# Data Protection Pursuant to the Right to Privacy in Human Rights Treaties

[Published in *International Journal of Law and Information Technology*, 1998, volume 6, pp. 247–284]

***Lee A Bygrave***

## Abstract

This paper examines the extent to which the basic principles of data protection laws may be read into provisions in human rights treaties proclaiming a right to privacy. Two such provisions are analysed in detail: Art 17 of the International Covenant on Civil and Political Rights and Art 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Case law developed pursuant to both provisions indicates that each have the potential to embrace all of the core principles typically found in data protection laws. However, this case law currently falls short of data protection laws in terms of both ambit and prescriptory guidance.

## 1. Introduction

Catalogues of fundamental human rights and freedoms as set out in certain multilateral treaties provide much of the formal normative basis for law and policy on data protection. This is expressly recognised in many data protection laws themselves. For example, the main object of the Council of Europe's (CoE) Convention on data protection[1] is "to secure … for every individual … respect for his fundamental rights and freedoms, and in particular his right to privacy …" (Art 1). One of the main objects of the European Community's (EC) Directive on data protection[2] is expressed in similar terms.[3]

While a broad range of rights and freedoms in these international catalogues can be said to inspire the principles found in data protection laws, it is the right to privacy or private life which is commonly regarded as forming the central basis for these principles.[4] Accordingly, focus in this paper is directed towards the legal reach of provisions proclaiming such a right. Two provisions are examined in detail: Art 17 of the International Covenant on Civil and Political Rights (ICCPR)[5] and Art 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).[6]

More specifically, this paper sketches the extent to which the above two provisions embrace the principles and guarantees found in data protection laws. Can, in other words,

---

1 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) adopted 28.1.1981, in force 1.10.1985.

2 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ No L 281, 23.11.1995, 31), adopted 24.10.1995.

3 See Art 1(1). See also recital 10 of the Directive (noting that "the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized ... in Article 8 of the European Convention for the Protection of Fundamental Rights and Freedoms"). Note too the Preamble to Australia's federal Privacy Act 1988 (indicating that the Act is, in part, "necessary to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence" pursuant to Art 17 of the International Covenant on Civil and Political Rights).

4 Again, this is manifested in Arts 1 of the CoE Convention and EC Directive on data protection, each of which single out the "right to privacy" as being especially pertinent in a data protection context.

5 Adopted 16.12.1966, in force 23.3.1976.

6 Adopted 4.11.1950, in force 3.9.1953.

these provisions function as data protection instruments in their own right? The issue is particularly significant for citizens in countries that (i) lack domestic data protection laws, (ii) are not legally or politically bound to introduce such laws pursuant to an international instrument dealing specifically with data protection,[7] but (iii) are party to the ICCPR and/or ECHR. If the right to privacy laid down in the latter treaties embodies the basic principles of data protection laws, the citizens may be able to gain some relief in cases where data on them are processed in violation of those principles. Of course, the governments of the countries concerned will also be under a legal duty to introduce rules on data protection in compliance with the ICCPR and/or ECHR.

The issue is also significant for citizens in countries that do have domestic data protection laws and/or are obligated to introduce such laws pursuant to an international instrument dealing specifically with data protection. If the right to privacy pursuant to the ICCPR and/or ECHR provides a *higher* standard of data protection than is provided by the domestic rules or the international instrument, the citizens may be able to gain some relief in cases where data on them are processed in compliance with domestic laws but not the ICCPR and/or ECHR. Again, the governments of the countries concerned will be under a legal duty to raise the domestic levels of data protection to the level required by either of the two human rights treaties.

Further, the issue is pertinent to resolution of the extent to which the enforcement mechanisms for the ECHR and ICCPR can be used to overcome deficiencies in the equivalent mechanisms for the international instruments dealing specifically with data protection. All of the latter instruments, with the exception of the EC Directives, lack judicial or quasi-judicial bodies for their interpretation and enforcement. However, if a breach of their provisions is also a breach of the ECHR and/or ICCPR, the enforcement mechanisms of the latter treaties may be used to overcome this deficiency.

