, feuillets mobiles, mise à jour No. 10 (2002), (72p.) 15-18 & 18sub1-18sub67; J. Goldman, 'Privacy and individual empowerment in the interactive age' in Y. Poullet, C. De Terwangne & P. Turner, *Privacy: new risk and opportunities*, Diegem, Story-Scientia, 1997, 70-71; T. Blom 'Privacy, EVRM en (straf)rechtshandhaving', in Ch. Brants, P. Mevis & T. Prakken (eds.), *Legitieme strafvordering. Rechten van de mens als inspiratie in de 21ste eeuw*, Antwerpen-Groningen: Intersentia Rechtswetenschappen 2001, 119-137.

[48] Cameron, who embraces rather uncritically the distinguishing criterion of the target's *expectation of privacy*, observes that the video or oral recording of a conversation or event in which the monitor participates is usually less serious an infringement of privacy than the same types of surveillance done by a non-participant. Equally, video surveillance of a person whispering to another in a public place is, arguably at least, less serious than oral surveillance of the same person because the target in the former situation knows that he or she can be observed, but does not know he or she can be heard (I. Cameron, *o.c.*, 85). But change these facts or add an element and a non-search or a non-privacy infringement becomes a search or an infringement. "Imagine, for example, a government policy allowing government officials, as a perk of power, to stand unobservable under bleachers and take snapshots of women's panties" (A.R. Amar, *o.c.*, 9). A search is a search, Amar observes, whether a police officer is just using his eyes when standing on the street or whether the same officer is targeting someone with binoculars. The difference between these two searches is that one may be much more reasonable than another (A.R. Amar, *o.c.*, 8-9). On the criterion of *reasonableness*, see below.

surveillance of the public space (CCTV). If Orwell's hallucinating novel *1984* triggers one powerful image, then it must be this of an unfree society where camera in the public space leave no room for a single bit of privacy. [49] Although CCTV has been around for almost two decades now, we had to wait until *Peck* (2003) before a rather straightforward constitutional check was arrived at.[50] Although the *Peck* judgment contains a solid check on reasonableness via principles such as proportionality and subsidiarity, the reader is forced to read through a long passage in which the Court is trying to make sense of earlier judgments, such as the above-cited *Herbecq* case, - judgments that are of a problematic nature, especially from a data protection perspective - ,[51] before arriving at the common sense observation that the events surrounding the filming "far exceeded any exposure to a passer-by or to security observation (as in the above-cited *Herbecq* case) and to a degree surpassing that which the applicant could possibly have foreseen when he walked in Brentwood on 20 August 1995".[52]

A rule of law approach v. a political approach towards Article 8 of the Convention

Article 8 has been an important yardstick for the Court to set out its conception of the concept of the 'rule of law', mentioned both in the Statute of the Council of Europe and in the Preamble to the Convention.[53] The 'rule of law' requires effective safeguards against arbitrary interferences by the authorities. Many cases in which the Court found that such safeguards were lacking involved Article 8.[54] It is interesting to note that the Court has developed this notion of the rule of law while assessing the legality requirement in Article 8, paragraph 2. In *Kruslin* and *Huvig* the Court held that the notion of "law" implies qualitative requirements, notably those of 'accessibility' and 'foreseeability', and comprises written as well as unwritten law.[55]
In literature there is much praise for the self-imposed task of qualitative control of legislation done by the Court. This is rightly so: poor laws that confer no meaning should be avoided in the sphere of human rights. However, insisting on the content of law, rather than on the formal basis of law, has brought the Court to a denial of the importance of a solid formal foundation for the law. The rejection of the requirement that (at least in Continental countries) privacy infringements should be based on a formal law, has allowed the Court to declare certain regulations "in accordance with the law" that have not even been debated and approved by a parliament.[56] It is

[49] G. Orwell, *Nineteen eighty-four*, London, Penguin, (1949) 1954.
[50] On *Peck* see below.
[51] See on these judgments: P. De Hert, *Privacy en het gebruik van visuele technieken door burger en politie. Belgische regelgeving vandaag en morgen*, Brussel, Politeia Uitgeverij, 1998, (178p.), 61-80.
[52] ECHR, *Peck v. United Kingdom,* judgment of 28 January 2003, § 62. Less evident is the subsequent *dictum* that "the disclosure by the Council of the relevant footage constituted a *serious* interference with the applicant's right to respect for his private life" (*Peck*, § 63).
[53] R.A. Lawson & H. Schermers, *l.c.*, x.
[54] See e.g., ECHR, *Kruslin v. France*, judgment of 24 April 1990, §§ 30-35, ECHRn *Niemietz v.* Germany, judgment of 16 December 1992, § 37 and ECHR, *Funke v.* France, judgment of 25 February 1993, § 56.
[55] ECHR, *Huvig v. France*, judgment of 24 April 1990, § 34 and ECHR, *Kruslin v. France*, judgment of 24 April 1990, § 35.
[56] See: P. Blontrock & P. De Hert, 'Telefoontap: Tournet, Peureur, Hüvig, Kruslin et les autres', *Rechtskundig Weekblad*, 1991-1992, 865-871; I. Cameron, *National Security And The European Convention On Human Rights*, The Hague/London/Boston,

noteworthy for our subject that the Court 'opened up' the legality requirement for unwritten law such as judge-made law (case law) in two cases that both concerned wire tapping. In both cases the Court explicitly referred to the phenomenon of perpetual technological change, as an argument to accept unwritten law as a legal ground for human rights limitations. [57] Because technology changes, the Court seems to suggest, judges will play an inevitable and important role in assessing their compatibility with the human rights framework. This position of the Court is not evident. In the sphere of human rights, one would expect a stricter position wherein decisions to implement new technologies that have an impact on the rights and liberties of the citizen are made by the legislator taking into consideration all relevant factors. One can hardly expect this assessment be properly done by judges. A formal approach towards the legality requirement ('no technology without law') would be more in line with constitutional wisdom. This approach, followed by other supranational human rights courts,[58] would strengthen the human rights framework in the area of criminal law considerably. Most countries lack a requirement of legality with regard to criminal law enforcement ('no investigation techniques that have no basis in formal law'). Even in countries that respect such a requirement, like the Netherlands, judges are known to give too much leeway to law enforcement authorities trying out new technologies.[59] Judges do not like to say 'no' to human-rights-infringing technologies that help combat crime but which lack a proper legal basis. One commentator of *Huvig* and *Kruslin* observed that tapping practices in France already existed in the nineteenth century, but were never properly 'framed' by national case law. Rather than there being case law clarifying an existing legal framework, the legal situation was built upon case law making up for the total lack of legislation.[60]

We have observed that the Court has gradually developed the view that a legal basis for privacy infringements should not only exist, but that it should also meet some qualitative requirements, namely accessibility and foreseeability.[61] Especially the latter requirement has allowed the Court to fuse the due process requirements of Article 6 ECHR and the effective remedy requirement of Article 13 into Article 8 ECHR concerning privacy. With regard to telephone tapping and other investigation

Kluwer Law International, 2000, (479p.), 34; R. Kouring-Joulin, 'De l'art de faire l'économie d'une loi (à propos de l'arrêt Kruslin et de ses suites)', *Receuil Dalloz Sirey.*, 1990, Chron. - XXXII.

[57] "(...) Settled case law of this kind cannot be disregarded. In relation to paragraph 2 of Article 8 (art. 8-2) of the Convention and other similar clauses, the Court has always understood the term "law" in its "substantive" sense, not its "formal" one; it has included both enactments of lower rank than statutes and unwritten law. (...) it would be wrong to exaggerate the distinction between common-law countries and Continental countries (...) Were it to overlook case law, the Court would undermine the legal system of the Continental States almost as much as the Sunday Times judgment of 26 April 1979 would have "struck at the very roots" of the United Kingdom's legal system if it had excluded the common law from the concept of "law" (Series A no. 30, p. 30, § 47). In a sphere covered by the written law, the "law" is the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments (ECHR, *Huvig v. France*, judgment of 24 April 1990, § 28)".

[58] See on the case law of the Inter-American Court: J.G.C. Schokkenbroek, *o.c.*,179.

[59] L. Keyser-Ringnalda. & K. Rozemond, 'Het hellend vlak argument in strafrechtelijke discussies', *Delikt & Delinkwent*, 1993, vol. 23, 621-649.

[60] R. Kouring-Joulin, 'De l'art de faire l'économie d'une loi (à propos de l'arrêt Kruslin et de ses suites)', *Receuil Dalloz Sirey.*, 1990, Chron. - XXXII.

[61] The expression "in accordance with the law" requires, firstly, that the impugned measure should have some basis in domestic law; secondly, it refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and that it is compatible with the rule of law. It also requires that the measure under examination comply with the requirements laid down by the domestic law providing for the interference. See e.g. *Kopp v. Switzerland*, judgment of 25 March 1998, § 55; *Perry v. the United Kingdom,* judgment of 17 July 2003, § 55.

techniques this has brought the Court to a very detailed set of conditions that have to be fulfilled by the legislatures and have to be respected by law enforcement authorities. These conditions oblige legislators to explicitly and precisely foresee which categories of persons can be the object of the measures, for which incriminations the measures can be taken, how long they can last, how reports/log books about the measures must be made up and, in case of later suspension of prosecution or acquittal, be destroyed. The Court is acting in these cases as a European legislator: any measure of telephone tapping in a Member State will be deemed legitimate if it meets the conditions.

In doing so, the Court remedies partly for it not being a constitutional court empowered to check on the 'constitutionality' or 'human rights compatibility' of legislation (*supra*). In *Huvig* the French government objected to an abstract assessment of its legislative policy. The Court responded that the legality requirement seen in the light of the principle of the rule of law entailed necessarily a review with a certain degree of abstraction.[62] It concluded that: "Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated".[63]
However, fusing into Article 8 the due process requirements of Article 6 ECHR and the effective remedy requirement of Article 13 is, so we believe, detrimental for both provisions, especially Article 13.[64] Elements of procedural rights are borrowed to construe a substantive norm, and the result is used to interpret the procedural rights. Although some rationale can be found to transform Article 8 into a procedural norm,[65] we feel that something odd is happening. Ian Cameron is obviously of the same opinion. He holds that these procedural requirements should not be seen as a feature of the legality requirement, but rather a requirement of Article 13 and/or a requirement of "necessity in a democratic society".[66] We prefer the first option. Article 8 is no place for procedural questions. The framers of the Convention have designed other articles for that purpose. The transformation of Article 8 into a source of procedural rights and conditions takes it away from the job it was designed for, viz. to prohibit unreasonable exercise of power.

---

[62] ECHR, *Huvig v. France*, judgment of 24 April 1990, §§ 30-31.
[63] ECHR, *Huvig v. France*, judgment of 24 April 1990, § 32.
[64] This article reads as follows: "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority ... ." The provision is not well-known, which is to nobody's surprise. Indeed, in *Klass* the Court introduced a heavily criticized restrictive or 'relative' approach. The Court considered that Article 13 has a subsidiary character to Article 8. Thus Article 13 could not be interpreted so as to nullify the efficacy of the measures of secret surveillance already found to be compatible with Article 8. The Court stated that "an effective remedy .... must mean a remedy which is as effective as can be having regard to the restrictive scope for recourse inherent in any system of secret surveillance"; *Klass v. Germany*, judgment of 6 September 1978, § 69). See the consequences of this approach for judicial checking on secret surveillance: I. Cameron, *o.c.*, 36-39.
[65] In *Silver and Others v. the United Kingdom* the Court made it clear that a law which "allows the exercise of unrestrained discretion in individual cases will not possess the essential characteristics of foreseeability and thus will not be a law for present purposes. The scope of the discretion must be indicated with reasonable certainty" (*Silver and Others v. the United Kingdom*, judgment of 25 March 1983, § 88-89). In cases such as *Klass, Huvig* and *Kruslin* the Court has also stated that adequate safeguards must also exist against abuse of the discretion established by law (*Klass*, § 63*, Huvig v. France*, judgment of 24 April 1990, § 34 and *Kruslin v. France*, judgment of 24 April 1990, § 35).
[66] I. Cameron, *o.c.*, 34.

Even if a restriction of privacy is foreseen by law and serves an objective listed under Article 8, paragraph 2 ECHR, this restriction must still be "necessary in a democratic society" and should not reach further than strictly necessary.[67] This condition inevitably implies an ultimate balancing of interests, a value judgment and/or a substantial choice, which cannot be found in an exegetic reading of the text or in a strict application of logical rules.[68] We think that such a balancing of interests that duly takes the weight of fundamental rights and freedoms into account is essential. In our opinion the Strasbourg judges are too hesitant and reluctant to do so and they clearly prefer the much more secure testing of the legality requirement (is there a law?).[69] This political function of human rights explains the importance of the requirement "necessary in a democratic society". Behind this requirement lies the true constitutional question with regard to law enforcement and privacy. What is "proportionate" will depend on the circumstances. According to Delmas-Marty, in determining proportionality the Court takes particularly into account the nature of the measure taken (its reach, whether it is general or absolute, its adverse consequences, the scope for abuse of the measure), whether the state concerned could have taken other measures or implemented them in a less drastic way, any status of the persons involved which legitimately renders their rights subject to greater limitation (e.g. prisoners) and finally, whether there are any safeguards which can compensate for the infringement of rights which a measure can create.[70]

Let us assume for a moment that the European Court sees to all those things when checking on the necessity requirement.[71] In that case the Court is doing what it should be doing. With Amar who speaks of the Fourth Amendment, but whose reasoning can be transposed, we believe that this is considering the central question of *reasonableness*.[72] The determination of reasonableness should be pragmatic, contingent and subject to easy revision.[73] What counts is the systematic application of the criteria: *all* searches and seizures and *all* infringements on the rights provided for by Article 8 by new modes of surveillance must be reasonable. Precisely because these searches and seizures and these infringements can occur in all shapes and sizes under a wide variety of circumstances, the criteria have to be pragmatic, contextual

[67] On this condition see K Rimanque, 'Noodzakelijkheid in een democratische samenleving -een begrenzing van beperkingen aan grondrechten', in *Liber Amicorum Frédéric Dumon,* Antwerpen, Kluwer Rechtswetenschappen, 1983, deel II, 1220.
[68] K Rimanque, *l.c.*, 1229.
[69] I. Cameron, *o.c.*, 35, P. De Hert, 'Strafrecht en privacy. Op zoek naar een tweede adem', *Rechtshulp. Maandblad voor de sociale praktijk*, 2003/10, 41-54. This is regrettable because there is a structural lack of information concerning the notion of the democratic state, which should be filled precisely by the legislature and the judges. Assertions such as "we must defend our democracy against terrorism" give the impression that democracy is a kind of substance existing in it. We never get to know what this substance is, but we are permanently invited and tempted to accept the proposition that we have to defend this democracy by all means, even undemocratic ones. However, democracy is no substance but a whole of practices and processes that we associate with the label "democratic". It consists of a permanent questioning of all the practices and processes which make a society democratic. The core of constitutional thinking is to participate in that questioning by focusing upon some values that we consider fundamental. See J. Blommaert, 'Veiligheid en democratie?', in Liga voor Mensenrechten (ed.), *Wordt de Europese ruimte van vrijheid, veiligheid en rechtvaardigheid een politiestaat?*, Gent, Liga voor Mensenrechten, 2003, (67-70), 67.
[70] M. Delmas-Marty, *The European Convention for the Protection of Human Rights,* Dordrecht, 1992, 71 quoted by I. Cameron, *o.c.*, 26. Concerning proportionality see also S. Van Drooghenbroeck, *La proportionnalité dans le droit de la convention européenne des droits de l'homme. Prendre l'idée simple au sérieux*, Bruxelles, Bruylant/Publications des FUSL, 2002, 790p.; W. Van Gerven, 'Principe de proportionnalité, abus de droit et droits fondamentaux', *Journal des Tribunaux*, 1992, 305-309.
[71] In fact we do not. Very often no more is performed than a very general and loose balancing exercise - where the individual's interests in enjoying a right are balanced against the interests of society as a whole in maintaining a restriction. See, amongst others on the principle of subsidiarity, below.
[72] A.R. Amar, *The Constitution and Criminal Procedure. First Principles*, New Haven and London, Yale U.P., 1997, 38-39. The US Fourth Amendment explicitly protects against "unreasonable" searches and seizures.
[73] A.R. Amar, *o.c.*, 39.

and subject to revision. Applying the reasonableness criterion avoids unworthy word-games about the nature of privacy and privacy infringements, discussed *above*.[74] Constitutional reasonableness encompasses substantive fairness and procedural regularity, and the two are often tightly intertwined, but in a sensible division of constitutional labour these issues are best respected for their own merits. Searches with a maximum of procedural guarantees might well be unreasonable in the light of Article 8, when they allow for an unwanted concentration of power. On the other hand it is well possible to conceive privacy infringements without procedural guarantees that are nevertheless reasonable, for instance the metal detectors at airports.[75] Elaborating codes of criminal procedure, for instance, with regard to telephone tapping, is not a command that follows from Article 8. We will come back to this after having discussed other provisions in the Convention that are relevant when assessing contemporary law enforcement measures and surveillance measures.

Physical liberty: a well protected European value?

Other relevant provisions are Article 3 prohibiting torture and inhuman or degrading treatment or punishment, Article 5 on detention and the right to liberty and Article 15 with regard to derogations in time of emergency. Article 3 seems particularly fit to deal with serious violations of human rights. Several cases concerning alleged violations of Article 3 have been brought before the Court. In *Aksoy* the Court recognized the serious problems of terrorism in South East Turkey and the difficulties faced by the Turkish state in taking effective measures against it.[76] It nevertheless found a violation of Article 3 in torturing a suspected terrorist and of Article 5 in holding a suspected terrorist in *incommunicado* detention without access to a judge or other judicial officer for fourteen days.[77] The Court held that even in the most difficult of circumstances, such as the fight against terrorism, the Convention prohibits in absolute terms torture or inhuman or degrading treatment or punishment.[78]

[74] We have the impression that some courts indulge in these games to avoid proper constitutional review. Both in European and American case law it appears that the judges are sensible to critcism concerning the right to privacy giving it less weight than other rights and interests. The fact that there is much debate concerning the definition of privacy (and the need to define it) is of course encouraging this development. The strength of the fundamental right - its flexibility which makes it possible to cope dynamically with new problems - turns out to be its weakness too. Because the notion of privacy is vague, it is possible and tempting to argue that there is no privacy. From that perspective it is, for example, easy to deny a privacy dimension to the use of control techniques in the professional sphere arguing that this sphere has nothing to do with the private sphere mentioned by Article 8 ECHR. That leads to case law which accepts that an employer is entitled to search the employees and to tap their telephones, without even inquiring into the violation of privacy. Examples of such judgments can be found in Belgium and the Netherlands, but also in the case law of the Strasbourg Court (*Lüdi*), with regard to police methods such as camera surveillance, observation and undercover. What happens here is that the application of the second paragraph of Article 8 is hindred, because the first paragraph is interpreted in such a way that the facts fall outside the scope of privacy (and thus: of the whole article). One may easily see the risk of avoiding the check on the second paragraph, by holding that an action complained of does not fall within the scope of the right in question or does not infringes this right. The American doctrine of the "expectation of privacy", which has been adopted by the European and Dutch judges, has been successfully used to this end. This doctrine considers privacy from a subjective point of view assuming that a person can only appeal to the privacy he can expect, and hence that offenders have no or lesser privacy because they know the police forces are trying to capture them. See P. De Hert & B.-J. Koops, 'Privacy is nog steeds een grondrecht', *Ars Aequi*, 2001, December, (vol. 50), 972-975. See also: A.R. Amar, *o.c.*, 8-9, 30 & 158.