At the same time, it should be noted that the enforcement mechanisms for the ECHR are more powerful than those for the ICCPR. Unlike the ECHR, the ICCPR lacks a proper judicial body to enforce its provisions.[8] The ICCPR has instead an oversight and complaints-handling body in the form of the Human Rights Committee.[9] Upon exhaustion of domestic remedies for complaints of breaches of rights contained in the ICCPR, persons may lodge complaints before the Committee, provided that the state party concerned has signed the first Optional Protocol to the Covenant. The views reached by the Committee on these complaints are not binding under international law, but they carry a great deal of weight otherwise.[10] These views, along with the Committee's reports and general comments to states parties under Art 40(4) of the ICCPR, provide authoritative guidance on the scope of the Covenant's provisions.

As indicated above, it is the basic principles of data protection laws which constitute the main points of departure in this paper for assessing the ambit of Art 17 of the ICCPR and Art 8 of the ECHR. These principles focus on the processing (ie, collection, registration,

---

7 There are four relevant instruments in this respect: (i) the CoE Convention on data protection (see *supra* n 1); (ii) the EC Directive on data protection (see *supra* n 2); (iii) the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD, 1980), adopted 23.9.1980; and (iv) the UN Guidelines Concerning Computerized Personal Data Files (Doc E/CN.4/1990/72, 20.2.1990), adopted by the UN General Assembly on 4.12.1990. Of these, only the first two listed are legally binding instruments. Note, though, that the CoE Convention does not require a CoE member state to implement its provisions until it is ratified by the state. A range of international instruments have also been adopted dealing with data protection for specified sectors of activity, but only one of these instruments is legally binding: this is the EC Directive 97/66/EC on the processing of personal data and the protection of privacy in the telecommunications sector (OJ No L 024, 30.1.1998, 1), adopted 15.12.1997.

8 The International Court of Justice does not have jurisdiction to hear complaints concerning breaches of the Covenant.

9 For a detailed description of the Committee and its operations, see D McGoldrick, *The Human Rights Committee: Its Role in the Development of the International Covenant on Civil and Political Rights* (Oxford: Clarendon Press, 1991).

10 *Ibid*, 151–152, and references cited therein; M Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (Kehl am Rhein/Strasbourg/Arlington: Engel, 1993), xix.

storage, use and/or dissemination) of personal data. By "personal data" is meant data (or information) that relate to, and allow identification of, individual physical/natural persons (and sometimes groups or organisations). The principles can be summarised as follows:

- personal data should be gathered by fair and lawful means (hereinafter termed "fair collection principle");
- the amount of personal data gathered should be limited to what is necessary to achieve the purpose(s) of gathering the data (hereinafter termed "minimality principle");
- personal data should be gathered for specified and lawful purposes and not processed in ways that are incompatible with those purposes (hereinafter termed "purpose specification principle");
- use of personal data for purposes other than those specified should occur only with the consent of the data subject or with legal authority (hereinafter termed "use limitation principle");
- personal data should be accurate, complete and relevant in relation to the purposes for which they are processed (hereinafter termed "data quality principle");
- security measures should be implemented to protect personal data from unintended or unauthorised disclosure, destruction or modification (hereinafter termed "security principle");
- data subjects should be informed of, and given access to, data on them held by others, and be able to rectify these data if inaccurate or misleading (hereinafter termed "individual participation principle"); and
- parties responsible for processing data on other persons should be accountable for complying with the above principles (hereinafter termed "accountability principle").

## 2. Relevant provisions on the right to privacy in international human rights instruments

At the apex of international human rights instruments lies the Universal Declaration of Human Rights of 1948. Its provisions dealing expressly with privacy are set out in Art 12, which states:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

In almost identical terms, Art 17 of the ICCPR provides:

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks".

Whereas the above provisions are framed essentially in terms of a prohibition on "interference with privacy", the equivalent provisions of Art 8 of the ECHR are framed in terms of a right to "respect for private life":

"1. Everyone has the right to respect for his private and family life, his home and 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".