[75] A.R. Amar, *o.c.*, 38-39.

[76] ECHR, *Aksoy v. Turkey*, judgment of 18 December 1996, § 84.

[77] ECHR, *Aksoy v. Turkey*, judgment of 18 December 1996, §§ 61- 65 and § 84.

[78] ECHR, *Aksoy v. Turkey*, judgment of 18 December 1996, § 62.

Furthermore, the Court introduced the obligation to carry out a thorough and effective investigation of incidents of torture.[79]
Article 5 secures to everyone the right to liberty and security of person. Its importance follows from its very detailed nature. The exceptions to the general right to liberty are many, but the wordings of the text are precise. Article 5, paragraph 2 protects the right to be informed of the reasons of arrest, whereas Article 5, paragraph 3 protects the right of everyone arrested or detained to be brought promptly before a judge, and the right to be released from pre-trial detention under certain conditions. Under Article 5, paragraph 4 everyone deprived of his liberty shall be entitled to challenge the lawfulness of his detention before a court (*habeas corpus*). Article 15 of the Convention allows the Contracting Parties to take measures derogating from their obligations under the Convention in time of public emergency. Derogation is not allowed for all the rights contained in the Convention and limits with regard to time and intensity are imposed on the exceptional measures that are allowed in the name of emergency.[80] Article 15 is the result of a delicate exercise to address the question of realizing justice in times of evil. It is based on the insight that special circumstances, such as war, terrorism and the existence of the mafia threaten our liberal democracies and justify more extreme state reactions, without giving room to unjust or excessive measures.[81]

The framework erected by Articles 3, 5 and 15 of the Convention and cases such as *Aksoy* and *Brogan*[82] partly explains optimistic messages in literature about the way a balance is sought and found within the framework of the European human rights Convention.[83] The framework does not allow for rhetoric about evil that demands that human liberties be put aside. Not all answers to terrorism are allowed, since some human rights in the Convention cannot be limited.[84] With regard to physical liberty Article 5 contains strict rights that stand in the way of uncontrolled and unlimited

[79] ECHR, *Aksoy v. Turkey*, judgment of 18 December 1996, § 61. See on these and other novelties introduced in *Aksoy*; R.A. Lawson & H. Schermers, 'Comment to ECHR, *Aksoy v. Turkey*, judgment of 18 December 1996',in R.A. Lawson & H. Schermers (eds.), *o.c.*, 665-670.
[80] Article 15 states that: "1. In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law. 2. No derogation from Article 2, except in respect of deaths resulting from lawful acts of war, or from Article 3, 4 (paragraph I) and 7 shall be made under this provision. 3. Any High Contracting Party availing itself of this right to derogation shall keep the Secretary-General of the Council of Europe fully informed of the measures which it has taken and the reasons therefore. It shall also inform the Secretary-General of the Council of Europe when such measures have ceased to operate and the provisions of the Convention are again being fully executed".
[81] See Stephen J. Schulhofer, 'Checks and Balances in Wartime: American, British and Israeli Experiences', *Michigan Law Review*, Vol. 102, 1906-1958.
[82] We observed that Article 5, paragraph 1 contains very precisely drafted exceptions with regard to deprivations of liberty. For instance, according to Article 5, paragraph 1 (c) of the Convention, an individual may be deprived of his liberty if a "lawful arrest or detention" is effected for "the purpose of bringing him before the competent legal authority" on "reasonable suspicion" of having committed an "offence". The applicants in the *Brogan* case, who were arrested under anti-terrorism legislation, argued inter allia that the authorities had never entertained a reasonable suspicion that they had committed an offence (ECHR, *Brogan and others v. the United Kingdom,* judgment of 29 November 1988 and of 30 May 1989, §§ 49-54). Moreover, they successfully argued that the *Prevention of Terrorism Act* (1984), allowing police detention without *habeas corpus* for seven days violated the Convention. The Court found that the police custody of four persons suspected of terrorism had violated Article 5, paragraph 3, as they had not been brought "promptly" before a judge (ECHR, *Brogan and others v. the United Kingdom,* judgment of 29 November 1988 and of 30 May 1989, §§ 55-62).
[83] Stephen J. Schulhofer, *l.c.*, 1906-1958. See esp. para. 4 on the case law of the European Court.
[84] Comp. with ECHR, *Tomasi v. France,* judgment of 27 August 1992, § 115 (Neither the necessities of criminal investigation, nor the difficulties that states encounter when combating terrorism, allow for limitations of the right to physical integrity contained in Article 3 of the Convention).

police arrest of suspected terrorists (*Brogan*).[85] When states rely on Article 15 in order to circumvent these rights - which is possible in principle - they are required to respect requirements of proportionality and time limitation and they are scrutinized by the Court.[86]

However, the combination of Articles 5 and 15 is not without drawbacks. There is a clear risk that states rely on Article 15 in order to prevent the Court from finding a violation of Article 5. *Aksoy* is one example where the Court has anticipated it, but there are other, less brutal cases where the combination has worked very well to the benefit of the state invoking the emergency clause.[87] After *Brannigan and McBride* more than one commentator has questioned the rather uncritical acceptance by the Court of the British arguments in favour of long police detentions without *habeus corpus*.[88] The principal argument advanced by the British has to do with the lack of 'hard' evidence that the police has when operating against suspected terrorists. Long detention without judicial review and with intensive police interrogations is needed to obtain more information and to shield the nature and the source of the police information from the defence, in view of protecting police informants and future use of police sources. A judicial procedure as required by Article 5, paragraph 3 would go against this.[89]

Without being able to measure to what extent these arguments have played a role in the Court's finding that there is no violation, we (again) find as a result a situation in which new law enforcement and surveillance techniques and the conditions that their application demands is made possible by the case law of the Court.[90] Presumably the biggest flaw in the Article 15 construction is its open character. There is no one-to-one obligation, e.g. in the case of terrorism, to fall back on this construction that demands certain procedural steps by the Member States open to scrutiny by the Court. On the contrary, Member States can choose to combat emergency type cases such as terrorism without falling back on Article 15. In these cases all the weight of the judicial human rights review will be on the analysis of the 'normal' requirements to limit human rights, such as the requirement of 'legality', 'legitimacy' and 'necessity' in Articles 8 to 11 of the Convention. The strictness of the Court's scrutiny of these

[85] A. Tanca, 'Human Rights, Terrorism and Police Custody', *EJIL*, 1991, No. 2, 269-277.

[86] In response to the *Brogan* judgment (*supra*) the UK Government decided to use its power under Article 15 of the Convention and derogate from its obligations under Article 5, paragraph 3. The legality of that derogation was subsequently reviewed when a similar complaint under Article 5 was lodged in the case of *Brannigan & McBride* (ECHR, judgment of 26 May 1993, §§ 39-74). Peter Brannigan and Patrick McBride were arrested in 1989 and detained for a period of five days. During this period, Brannigan was interrogated 43 times, McBride 22 times. In line with *Brogan*, the Court finds a clear violation of Article 5, paragraph 3, but accepts the use of the derogation offered by Article 15. In the case of *Aksoy*, the Turkish Government also sought to rely on Article 15 in order to prevent the Court from finding a violation of Article 5. The Court expressly reserved the right to examine whether the derogation met the requirements of Article 15, paragraph 3 (ECHR, *Aksoy v. Turkey*, judgment of 18 December 1996, § 86).

[87] R.A. Lawson & H. Schermers, *l.c.*, vi and vii. In the very first case that was decided by the Court, *Lawless*, the fact that Ireland had introduced emergency measures played a decisive role. Although the Court found that Article 5 §§ 1 (c) and 3 had not been complied with, the Irish derogation under Article 15 precluded the conclusion that the Convention had been breached (ECHR, *Lawless v. Ireland,* judgment of 1 July 1961, §§ 20-47). See also *Brannigan & McBride* discussed above.

[88] J-P. Loof, 'Brogan en de staatsnood van artikel 15 EVRM, of hoe het Europees Hof Noord-Ierland een noodtoestand bezorgde', *NJCM-Bulletin*, 1993, No. 7, 793-810; Ch. Ledure, 'Garanties minimales contre la détention arbitraire et pour le droit à un procès équitable en periode d'exception', *Revue Belge de Droit Intenational*, 1994, No. 2, 632-690.

[89] ECHR, *Brannigan & McBride v. the United Kingdom,* judgment of 26 May 1993, § 56.

[90] This finding had to be combined with our understanding of the Article 8 case law that entrusts the reception of these techniques to the judge, rather than the legislator (see above). See also our discussion of the Article 6 case law below.

requirements thus becomes very important. We will come back to this after a short discussion of Article 6.

Article 6 and new modes of surveillance

The right to a fair trial, guaranteed by Article 6 of the Convention, constitutes a basic element of a democratic society governed by the rule of law. In the Convention, the provision finds its natural place after Article 5 that governs the pre-trial detention. The recent convictions of Turkey in the famous case of Abdullac Öcalan are illustrative for the relevance of Article 6.[91]
As to the specific guarantees under Article 6, the second paragraph states that 'Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law'. This right is also included in Article 48 of the European Union Charter of Fundamental Rights.[92] Several guarantees are not mentioned expressly in Article 6 of the Convention. They have been developed in the Court's case law.[93] Of importance here is *Funke*,[94] where the Court accepted that Article 6, paragraph 1 includes a right to silence and the privilege against self-incrimination. Even though Article 6 of the ECHR does not mention the *nemo tenetur* principle the Court has decided that it is a part of the more general idea of a fair trial contained in the first subsection of Article 6. *Funke* is followed by *Saunders*.[95] In this case the Court held that there is a close connection between the right not to incriminate oneself and the ECHR presumption of innocence, stated in the second paragraph of Article 6. According to the Court the right not to incriminate oneself means that a suspect cannot be forced to supply evidence for his conviction and consequently the prosecuting authority has to collect evidence without the back up of items of evidence obtained by force or pressure.[96] Discussing Article 6 in the context of modern surveillance and law enforcement strategies is an intuitive choice in two regards.

[91] ECHR, *Öcalan v. Turkey*, judgment of 12 May 2005 *(Application no. 46221/99)*. In a first judgment on 12 March 2003 the Court had found several violations of the Convention. It *inter allia* held unanimously that there had been a violation of Article 5, paragraph 4 of the Convention on account of the lack of a remedy by which the applicant could have the lawfulness of his detention in police custody determined; unanimously that there had been a violation of Article 5, paragraph of the Convention on account of the failure to bring the applicant before a judge promptly after his arrest; unanimously that there had been a violation of Article 6, paragraph 1, taken together with Article 6, paragraph 3 (b) and (c) of the Convention; and by six votes to one that there had been a violation of Article 6, paragraph 1 of the Convention in that the applicant had not been tried by an independent and impartial tribunal. On 9 June 2003 the applicant and on 11 June 2003 the Government requested that the case be referred to the Grand Chamber, in accordance with Article 43 of the Convention. In the new judgment delivered by the Grand Chamber, most convictions based on Article 5 and 6 were upheld.
[92] Article 48.1 of the Treaty is almost exactly the same as Article 6(2) of the ECHR: "Everyone who has been charged shall be presumed innocent until proved guilty according to law" Full text of the Charter of Fundamental Rights of the European Union, *Official Journal* C 364/1, 18-12-200: http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf.
[93] See in more detail: R.A. Lawson & H. Schermers, *l.c.*, xxi-xxii.
[94] ECHR, *Funke v. France*, judgment of 25 February, § 44.
[95] ECHR, *Saunders v. the United Kingdom*, judgment of 17 December 1996, § 68.
[96] ECHR, *Saunders v. the United Kingdom*, judgment of 17 December 1996, § 68. "The Court recalls that, although not specifically mentioned in Article 6 of the Convention (art. 6), the right to silence and the right not to incriminate oneself are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6 (art. 6). Their rationale lies, inter alia, in the protection of the accused against improper compulsion by the authorities thereby contributing to the avoidance of miscarriages of justice and to the fulfilment of the aims of Article 6 (see the above-mentioned John Murray judgment, p. 49, para. 45, and the above-mentioned Funke judgment, p. 22, para. 44). The right not to incriminate oneself, in particular, presupposes that the prosecution in a criminal case seek to prove their case against the accused without resort to evidence obtained through methods of coercion or oppression in defiance of the will of the accused. In this sense the right is closely linked to the presumption of innocence contained in Article 6 para. 2 of the Convention".

Firstly, one could question whether collecting data on the population at large (and not only on suspected persons) is reconcilable with the notion of the presumption of innocence and fairness.[97] Intuitively, one would assume that the notion commands that only suspected persons are the object of state surveillance. However, the text of Article 6, paragraph 2 only envisages procedures of criminal law. It is only within such (formal) procedures that persons are presumed innocent, even when they are considered to be suspects. The presumption only protects persons who are labelled 'suspects' in order to bring them before a criminal court,[98] it does not protect other persons (e.g. who are not suspect or 'suspects' who are not brought before a criminal court). Hence, the presumption is not operative outside the context of the traditional criminal procedure. Consider the example of biometric technologies used for security purposes. True as it is that the Court has condemned the use of broad terms in warrants and the lack of any special procedural safeguards in *Niemietz*,[99] the use of biometrics in large scale applications, such as border and airports checks, does not fit in a traditional scenario of criminal investigation.[100] A broad, preventive application of biometrics will not, so we believe, be subjected to the *Niemietz* test. Note also that already with the 1990 Schengen Information System, requests for surveillance made by police and by national secret intelligence agencies, were made possible linking police interventions to a mere suspicion of danger. Seemingly Europe does not have too many problems with the lowering of the probable cause standard that is often imposed on traditional police work.[101]

Secondly, since many of these contemporary strategies imply some sort of cooperation of the subject (showing a passport, giving data, enrolling in biometrical schemes ...), a discussion of *nemo tenetur* is not without logic. We saw that according to the Court the right not to incriminate oneself means that a suspect cannot be forced to supply evidence for his conviction and consequently the prosecuting authority has to collect evidence without the back up of items of evidence obtained by force or pressure. Can this be read as a prohibition of practices forcing someone to hand over biometrical

---

[97] Comp. with D.H. Kaye, Michael E. Smith & Edward J. Imwinkelried, 'Is a DNA Identification Database in Your Future?', *Criminal Justice*, (Journal of the American Bar Association Section of Criminal Justice), Fall 2001, No. 19, 5-9; D.H. Kaye, Michael E. Smith & Edward J. Imwinkelried, 'The Constitutionality of DNA Sampling on Arrest', *Cornell Journal of Law and Public Policy*, Vol. 10, No. 3, Summer 2001, 455-509 via http://homepages.law.asu.edu/~kayed/cv/cv_pubs.htm

[98] Only those "charged with a criminal offence shall be presumed innocent until proved guilty according to law".

[99] In this case the European Court found a search and seizure in a lawyer's office to be a violation of the proportionality requirement that lurks behind the wordings of "necessary in a democratic society". After having found that the facts having triggered the investigation (pressure on a judge) were not of a minor nature, the Court noted the broad terms of the warrant and the lack of any special procedural safeguards, such as the presence of an independent observer in German law. Moreover the search impinged on professional secrecy to an extent that appears disproportionate in the circumstances. The Court then added the following: "it has, in this connection, to be recalled that, where a lawyer is involved, an encroachment on professional secrecy may have repercussions on the proper administration of justice and hence on the rights guaranteed by Article 6 (art. 6) of the Convention" (ECHR, *Niemietz*, *l.c.*, § 37)

[100] See our discussion of permanent and automated surveillance and the break with the logic of the traditional criminal investigation, above.

[101] The European Convention does not explicitly require that all surveillance and police powers be based on probable clause. It is uncertain whether the *Niemietz* dictum can be interpreted as such a requirement and, if yes, whether this is true for all kinds of surveillance. Comparative analysis shows that the requirement is not solidly anchored in the respective legal systems of the European Member States. See: J. Pradel, 'Criminal Evidence', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *Harmonisation in Forensic Expertise. An Inquiry into the Desirability of and Opportunities for International Standards*, Amsterdam, Thela Thesis, 2000, (411-429), 422. Critical about the idea that the requirement to act on probable cause follows from the US Constitution is A.R. Amar, *The Constitution and Criminal Procedure. First Principles*, New Haven and London, Yale U.P., 1997, 34. Even when one assumes that the requirement of probable cause follows from constitutional law, it can still be argued that database research meets this requirement, because matching can be equated with starting up an investigation or hearing witnesses. See on this position A.P.A. Broeders, *Op zoek naar de bron. Over de grondslagen van de criminialistiek en de waardering van het forensisch bewijs,* Deventer, Kluwer, 2003, (565p., with English summary) 214-215

traces or using biometrical traces against his will? *Funke* did not to seem to exclude this reasoning and there are precedents for this broad interpretation in the case law of some Member States. However, the US Supreme Court rejected the broad interpretation and limited the *nemo tenetur* principle to the forced issuing of proof with a 'testimonial or communicative nature'.[102] Apparently this case has served as guidance for the European Court which in the 1996 *Saunders* judgment opted for a limited interpretation: "The right not to incriminate oneself is primarily concerned, however, with respecting the will of an accused person to remain silent. As commonly understood in the legal systems of the Contracting Parties to the Convention and elsewhere, it does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, *inter allia*, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing".[103]
This case law reduces the *nemo tenetur* principle to two very narrow concerns, viz. to protect the accused against torture *and* to protect the judicial machinery from false statements made by the defence. In this narrow understanding, no other concerns are protected by the said principle.[104]