Express protection for "private life" is also found in Art V of the 1948 American Declaration of the Rights and Duties of Man, and in Art 11 of the American Convention on Human Rights (ACHR) of 1969. Article V of the Declaration states:

"Every person has the right to the protection of the law against abusive attacks upon his honor, his reputation, and his private and family life".

Article 11 of the ACHR provides:

"1. Everyone has the right to have his honour respected and his dignity recognized.
2. No one may be the subject of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
3. Everyone has the right to protection of the law against such interference or attacks".

The other major regional human rights catalogue – the African Charter on Human and People's Rights of 1981 – omits express protection for privacy or private life.[11]

Much of the terminology in the above provisions is diffuse. Moreover, authoritative material on their precise ambit in the context of processing personal data is scarce. This is especially the case with the American instruments. Some case law, however, has been developed around Art 8 of the ECHR and Art 17 of the ICCPR which indicates that both provisions embrace core data protection principles. This case law provides indication of a similar potential with respect to the privacy provisions in the American human rights instruments.[12]

## 3 Article 17 of the ICCPR

Case law developed around Art 17 of the ICCPR provides the clearest indication that the right to privacy in international law harbours core data protection principles. This is particularly significant as the ICCPR has the greatest reach of treaties on human rights, having been ratified by some two-thirds of the world's nation-states.[13]

In its General Comment 16, the Human Rights Committee has stated that Art 17 requires legal implementation of essential data protection guarantees in both the public and private sectors. In the words of the Committee:

"The competent public authorities should only be able to call for such information relating to an individual's private life the knowledge of which is essential in the interests of society as understood under the Covenant. [...] The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals

---

[11] This omission is not repeated in all human rights catalogues generated outside the Western, liberal-democratic sphere. See, for instance, the Cairo Declaration on Human Rights in Islam of 5.8.1990 (UN Doc A/45/421/5/21797, 199), Art 18 of which expressly recognises a right to privacy for all individuals.

[12] Note, for instance, that the jurisprudence of the European Court of Human Rights has generally exercised considerable influence on the decision making of the Inter-American Court of Human Rights, which is charged with hearing and determining complaints of breaches of the ACHR: see JG Merrills, *The Development of International Law by the European Court of Human Rights* (Manchester: Manchester University Press, 1993, 2nd ed), 18–19 and cases cited therein.

[13] Nowak, *supra* n 10, xxi.

and bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination".[14]

These words seem clearly inspired by the now considerable body of legal instruments on data protection found both nationally and internationally. At the same time, it is worth noting that the data protection guarantees listed here by the Committee are significantly truncated relative to the principles specified in ordinary data protection instruments. For instance, the Committee reads into Art 17 a limitation on collection of personal data but without specifying the need to ensure that the manner of collection is fair.[15] Similarly, the Committee mentions the need for security measures but relates these only to ensuring that personal data are kept confidential. No mention is made of the need to ensure that personal data are also safeguarded against unauthorised alteration or destruction or are otherwise adequate, relevant and not excessive in relation to the purposes for which they are processed.[16] No mention is made either of special categories of data that may require a more stringent level of protection.[17] Further, the principle of purpose specification laid down by the Committee is looser than the equivalent principle set down in, eg, Art 5(b) of the CoE Convention on data protection.[18] The principles that are dealt with most comprehensively by the Committee concern rights on information access and rectification, but these seem to be formulated only in relation to computerised ("automatic") files.

It is surprising that the Committee's specification of data protection principles is so truncated, given that the Committee had at the time of writing its General Comment several authoritative sets of more comprehensive data protection principles to which it could refer. This raises the question of whether or not the principles laid down by the Committee are intended to delineate exhaustively the extent to which Art 17 embraces data protection. One might argue that, in keeping with conceptions of "privacy" in terms of seclusion or limited accessibility, the Committee has purposefully angled its general comment to give priority to safeguarding the interest of persons in keeping information about themselves out of the hands of others. Supporting this argument is, *inter alia*, the Committee's relatively narrow conception of the purpose of security measures.[19] However, the Committee's specification of access and rectification rights would seem to point to broader concerns, such as ensuring that

---

[14] General Comment 16, issued 23.3.1988 (UN Doc A/43/40, 181–183; UN Doc CCPR/C/21/Add.6; UN Doc HRI/GEN/1/Rev 1, 21–23), paras 7 & 10.