A human rights framework for the maximum security society?
Apparently the soft nature of contemporary surveillance and law enforcement strategies ('it does not hurt when enrolling in a biometrical scheme') accounts for the trouble of finding constitutional anchors to discuss it. Such a framework may not be a priority for the John Poindexters of this world, but is nevertheless desired by those that see the *maximum security society* as a threat to liberty interests. These concerns are genuine. Policymakers and civil society understand that national authorities, when confronted with serious forms of crime or terrorism, may face a dilemma. On the one hand they are responsible for the protection of society and its citizens; on the other hand they must respect human rights, including the rights of suspects. When the level of crime is perceived to threaten the *ordre public*, there may be pressure to take repressive measures at the expense of human rights.[105] The appeal to human rights is made to counterbalance this tendency and to seek what we have called constitutional reasonableness. Requirements such as the requisite in Article 8, paragraph 2 of the Convention that a law restricting privacy must be 'necessary in a democratic society' support demands for decisions that are well informed and based on careful consideration. Many recent post-9/11 developments in and outside Europe seemingly go against these requirements.[106] It suffices simly to take a close look at the arguments

[102] Supreme Court, *Solomon Fisher v. United States*, 425 US 391. B. Swart, 'The Case law of the European Court of Human Rights in 1993', *E.J.C.C.L.C.*, 1994, No. 2, 187.
[103] ECHR, *Saunders v. the United Kingdom*, judgment of 17 December 1996, § 69.
[104] "Often, investigators will be able to eliminate false leads with little effort and little burden on the DNA-based suspects. Moreover, the total number of people subjected to investigation, whether intrusive or not, frequently will be less with the population-wide database because many individuals who might have been suspects under traditional methods of investigation will have been excluded by the initial database search" (D.H. Kaye, Michael E. Smith & Edward J. Imwinkelried, *l.c.*, 6).
[105] R.A. Lawson & H. Schermers, *l.c.*, xxi-xxii.
[106] Comp. Caroline Goemans & Jos Dumortier, 'Mandatory retention of Traffic Data in the EU: Possible Impact on Privacy and On-Line Anonymity', in C. Nicoll, J.E.J. Prins & M.J.M. Van Dellen (eds.), *Digital Anonymity and the Law. Tensions and Dimensions*, Volume 2 Information Technology & Law Series (IT&Law Series), The Hague, TMC Asser Press, 2003, 161-183.

raised by civil liberty groups against the so-called CAPPS II initiative, which was initiated with the aim of air passenger profiling, combining the latest technological tools with pro-active intentions.[107] One of the arguments is that powers will not be used for their original purposes.[108] Another argument has to do with the lack of judicial remedies.[109] Due to a lack of oversight and reporting requirements citizen will be unable to control the use of the initiative.[110] It would be an interesting exercise to consider the legitimacy of the CAPPS II initiative, once accountability is provided for. Arguments concerning possible errors[111] and negligence of police officers,[112] suggest that the key concern is with power. The question of whether a privacy-infringing initiative is capable of being controlled replaces the question of whether an initiative infringes privacy. The question of constitutional reasonableness is a legitimate and political question,[113] but can the European human rights framework be used to demand accountability with regard to this question?

There is no empirical data concerning the current performance of the existing surveillance systems and there are no precise data as to why new surveillance systems and facilities are needed. Moreover, all the decisions seem to have been taken already, while a general and coherent debate in the European Parliament and the national Parliaments has not even taken place. See, amongst others, Privacy International, Statewatch and EDRI, *An Open Letter to the European Parliament on Biometric Registration of All EU Citizens and Residents*, November 30, 2004, 14p via http://www.edri.org/campaigns/biometrics/0411 or www.privacyinternational.org. See also: 'EU governments blackmail European Parliament into quick adoption of its report on biometric passports' 27 November 2004, via http://www.statewatch.org/news/2004/nov/12biometric-passports-blackmail.htm

[107] See e.g. D.L. Sobel, 'The status of the Computer Assisted Passenger Pre-Screening System (CAPPS II)', Statement of the General Counsel of EPIC before the House Committee on Transportation and Infrastructure Aviation Subcommittee on 17 March 2004, 15p. <http://www.epic.org/privacy/airtravel/capps_testimony_3_04.pdf>

[108] "Terrorists, however, have been known to go to great lengths to look like most people. Former Transportation Security Agency chief John Magaw refused to endorse a "trusted traveler" card, fearing that it would be the first thing a terrorist would try to obtain. New profiling and identification programmes will convert airport security into all-purpose police stops where criminals, deadbeat dads, and others seeking to avoid law enforcement for non-aviation-security-related reasons face the risk of being arrested" ('Air Travel Privacy', the introduction to EPIC's page with aviation security and privacy-related documents, <http://www.epic.org/privacy/airtravel/>).

[109] "The TSA system would be exempt from federal privacy protections that grant individuals access to government records to enable them to correct potential errors. Travelers would therefore not be informed when the database is used to deny them of any benefit or right. This would prevent passengers from learning what is compiled on them, how their threat level was determined, how information has been used against them, or even, whether they have been labeled a threat"; C. Laurant, 'Statement' Committee on Citizens' Freedoms and Rights, Justice and Home Affairs Public Seminar: *Data Protection since 11 September 2001: What Strategy for Europe?*, European Parliament – March 25, 2003, 3.

[110] "Without a transparency requirement on the US government's shoulders, the system could easily be abused and lead to capricious, unfair, or politically biased decisions on who to stamp as suspect" (C. Laurant, *l.c.*, 3).

[111] "Barring data subjects from accessing and correcting their records is very likely to generate many inaccuracies and errors, make the system less secure, and prevent the system from learning from its own mistakes when making risk assessments" (C. Laurant, *l.c.*, 7).

[112] "(P)assengers' data used by the CAPPS II system could later be used for different purposes not originally considered. The example of no-fly lists that the FBI circulated after September 11 shows the tendency that the government has to apply existing schemes to new purposes. In the FBI's "Project Lookout" the US law enforcement agency gave private companies a list of hundreds of names of persons the agency wanted to talk to. The list was widely circulated and quickly became riddled with inaccurate information as it was transferred from company to company. The list, once established for a legitimate purpose—the combat against terrorism—was used later for denying jobs to, or arbitrarily discriminating against, innocent people" (C. Laurant, *l.c.*, 3).

[113] The question is legitimate because proponents of the European human rights framework and civil society in general know that the longer a technology is used, the more entrenched in life it becomes. They feel that the current (legal) system gives too much leeway to new technological developments that are incepted without proper interrogation from and altering to a human rights perspective. They also feel the American pressure and know about America's mass installation of security technologies (metal detectors, scanners, CCTV's, iris recognition systems, alarms, locks, intercoms, and other forms of surveillance, detection, access control and biometric equipment) in schools, government premises, stores, offices, workplaces, recreation areas, streets and homes; and other public places, without understanding all the purposes behind this security build-up. Common sense pushed people to adopt a critical attitude (that regrettably is hardly echoed in the current legal framework), refusing to accept simple answers about safety and protection when there is little evidence that security technology actually makes us safer. They have heard about the paradox of technology, viz. that technology that is said to do good also produces unintended negative consequences and does not live to the promises of those that develop and seal it. They realize that police forces often use new technological security tools on poor and non-white people, and fear social outrage about discriminating practices. See Ronnie Casella, 'The False Allure of Security Technologies', *Social Justice*, 2003, Vol. 30, No. 2, 82-93.

Our skepticism can be best understood when looking at the recent case of *Lorsé*.[114] Lorsé, placed under a special detention regime (*EBI*)[115] complained *inter allia* about the following practices: his cells were weekly subjected to a more thorough search; at the same time or immediately afterwards he was frisked and strip-searched;[116] frisking and strip-searching also took place on arrival in and release from the special detention regime, before and after "open" visits and after visits to the clinic, the dentist's surgery or the hairdresser's.[117] He challenged these practices under Article 3 of the Convention prohibiting torture and inhuman or degrading treatment or punishment. Lorsé also made reference to the right to have privacy *and* family life respected, enshrined in Article 8 of the Convention. He argued that the large number of security measures in force, in particular the systematic strip-searching but also the monitoring of Mr Lorsé's telephone conversations and correspondence as well as the daily inspection of his cell, left Mr Lorsé not the tiniest space for a private life.[118] The reaction of the Court illustrates nicely our point about a solid human rights framework for harsh measures and an uncertain one for soft measures of surveillance. Everybody will agree that the strip search, including an anal inspection, qualifies as the former. And so did the Court. Although it had previously found that strip searches were necessary on occasions to ensure prison security or to prevent disorder or crime,[119] it concluded this time that the combination of routine strip-searching with the other stringent security measures amounted to inhuman or degrading treatment in violation of Article 3 of the Convention.[120]

A different outcome was reached with regard to the 'softer' surveillance techniques applied on Lorsé. After application of the criteria of Article 8, paragraph 2 the Court found no violation for the routine wire tapping and the other privacy-infringing surveillance measures. The restrictions complained of were based on a legal basis (the legality requirement). Moreover, it also accepted that they pursued the legitimate aim of the prevention of disorder or crime within the meaning of Article 8, paragraph 2 of

[114] ECHR, *Lorsé and others v. the Netherlands*, judgment of 4 February 2003 (Application no. 52750/99).

[115] '*Extra Beveiligde Inrichting'* or Extra Security Institution.

[116] The strip search, which involved an external viewing of the body's orifices and crevices, including an anal inspection, was carried out in a closed room and, whenever possible, by a person of the detainee's own gender. The EBI governor, or in urgent cases an EBI officer or employee, could decide that the detainee must be subjected to an internal body search if this was considered necessary to prevent the maintenance of good order or safety within the prison, or to protect the detainee's own health. An internal body search is usually carried out by a doctor, but he may also instruct a nurse to carry out the search.

[117] The main applicant alleged that the detention regime to which he was subjected in a maximum security prison constituted inhuman and/or degrading treatment in the sense of Article 3 of the Convention and infringed their right to respect for their private and family life (Article 8), and that they did not have an effective remedy in respect of their complaint of inhuman treatment (Article 13).

[118] They further complained of the conditions under which visits from the other applicants to Mr Lorsé had had to take place: behind a glass partition with no possibility of physical contact save for a handshake once a month. Bearing in mind that all communications between Mr Lorsé and his wife and children were monitored, the applicants contended that Mr Lorsé's detention in the EBI constituted an unjustified interference with the rights of his wife and children to respect for their private and family life as well.

[119] See ECHR, *Valašinas v. Lithuania*, no. 44558/98, § 117; *Iwańczuk v. Poland*, no. 25196/94, § 59, 15 November 2001, unreported; *McFeeley et al. v. the United Kingdom* (application no. 8317/78, Commission decision of 15 May 1980, *DR* 20, 44, § 60-61). In the cases of *Valašinas* and *Iwańczuk* one occasion of strip search was at issue, whereas the case of *McFeeley et al.* concerned so-called "close body" searches, including anal inspections, which were carried out at intervals of seven to ten days, before and after visits and before prisoners were transferred to a new wing of the Maze Prison in Northern Ireland, where dangerous objects had in the past been found concealed in the recta of protesting prisoners.

[120] ECHR, *Lorsé and others v. the Netherlands*, *l.c.*, § 73-74. The Court considered that in the situation where Mr Lorsé was already subjected to a great number of control measures, and in the absence of convincing security needs - bearing in mind that at no time during Mr Lorsé's stay in the EBI did it appear that anything untoward was found in the course of a strip search - the practice of systematic (weekly) strip searches that was applied to Mr Lorsé for a period of more than six years diminished his human dignity and must have given rise to feelings of anguish and inferiority capable of humiliating and debasing him.

the Convention (the requirement of legitimacy).[121] Also, in the circumstances of the present case the Court found that the restrictions of the applicants' right to respect for their private and family life did not go beyond what was necessary in a democratic society to attain the legitimate aims intended (the necessity requirement). Crucial in this respect was the government argument that Lorsé was placed in a special detention regime because the authorities thought it likely that he might attempt to escape.[122] The Court held that is was not its role to assess the accuracy of this contention and therefore it accepted that the authorities were entitled to consider that an escape by Mr Lorsé would have posed a serious risk to society.[123]

A benevolent human rights reception of contemporary modes of surveillance

At first sight *Lorsé* fuels the argument of those who hold that human rights law is a relevant test for the application of new identification *and* control technologies. Systematic searches and all-encompassing measures of control, leaving not the tiniest space for a private life, are subjected to a constitutional reasonableness test taking into account all constitutional relevant factors. However, a closer looks reveals that there are in reality two tests. A test of strict scrutiny with regard to the harsher technologies and a more flexible test, made possible through the use of the 'margin of appreciation', for the softer technologies that are assessed within the framework of Article 8.

Lorsé and its benevolent treatment of softer techniques is by no regards unique. The Strasbourg institutions seem to find more and more difficulty in recognizing the fundamental nature of privacy and the plain fact that it does not require blood (but technology) to violate it.[124] In the past the (now abolished) European Commission of Human Rights showed very little concern for the way police obtained fingerprints and photographs of suspects and the subsequent use of this data.[125] The record of the Court is not better. In *Murray* the Court disregarded questions concerning the legality of police powers to take pictures from apprehended persons and the proportionality of collecting background data.[126] Confidence in law enforcement combined with perceived users acceptance seemingly makes the Court unfit to apply its criteria and usual standards whenever softer techniques are used. In our work on the case law of the Court with regard to evidence and the exclusion of illegally obtained evidence, we have found that whenever the Court is ready to recognize that a certain problem is a problem falling within the scope of Article 8, paragraph 1 of the Convention, it is

[121] ECHR, *Lorsé and others v. the Netherlands*, *l.c.*, § 84.
[122] ECHR, *Lorsé and others v. the Netherlands*, *l.c.*, § 85 *juncto* 86.
[123] ECHR, *Lorsé and others v. the Netherlands*, *l.c.*, § 85.
[124] P. De Hert & B.-J. Koops, *l.c.*, 972-975
[125] See for a detailed analysis of Commission cases such as *Friedl v. Austria* (1995), *Doorson v. the Netherlands* (1996) and *Herbecq v. Belgium* (1998): Paul De Hert, *Privacy en het gebruik van visuele technieken door burger en politie. Belgische regelgeving vandaag en morgen,* Brussels, Politeia Uitgeverij, 1998, (178p.), 61-80. See also: P. De Hert & S. Gutwirth 'Making sense of privacy and data protection. A prospective overview in the light of the future of identity, location based services and the virtual residence' in Institute for Prospective Technological Studies - Joint Research Centre, *Security and Privacy for the Citizen in the Post-September 11 Digital Age. A prospective overview*, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), July 2003, IPTS-Technical Report Series, EUR 20823 EN, (111-162), 122.
[126] ECHR, *Murray v. the United Kingdom*, judgment of 28 October 1994, *Series A*, No. 300-8.

often brought to weaken its application of the criteria contained in Article 8, paragraph 2.[127] Cases such as *Khan* and *P.G. and J.H. v. the United Kingdom* are one step further in this evolution.[128] In both cases the Court found privacy-infringing practices that disrespect the criteria in Article 8, paragraph 2. However, convictions by national judges of criminals were nevertheless accepted by the European Court within the framework of the right to a fair trial laid down in Article 6 of the Convention.

Would *Lorsé* have had a different outcome if Lorsé would have been subjected to body scans instead of more physical anal and internal inspections? Would the Court still have concluded that there was a violation of Article 3 or would it rather have considered that everything that the applicant complained of fell within the scope of Article 8, paragraph 1 and did not run counter to the criteria of Article 8, paragraph 2? We believe that the latter conclusion would have been reached. Enhancing both the reliability and the 'softness' of surveillance measures contributes to their legal receptiveness and apparently silences civil liberty arguments.[129] All softer surveillance techniques need to be sanctioned by the European human rights machinery is a certain degree of user's acceptance and for governments to offer some ground for their use.[130] The relative irrelevance of the current human rights framework in this respect is nicely illustrated by a series of Bills in Britain allowing the police unlimited possibilities to retain DNA samples and fingerprints of innocent persons.[131] In the run-up to the final, police-friendly regulation, Prime Minister Tony

[127] P. De Hert & P. Ölçer, 'Het onschadelijk gemaakte Europees privacybegrip. Implicaties voor de Nederlandse strafrechtspleging', *Strafblad. Het nieuwe tijdschrift voor strafrecht*, 2004, vol. 2, No. 2, 115-134

[128] ECHR, *Khan* v. *the United Kingdom,* judgment of 12 May 2000. The *Khan* judgment accepted that the admission of evidence obtained in breach of the privacy right against an accused person is not necessarily a breach of the required fairness under Article 6 (the right to a fair trial). Evidence was secured by the police in a manner incompatible with the requirements of Article 8 of the Convention, and yet, it was admitted in evidence against the accused and led to his conviction, since the process taken as a whole was faire in the sense of Article 6 ECHR. See also § 79 of *P.G. and J.H. v. the United Kingdom*: "applicants had ample opportunity to challenge both the authenticity and the use of the recordings"; *P.G. and J.H. v. the United Kingdom*, judgment 25 September 2001

[129] In the nineties advances in DNA technology made it possible to produce good DNA profiles from biological material other than blood. With the argument that the procedure for taking saliva samples is less intrusive than drawing blood samples, the Dutch legislator lowered the threshold for obtaining samples of biological material without consent considerably, with the result that DNA analysis became possible for more types of offences. See Lia van der Westen, 'Legal Regulations Governing Forensic Scientific Methods', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *Harmonisation in Forensic Expertise. An Inquiry into the Desirability of and Opportunies for International Standards*, Amsterdam, Thela Thesis, 2000, (283-291), 290. In 1998, Corien Prins, to our knowledge, was one of the first to analyse the impact of biometric technology on the area of fundamental rights as laid down in the European context (J.E.J. Prins, 'Making our body identify for us: legal implications of biometric technologies', *Computer, Law & Security Report*, 1998, Vol. 14, No. 3, (159-165), 161). To her own surprise, this in-depth analysis did not produce a negative result for the use of unique characteristics of a human being such as his fingerprint, iris or hand geometry. Starting point is her observation "that with most biometric technologies no penetration of the body's surface is required, meaning that the use of these technologies will not be deemed unreasonably intrusive from this perspective". This technical fact explains all in the light of the human rights analysis.

[130] Apparently, this is the case with the major biometric applications. When European Commissioner Vitorino addressed the members of the European Parliament to defend the inclusion of biometrical data in the new European passports, his argument was that high-tech identification systems would eventually protect European citizens and safeguard, not limit their freedoms and rights. 'Biometrics will dramatically improve the accuracy of identification and protect citizens from wrong identification and having identification stolen by someone else,' he said, adding that the Commission's goal is to find reliable and efficient measures to 'support the free movement of persons'. Mr Vitorino also dismissed claims that the use of biometrics for identification purposes would result in treatment of EU citizens as crime suspects: 'As a Portuguese citizen I was ten years old when I was fingerprinted for a national identity card. I do not see that I was considered a criminal,' he said. Cf. 'European Commissioner Highlights benefits of biometric passports', 4 March 2004, via http://europa.eu.int/ida/en/document/2221/355.