[15] Cf the fair collection principle as set down in, eg, Art 6(1)(a) of the EC Directive on data protection (personal data must be "processed fairly and lawfully").

[16] Cf the security and data quality principles as set down in, eg, Arts 17(1) and 6(1)(c) of the EC Directive on data protection. Article 17(1) provides, *inter alia*, that appropriate measures must be taken to protect personal data "against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access". Article 6(1)(c) provides that personal data must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".

[17] By contrast, the majority of data protection laws single out certain types of personal data (eg, data on a person's ethnic origins, religious beliefs, sexual habits or criminal convictions) as warranting special protection.

[18] Article 5(b) of the Convention states that personal data undergoing automatic processing shall be "stored for specified and legitimate purposes and not used in a way incompatible with those purposes".

[19] See also Nowak, *supra* n 10, 296–297 (claiming that data protection pursuant to Art 17 is a "special form of respect for intimacy", the latter notion being defined in terms of non-disclosure of "private characteristics, actions or data").

persons are able to orient themselves and maintain some sort of control over their informational environs. If so, there is little reason for not being able to treat the Committee's General Comment as merely laying down some but not all of the data protection guarantees capable of specification pursuant to Art 17.

It is also worth noting that the Human Rights Committee in subsequent case law has defined the notion of privacy in Art 17 as denoting more than simply a sphere of seclusion for oneself; it is also "a sphere of a person's life in which he or she can freely express his or her identity, be it by entering into relationships with others or alone".[20] Defined thus, "privacy" in Art 17 has been given a considerable potential for expansion, a potential that may, for example, be exploited to strengthen data subjects' ability to rectify registered data on themselves which do not correspond to their self-perception.[21] Concomitantly, the *Coeriel and Aurik* decision indicates that the notion of "private life" in General Comment 16 should not be interpreted narrowly; in other words, to be protected under Art 17, data on a person's private life need not refer only to what the person does in the intimacy of his/her home but also to, say, his/her professional activities.[22]

Further, there is little good reason for limiting the application of Art 17 to situations in which personal data are collected, stored or further processed by computerised/automated methods: manual processing can also threaten a person's privacy.[23]

## 4. Article 8 of the ECHR

### *4.1. Introductory comments*

The case law pursuant to Art 8 of the ECHR which touches upon data protection issues is relatively extensive.[24] At the same time, though, it has not yielded within the confines of one judgment a sweeping pronouncement on data protection principles along the lines of that contained in General Comment 16 of the Human Rights Committee. Instead, the Strasbourg organs have inched towards a recognition of various data protection guarantees in Art 8 on a case-by-case basis. Concomitantly, these guarantees have tended to be linked to the concrete circumstances of the particular case, making it difficult to apply them more generally. Hence, the following analysis of the extent to which Art 8 embraces data protection principles is necessarily more complicated and lengthy than in relation to Art 17 of the ICCPR.

To begin with, the European Commission and Court of Human Rights have taken a broad, evolutive view of the ambit of Art 8 of the ECHR. This is in keeping with their intention to apply the Convention as a "living instrument which ... must be interpreted in the light of present-day conditions".[25] In line with Art 31(1) of the 1969 Vienna Convention on

---

[20] *Coeriel & Aurik v the Netherlands* (1994) Comm 453/1991, para 10.2, reported in, *inter alia*, (1994) 15 *HRLJ*, 422. See also Nowak, *supra* n 10, 297 (defining the right to privacy in Art 17 as protecting "that area of individual autonomy in which human beings strive to achieve self-realization ... alone or together with others").

[21] Cf the case law (presented *infra* section 4.4) on transsexuals' rectification rights under Art 8 of the ECHR.

[22] See also the line taken by the European Court of Human Rights, described *infra* section 4.1. Data protection laws generally apply to all data that permit identification of an individual person, not just to data that relate to a particular sphere of a person's activity: see, eg, Art 2(a) of the EC Directive on data protection.

[23] The CoE Convention and UN Guidelines on data protection (see *supra* n 7) apply primarily to automated data files but allow for the optional extension of their principles to non-automated files. This approach is now dated: see, eg, the EC Directive on data protection which applies to both manual and automated data processing. Note too that the Strasbourg organs have not distinguished between computerised and manual data processing when interpreting the protective ambit of Art 8 of the ECHR.

[24] Case law pursuant to other articles in the ECHR – notably Arts 6, 10 and 13 – has also on occasion touched upon data protection issues, but it is Art 8 case law that is of central importance here.

[25] *Tyrer v UK* (1978) *Series A of the Publications of the European Court of Human Rights* (hereinafter "Series A"), No 26, para 31.

the Law of Treaties,[26] the Court and Commission have put weight on the basic object and purpose of the ECHR when interpreting its provisions. The object and purpose have been defined in terms of protecting human rights and promoting the ideals and values of democratic society.[27] The Strasbourg organs have also been influenced by the development since 1950 of common legal and ethical standards in the CoE member states. On the basis of such developments, the Court and Commission have been prepared to read into the Convention additional requirements for improving the protection of persons in relation to problems that may not have been specifically addressed or contemplated by the Convention's drafters. But they have done so only with respect to requirements that are viewed as "inherent" in a stated right; ie, as "based on the very terms of the ... [stated right] read in its context and having regard to the object and purpose of the Convention".[28] As Harris *et al* note, though, "the line between judicial interpretation and legislation can be a difficult one to draw, particularly in the case of generally worded provisions".[29]

The introduction during the 1970s and 1980s in many of the CoE member states of data protection laws based on a common set of principles, together with the conclusion of international agreements on data protection – most notably the CoE Convention of 1981 – have no doubt engendered readiness on the part of the Strasbourg organs to read into the ECHR (particularly Art 8) a requirement that member states respect basic data protection guarantees. At the same time, however, one finds few explicit references in the case law of the Strasbourg organs to the above legal instruments on data protection. Moreover, one cannot assume that the ECHR will invariably be interpreted by the Strasbourg organs in complete conformity with these instruments' requirements. The Court and Commission have insisted that the provisions of the ECHR have an autonomous meaning in relation to provisions found in other legal instruments.[30] Nevertheless, there is little doubt that the principles found in the CoE Convention on data protection have influenced, and will continue to influence, the way in which the Strasbourg organs interpret the ECHR. In this regard, it is instructive to note the following comment by the Court's former president, Rolv Ryssdal:

"For our part, we in Strasbourg should not ignore the basic principles laid down in the Data Protection Convention in addressing ourselves to those issues which do come before us. Those basic principles are a sectoral implementation of Article 8 of the European Convention on Human Rights in the context of automatic data processing and may therefore [be employed] in aid in interpreting that provision".[31]

The "essential" object of Art 8 has been expressed in terms of protecting "the individual against arbitrary interference by the public authorities in his private or family life".[32] As for the basic ambit of the right to respect for private life, this has been expressed by the Commission as being "such that it secures to the individual a sphere within which he can

---

[26] The provisions of the Vienna Convention constitute a general point of departure for the Court's interpretation of the ECHR: see *Golder v UK* (1975) Series A, No 18, para 29. For an overview and discussion of the Court's interpretative methods generally, see, eg, DJ Harris, M O'Boyle & C Warbrick, *Law of the European Convention on Human Rights* (London/Dublin/Edinburgh: Butterworths, 1995), 5ff; Merrills, *supra* n 12, chapt 4.