[131] See 'UK: Police can keep DNA of innocent people indefinitely', 4p. via http://www.statewatch.org/news/2004/sep/03uk-dna-database.htm. Under the Police and Criminal Evidence Act 1984 (PACE) police could take body samples (DNA from mouth swabs) where people were suspected of having committed a "serious arrestable offence". The same law stipulated, in PACE, Section 64, that in case of DNA samples taken from a "person who is not suspected of having committed an offence or is not

Blair declared: "I believe the civil liberties argument is completely misplaced. This is using technology to catch criminals". An appeal was lodged by a person who was 11 years old when his fingerprints and DNA samples were taken and by a man whose case was never brought to court but whose data were nevertheless kept in the database. Both argued that the database with their fingerprints and DNA samples contravened their rights enshrined in Articles 8, paragraph 1 (privacy) and Article 14 (discrimination). Apparently Blair's argument found favour with the members of the House of Lords who had to consider the merits of the case. One Lord concluded that there no privacy issue was at stake at all ('Article 8, paragraph 1 of the ECHR is not engaged') and added: *"If I am wrong in this view, I would say any interference is very modest indeed"*.[132] On 22 July 2004 the House of Lords dismissed the case merely with reference to the reliability argument.[133]

Understanding 'necessity' in the context of Article 8: no more than proportionality

For one commentator the DNA development in Great Britain "*demonstrates the fundamental shortcoming of the law in protecting liberties and privacy. Providing data is "lawfully" collected there can be no objection whatsoever - but what if the laws themselves are contrary to the standards of a democratic society?*".[134]
The fundamental shortcoming we observe is Strasbourg's reluctance to carry out the political control of human rights infringements that is made obligatory by the requirement in the second paragraphs of Articles 8 to 11 that restrictions must be "necessary in a democratic society". In our opinion the Strasbourg judges are too hesitant and reluctant to apply this check and they clearly prefer the much more secure testing of the legality requirement (is there a law?). In the context of Article 10 ECHR (freedom of expression) the Court has observed that "necessary ... is not synonymous with *indispensable*, neither has it the flexibility of such expressions as *admissible*, *ordinary*, *useful*, *reasonable* or *desirable,* but that it implies a *pressing social need*".[135] It is for the national authorities to make the initial assessment as to whether this is the case; as was mentioned above, they enjoy a "margin of appreciation"

---

prosecuted or is acquitted of the offence, the sample must be destroyed" and "cannot be used in evidence against that person or for the purposes of any investigation of an offence". Although the scope of the law was widened in 1994 with the Criminal Justice and Public Order Act 1994 it was still based on the simple proposition that if a person was innocent - never charged or found not guilty of charges brought against him then fingerprints and DNA samples taken should be destroyed. The next change came in 2001 when the Criminal Justice and Police Act amended Section 64 of PACE to allow fingerprints and DNA samples to be retained indefinitely where they "were taken from a person in connection with the investigation of an offence". This change was prompted because it transpired that many police forces were not complying with the law as it stood by failing to destroy the fingerprints and DNA samples of those not charged with any offence or who were acquitted.

[132] Lord Steyn quoted in 'UK: Police can keep DNA of innocent people indefinitely', *l.c.*, 2.

[133] *"It is of paramount importance that law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science. It enables the guilty to be detected and the innocent to be rapidly eliminated from enquiries. Making due allowance for the possibility of threats to civil liberties, this phenomenon has had beneficial effects"* (Lord Steyn) and *"it seems to me that the benefits of the larger database are so manifest and the objections to it so threadbare that the cause of human rights generally would inevitably be better served by the database's expansion than its proposed contraction. The more complete the database, the better chance of detecting criminals, both those guilty of crimes past and those whose crimes are yet to be committed. The better chance too of deterring from future crime those whose profiles are already on the database"* (Lord Brown).

[134] T. Bunyan, 'Slide into authoritarianism?' via http://www.statewatch.org/news/2004/sep

[135] *Handyside v. United Kingdom*, judgment of 7 December 1976, § 48.

in doing so. Nevertheless, the Court will examine whether the reasons given by the national authorities for the measures taken were "relevant and sufficient" for the purposes of the Convention and whether the restriction was "proportionate" to the legitimate aim pursued.[136]
Many commentators of the European Convention fail to see that there is no such thing as a well-established case law with regard to the requirement "necessary in a democratic society" in the second paragraphs of Articles 8 to 11. Most commentators use Article 10 case law to explain the requirement in the context of Article 8. However, we are not aware of many cases with regard to Article 8 where these kinds of exercises are repeated. Almost always the requirement of "necessity" is brought back to the question of proportionality, in some cases supplemented by the requirement that the reasons for the interference are relevant and sufficient.[137] Only in the recent *Peck* judgment one can find some word games referring to the semantic exercise in the context of Article 10 discussed above.[138]
The reluctance of the judges to check the necessity requirement in Article 8 not only follows from their mild check of proportionality (as opposed to necessity), but also from their willingness to give Member States a wide margin of appreciation when creating privacy-limiting powers. We seldom find strict scrutiny by the European Court in the context of Article 8.[139]

Understanding the differences in application by the Court of Articles 8 and 10 is crucial for understanding the European human rights framework. In Europe, the rights in Article 8 are simply less fundamental than the rights in Article 10.[140] Skeptics would add that Article 10 is only important in Europe because as a rule it does not threaten governmental powers (many freedom-of-expression conflicts are of a horizontal nature), whereas Article 8, mainly governing the difficult relationship between individual rights and collective interests, is too important to governments to be of fundamental significance.

[136] See e.g. ECHR, *Young, James & Webster v. the United Kingdom*, judgment of 13 August 1981, § 63; ECHR, ECRM, *Jeffrey Dudgeon v. Ireland*, judgment of 22 October 1981, § 61; ECHR, *Rees v. the United Kingdom*, judgment of 17 October 1986, § 44 and ECHR, *Moustaquim v. France*, judgment of 18 February 1991, § 46.
[137] P. De Hert, *Artikel 8 EVRM. De bescherming van privacy, gezin, woonst en communicatie* , *o.c.*, 40-60. Compare with §76 of the *Peck* judgment: "In determining whether the disclosure was "necessary in a democratic society", the Court will consider whether, in the light of the case as a whole, the reasons adduced to justify the disclosure were "relevant and sufficient" and whether the measures were proportionate to the legitimate aims pursued" (ECHR, *Peck v. United Kingdom,* judgment of 28 January 2003).
[138] See the use of the term 'pressing social need' in the following quote: "In such circumstances, the Court considered it clear that, even assuming that the essential complaints of *Smith and Grady* before this Court were before and considered by the domestic courts, the threshold at which those domestic courts could find the impugned policy to be irrational had been placed so high that it effectively excluded any consideration by the domestic courts of the question of whether the interference with the applicants' rights answered a pressing social need or was proportionate to the national security and public order aims pursued, principles which lay at the heart of the Court's analysis of complaints under Article 8 of the Convention."; *Peck*, § 100
[139] See also: Y. Arai-Takahashi, *o.c.*, 91. In *Dudgeon* the Court applied a standard of strict scrutiny. Homosexuality touches one of the most intimate aspects of our private life and cannot be limited without serious reasons: 'not only the nature of the aim of the restriction but also the nature of the activities involved will affect the scope of the margin of appreciation. The present case concerns a most intimate aspect of private life. Accordingly, there must exist particularly serious reasons before interferences on the part of the public authorities can be legitimate for the purposes of paragraph 2 of Article 8' (ECRM, *Jeffrey Dudgeon v. Ireland*, judgment of 22 October 1981, § 52).
[140] P. De Hert & S. Gutwirth, 'Grondrechten: vrijplaatsen voor het strafrecht? Dworkins Amerikaanse trumpmetafoor getoetst aan de hedendaagse Europese mensenrechten' in Haveman, R. & Wiersinga, H. (eds.), *Langs de randen van het strafrecht*, Nijmegen, Wolf Legal Pu., 2005.

A great deal of critical work will have to be done in the future to assess the real weight of the European human rights framework. We will end with two observations on the criteria of subsidiarity

A subsidiarity test against softer surveillance?