[27] See, eg, *Soering v United Kingdom* (1989) Series A, No 161, para 87; *Kjeldsen, Busk Madsen and Pedersen v Denmark* (1976) Series A, No 23, para 53.

[28] *Golder*, *supra* n 26, para 36.

[29] Harris *et al*, *supra* n 26, 8. See further P Mahoney, "Judicial Activism and Judicial Self-Restraint in the European Court of Human Rights: Two Sides of the Same Coin" (1990) 11 *HRLJ*, 57–88.

[30] Harris *et al*, *supra* n 26, 17.

[31] R Ryssdal, "Data Protection and the European Convention on Human Rights", in *Data Protection, Human Rights and Democratic Values*, Proceedings of the 13th Conference of Data Protection Commissioners held 2–4 October 1991 in Strasbourg (Strasbourg: CoE, 1992), 42.

[32] *Case "Relating to Certain Aspects of the Laws on the Use of Languages in Education in Belgium"* (1968) Series A, No 6, para 7. See also *Marckx v Belgium* (1979) Series A, No 31, para 31; *Airey v Ireland* (1979) Series A, No 32, para 32.

freely pursue the development and fulfilment of his personality".[33] Both the Commission and the Court have stressed that this right embraces more than merely safeguarding a sphere of seclusion in which the individual may act autonomously. It also gives some protection for inter-personal relationships both inside and outside the domestic realm. Thus, in *Niemitz v Germany*, the Court held:

"it would be too restrictive to limit the notion [of 'private life'] 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. There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world".[34]

Article 8 does not merely oblige a state party to abstain from interfering with private life; it additionally creates "positive obligations" on the state party to take action to ensure that private life is effectively respected.[35] For instance, it has been held that, under certain circumstances, a state party is obliged under Art 8(1) to establish a procedure for independently determining persons' demands for access to information kept on them by a public authority.[36] As shown below, however, the content of a state party's positive obligations under Art 8 in relation to the data-processing activities of its own agencies has yet to be fully established. This is partly because the Court and Commission allow a state a certain "margin of appreciation" in determining for itself the legitimate extent of its positive obligations. The ambit of this margin necessarily varies from case to case, making it difficult to set down a complete set of obligations in the abstract.

Further to these positive obligations, the Court has held that Art 8 "may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals themselves".[37] At the time of writing this paper (June 1998), the issue of whether or not Art 8 provides protection against the data-processing activities of private bodies has not been conclusively determined by the Strasbourg organs.[38] This is in contrast to

---

33 *Deklerck v Belgium* (1980), Application No (hereinafter "Appl") 8307/78, 21 *Decisions and Reports of the European Commission of Human Rights* (hereinafter "DR"), 116, 124.

34 (1992) Series A, No 251-B, para 29. See also *Halford v United Kingdom* (1997) *Reports of Judgments and Decisions* (hereinafter "Reports"), 1997-III, 1004 (confirming that telephone calls made from business premises may be covered by the notion of "private life" in Art 8(1)). Note too the Commission's statement in *X v Iceland* (1976) Appl 6825/74, 5 DR 86, 87 ("[f]or numerous Anglo-Saxon and French authors, the right to respect for 'private life' is the right to privacy, the right to live, as far as one wishes, protected from publicity ... In the opinion of the Commission, however, the right to respect for private life does not end there. It comprises also, to a certain degree, the right to establish and to develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's own personality"). Both statements are similar to the view of privacy in Art 17 of the ICCPR taken by the Human Rights Committee in *Coeriel & Aurik v the Netherlands*, *supra* n 19.

35 *Marckx*, *supra* n 32, para 31; *Airey*, *supra* n 32, para 31.

36 *Gaskin v United Kingdom* (1989) Series A, No 160, discussed *infra* section 4.4.

37 *X and Y v Netherlands* (1985) Series A, No 91, para 23.

38 In this respect, special note should be made of *Winer v United Kingdom* (1978) Appl 10871/84, 48 DR 154, in which the Commission refused to find that a private organisation's publication of a book containing both true and false statements about the applicant's sexual activities amounted to a breach of Art 8. The Commission's refusal was based partly on the fact that English law provided the applicant with a remedy in defamation as far as the publication of the false statements was concerned. As for the publication of the true statements (which, in English law, fell outside the tort of defamation), the Commission was reluctant to provide the applicant with a remedy pursuant to Art 8 because to do so would curtail the right to freedom of expression in Art 10 of the ECHR. As Harris *et al* comment, the Commission decision in *Winer* "does not decide ... that there is no positive obligation to protect against invasions of privacy by the press or other private persons by the revelation of private information in a case in which there is no remedy at all on the facts. Nor does it address the situation

the General Comment by the Human Rights Committee on Art 17 of the ICCPR which, as shown above, clearly establishes that Art 17 necessitates protection of persons from interferences by private bodies' data-processing practices. It is extremely doubtful that the Court or Commission would not interpret Art 8 as providing some measure of protection against the data-processing activities of private bodies, particularly given that these activities are regulated by most European data protection laws, including the CoE Convention on data protection. There is, in other words, firm evidence of common ground amongst CoE member states for applying data protection rules to private data controllers. There is also evidence from as far back as 1970 of some consensus amongst member states for holding that Art 8 ought to be read as affording protection from at least some private actors' data-processing activities.[39]

Another matter, though, is that even if the Court were to hear a case of alleged abuse by private bodies, it would be likely to act extremely cautiously when determining the extent to which the state concerned has not fulfilled its positive obligation(s) to protect persons from such abuse. This is because the Court would run the risk of prompting state intervention in the private sphere which could in turn undermine the very interests that Art 8 or other Convention provisions (eg, Art 10) are intended to safeguard. Accordingly, it is probable that the Court would accord states a broad "margin of appreciation" in such a case, at least as a point of departure for its deliberations.[40]

Up until the present day, the bulk of case law concerning data protection pursuant to Art 8 has centred upon state authorities' processing of personal data. I present this case law below, first in the light of Art 8(1), then in the light of the exemptions in Art 8(2). This is followed by a presentation of case law on the rights of persons to gain access to, and rectify, data kept on them by public authorities.

### *4.2. Interference with respect to Article 8(1)*

The case law makes clear that the surreptitious interception by state agencies of a person's communications constitutes an interference with the person's right under Art 8(1), and thus falls to be justified under Art 8(2). The leading cases here are *Klass and Others v Germany*[41] and *Malone v United Kingdom*,[42] each of which were occasioned by state agencies' secret tapping of persons' telephone calls. In both cases, the Court held these activities as contravening Art 8(1), though in *Klass* the Court went on to find the activities justified under Art 8(2). The more recent case of *Halford v United Kingdom* confirms that telephone calls

---

where the interference with privacy takes the form of an intrusion (eg by electronic eavesdropping or photography) in search of information, in which case a limitation on freedom of expression or any other Convention right would not be directly involved": Harris *et al*, *supra* n 26, 326. Moreover, the *Winer* decision has little bearing on how the Court or Commission might assess a range of other situations involving private sector use of personal data, such as the sale of customer lists without the consent of the customers concerned.

39 See para C7 of Res 428 (1970) adopted by the CoE Parliamentary Assembly on 23.1.1970 ("The right to privacy afforded by Article 8 ... should not only protect an individual against interference by public authorities, but also against interference by private persons including mass media"). Note too that there seems to be broad support amongst academic commentators on the ECHR for construing Art 8 so that it covers data processing by private bodies: see, eg, P van Dijk & GJH van Hoof, *Theory and Practice of the European Convention on Human Rights* (Deventer/Boston: Kluwer Law and Taxation Publishers, 1990, 2nd ed), 372; P Falck, *Personvern som menneskerett. Den europeiske menneskerettighetskonvensjon artikkel 8 som skranke for innsamling, behandling og bruk av personopplysninger*, Det juridiske fakultets skriftserie nr 56 (Bergen: University of Bergen, 1995), 24–25; D Feldman, "The Developing Scope of Article 8 of the European Convention on Human Rights" (1997) *EHRLR*, 265, 272; A Clapham, *Human Rights in the Private Sphere* (Oxford: Clarendon Press, 1993), 214, 286. The latter work should be singled out for particular mention on account of its excellent, sustained argument that the ECHR generally ought to apply so as to protect victims of abuse from private bodies.