It is often said that with regard to the requirement 'necessary in a democratic society' the Courts looks at the requirement of proportionality (does the aim justify the means) *and* the requirement of subsidiarity (are there other less intrusive means available?). The requirement of subsidiarity is a common feature in the regulations on telephone tapping in most Member States:[141] telephone tapping is not only limited to serious cases (principle of proportionality), but also only to be used as a last resort when no other technique might do the work (principle of subsidiarity). The idea of subsidiarity is often upheld in human rights literature concerning new technologies.[142] It is intended to put sensible limits on privacy-infringing procedures. It seemingly presents a powerful limitation on the freedom of the legislator to define powers and the right of government officials to apply powers. Privacy infringements would then only be possible if there is no other means to safeguard the public interest at stake in a less-invasive-to-privacy way, or less violating of the data subject's rights.[143]

Firstly, we ask whether the criteria really exist in the minds of the Strasbourg judges. A careful analysis of the Article 8 ECHR case law shows that the Court almost never relies on this criterion borrowed from the Article 10 ECHR case law.[144] *Peck* is in fact one of the first judgments in which the criterion is applied, although the Court does not identify it as such.[145]
Unfortunately there are not many other precedents showing this straightforward use of the subsidiarity test. The facts in Perry are rather 'innocent'. It is not a case dealing with the delicate balance between privacy and national security interests. It can be

[141] J. Pradel, 'Criminal Evidence', in J.F. Nijboer & W.J.J.M. Sprangers (eds.), *Harmonisation in Forensic Expertise. An Inquiry into the Desirability of and Opportunies for International Standards*, Amsterdam, Thela Thesis, 2000, (411-429), 423. It was introduced in Article 90*ter* of the Belgian Code of Criminal Procedure governing telephone tapping by the law of 30 June 1994.
[142] See e.g. María Verónica Pérez Asinari & Yves Poullet, 'The Airline Passenger Data Disclosure Case and the EU-US Debate', *Computer Law & Security Report*, 2004, vol. 20, No. 2; 98-116.
[143] María Verónica Pérez Asinari & Yves Poullet, *l.c.*, 105.
[144] P. De Hert, *Artikel 8 EVRM en het Belgisch recht. De bescherming van privacy, gezin, woonst en communicatie*, Gent, Mys en Breesch Uitgeverij, 1998, 367p.
[145] ECHR, *Peck v. the United Kingdom,* judgment of 28 January 2003 (to hand over CCTV images to the media violates Article 8 ECHR and in particular the requirements of proportionality and subsidiarity, since other alternatives to generate publicity for the CCTV initiative exist). See especially § 76 of *Peck*: "In determining whether the disclosure was "necessary in a democratic society", the Court will consider whether, in the light of the case as a whole, the reasons adduced to justify the disclosure were "relevant and sufficient" and whether the measures were proportionate to the legitimate aims pursued". See also: ECHR, *Hatton v. the United Kingdom*, judgment of 2 October 2001. In *Peck* the Court did not dispute that CCTV systems are important for detecting and preventing crime and that the release of CCTV material with the aim of promoting their effectiveness in the prevention and detection of crime could render their role more successful. However, at least three alternatives were available for the local Council to allow it to achieve the same objectives: obtaining consent of the person filmed prior to disclosure; masking the relevant images itself or obliging the media to mask those images. The Council did not explore the first and second options. The Court also considered that the steps taken by the Council in respect of the third were inadequate. Accordingly, the disclosures by the Council of the CCTV material to media such as the BBC were not accompanied by sufficient safeguards to prevent disclosure inconsistent with the guarantees of respect for the applicant's private life contained in Article 8 of the Convention. As such, the disclosure constituted a disproportionate and therefore unjustified interference with his private life and a violation of Article 8 of the Convention" (*Peck,* § 87).

doubted that many other cases will follow in this context in the light of the margin of appreciation that is recognized in that area.
Secondly, it can be doubted whether the subsidiarity test properly applied will work *against* new modes of surveillance. What standard makes one practice less intrusive than another? How to measure intrusiveness? Is something or some power more intrusive when it touches upon a wide range of rights and liberties? Or when it deeply impacts one right or liberty? When it is applied secretly? When there are no alternatives? When there are alternatives? When it is applied systematically? When it is applied without judicial intervention? When there is immediate harm? When there is no immediate harm, but potential harm in the future? What makes us so certain that e.g. biometrics and other contemporary technologies used in law-enforcement counter-measures are more intrusive than other identification and verification practices? Is not a system based on large-scale biometric identification 'better' than a system of harsh reactive police powers? The idea to qualify softer technologies as more human-rights friendly is tempting. Although we reject it and believe that their secret nature makes them very dangerous from a human rights perspective, we note that the idea easily finds defenders in circles of policy-makers and even in literature.[146] In the Belgian DNA Bill of 22 March 1999, the legislator consciously omitted the subsidiarity criterion, although he had used it in 1994 to regulate telephone tapping, The rationale is that DNA analysis is perfectly suited to obtain certainty in an early phase of the criminal investigation concerning someone's involvement in a crime, in order to avoid wrong investigative orientations. A negative DNA test avoids time-consuming investigative steps, such as witness confrontations, needed to establish the innocence of persons that consented to having their DNA analysed. These elements explain the willingness of the Belgian legislator to make DNA analysis possible at the same time as and *before* other more classical investigative steps.[147]

Conclusions

In this contribution we have added a critical note to the literature on the importance of the European human rights framework with regard to law-enforcement counter-measures after 9/11. Our results confirm the recent 'realistic' reading of the American human rights framework by the famous communitarian author Amitai Etzioni.[148] In his analysis, Etzioni criticizes civil libertarians who, without necessarily opposing making concessions to advance public safety, place the burden on the government to prove that such concessions are needed. These civil libertarians, Etzioni observes, call for a strict scrutiny approach and demand a more restrictive definition of the conditions under which the new technologies can be used.[149]

[146] Comp. A. Etzioni, 'Implications of Select New Technologies for Individual Rights and Public Safety', *Harvard Journal of Law & Technology*, 2002, Vol. 15, No. 2, (1-43), 27.
[147] B. De Smet, *Vergelijkend DNA-onderzoek in strafzaken*, Ghent, Larcier, Reeks CABG, 2003, (53p.) 20 with ref.
[148] A. Etzioni, 'Implications of Select New Technologies for Individual Rights and Public Safety', *Harvard Journal of Law & Technology*, 2002, Vol. 15, No. 2, (1-43), 34
149. A. Etzioni, *l.c.*, 2-3 with ref. to Nadine Strossen, 'Remarks at the Communitarian Dialogue on Privacy vs. Public Safety' (Nov. 26, 2001), *at* http://www.gwu.edu/~ccps/privtrans.html and to Jerry Berman, Executive Director, Center for Democracy

These claims are of course rejected by Etzioni, who notes that, historically, courts have found searches to be reasonable when they serve a compelling public interest, such as public safety or public health.[150] He demonstrates that most new technologies meet the necessity requirement simply because they are reliable and cannot be replaced by alternatives,[151] and concludes that denying public authorities the law enforcement tools and the technology they need to do their work, is simply no good option. What should be done instead is to focus more on accountability before denying powers to law enforcement.[152]

Without sharing Etzioni's conclusions, we find his analysis pertinent for a better understanding of the contemporary human rights framework, also in Europe. The application of the current human rights framework simply does not produce satisfying results. The European Convention, in particular where it uses the wording "necessary in a democratic society" invites a critical assessment of new identification schemes taking into account all constitutional relevant factors. However, on the basis of the existing case law one cannot deduce too many constraints for the present development with regard to contemporary law-enforcement counter-strategies. Although we favour strict scrutiny by the Court in all cases involving 'hard' *and* 'soft' surveillance and other law-enforcement counter-measures, this standard is not upheld by the Court. Overestimating the readiness of the Court to check on security strategies in the Member States does not clarify the debate. Although several authors maintain that general regulations that allow for privacy infringements will probably not pass the quality of law test nor the proportionality test imposed by the Court,[153] some European Member States have elaborated broad regulations with regard to data retention,[154] and will probably never be sanctioned by the European Court.
Without giving up on the principles that foster hope in the current human rights framework, we would like to suggest more attention in literature to the precise nature of the standards of scrutiny operated by the European Court. Realizing that the current human rights framework will not hold back security uses of contemporary technology, should make us better understand the vulnerability of our legal system and its balance between liberty and security. National and European legislators should realize that their powers to define new measures largely remain unchecked by the European judicial mechanism. Hence, before deciding on legislation, they need to pay more attention to relevant questions inspired by constitutional reasonableness.

---

and Technology*, Civil Rights and Anti-Terrorism Efforts: Hearing before the Senate Subcomm. on Constitution, Federalism and Property Rights of the Senate Comm. on the Judiciary*, 106th Cong. (2001).

150 A. Etzioni, *l.c.*, 2-3 with ref. to US case law such as *Vernonia School District 47J v. Acton*, 515 U.S. 646, 661 (1995) (defining a compelling state interest as "an interest that appears *important enough* to justify the particular search at hand, in light of other factors that show the search to be relatively intrusive upon a genuine expectation of privacy."), *United States v. Doe*, 61 F.3d 107, 109-10 (1st Cir. 1995) ("[R]outine security searches at airport checkpoints pass constitutional muster because the compelling public interest in curbing air piracy generally outweighs their limited intrusiveness.") and *Marshall v. Horn Seed Co.*, 647 F.2d 96, 102 (10th Cir. 1981) (holding that "the compelling public interest in preventing or speedily abating hazardous conditions . . . demands relaxation of the traditional probable cause test for administrative inspections. . . .").

151 A. Etzioni, *l.c.*, 27.

152 A. Etzioni, *l.c.*, 43.

153 Compare with the similar findings of Goemans and Dumortier with regard to mandatory data retention: C. Goemans & J. Dumortier, 'Mandatory retention of Traffic Data in the EU: Possible Impact on Privacy and On-Line Anonymity', *l.c.*, 161-183.

154 See for instance on the Belgian Article 109b of the law of 11 March 1991 introduced by the laws of 11 June 1998 and 28 November 2000: Yves Poullet, 'The Fight against Crime and/or the Protection of Privacy: A Thorny Debate', *International Review of Law Computers & Technology*, 2004, Vol. 18, No. 2, 251-273.

Of course, nothing prevents the European legislator from seeking constitutional guidance in European human rights law and from trying to grasp the meaning behind the texts, knowing not to expect close scrutiny from the Court if the legislator fails to do this. When the maximum-security society comes to us without mediation, it will primarily be the European legislator's, not the judge's responsibility.