40 See further Clapham, *supra* n 39, 220ff.

41 (1978) Series A, No 28.

42 (1984) Series A, No 82.

need not be made in a domestic setting in order to qualify for protection under Art 8; also telephone calls made from business premises may be covered.[43]

The mere existence of laws and practices allowing state agencies to carry out secret surveillance of citizens may be sufficient to interfere with citizens' rights under Art 8(1).[44] This considerably eases the burden on an applicant of showing that he/she has been the victim of an interference occasioned by surreptitious surveillance measures.[45] A similar line has been taken in relation to scrutiny by prison authorities of prisoners' correspondence: the mere fact that prison rules allow for the opening and perusal of prisoners' correspondence may mean that a prisoner can claim to be a victim of interference with his/her right pursuant to Art 8(1).[46] In the absence of laws and practices permitting surveillance, victim status will only be recognised when applicants can prove that there is a "reasonable likelihood" that the actions allegedly constituting interference have occurred.[47]

Security clearances of potential employees involving the surreptitious registration and communication of information about these persons' private lives may contravene Art 8(1). The leading case here is *Leander v Sweden*,[48] which concerned a Swedish carpenter who was prevented from gaining employment at a naval museum because police records (to which he was refused access) contained information on his past activities supposedly showing him to be a security risk. According to the Court,

"[b]oth the storing and release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1".[49]

However, the Court went on to find this interference as justified pursuant to Art 8(2).[50] It would appear from the above-cited statement that the Court in fact found a plurality of interferences, one being the storage of the information by the police, another being the disclosure of this information to the naval authorities in connection with their security check on Leander (ie, the word "both" in the above-cited statement is best read in terms of "either ... or"). In both cases, the information and its processing were secret *vis-à-vis* the data subject. The Court did not specifically address the issue of the extent to which it viewed the secrecy of the information and its processing as a necessary element of the two interferences mentioned above.[51] In the light of the *Klass* and *Malone* decisions, it can be argued that the Court would (and should) have found an interference even if the information and its processing were known to the data subject all along: after all, the mere knowledge that one is undergoing

---

43 *Supra* n 34, para 44.

44 *Klass*, *supra* n 41, paras 34 & 41; *Malone*, *supra* n 42, paras 64 & 86.

45 According to Art 25 of the ECHR, a private party may only bring an action before the Strasbourg organs on the basis that he/she/it is a victim of a breach of the Convention. The conditions under which a person may claim victim status without having to prove victimisation "are to be determined in each case according to the Convention right or rights alleged to have been infringed, the secret character of the measures objected to, and the connection between the applicant and those measures": *Klass*, *supra* n 41, para 34. See also paras 64 & 86 of the *Malone* judgment.

46 See *Campbell v United Kingdom* (1992) Series A, No 233, para 33.

47 *Halford*, *supra* n 34, paras 47 & 57. See also *Hilton v United Kingdom* (1988) Appl 12015/86, 57 DR 108, 119. At the same time, the Commission has made clear that, in order for a breach to occur, "it is not necessary that the person actually show that … information has been used to his detriment": *ibid*, 117–118. See also *Hewitt and Harman v United Kingdom* (1989), Appl 12175/86, 67 DR 88, 99.

48 (1987) Series A, No 116.

49 *Ibid*, para 48.

50 In November 1997, however, the Swedish State was revealed to have deliberately misled the Court about the full extent of the surveillance to which Leander was subjected. The State subsequently paid Leander SEK 400,000 as compensation for injustices caused him. See further D Töllborg (ed), *National Security and the Rule of Law*, (Gothenburg: Centrum för Europaforskning, Göteborgs Universitet, 1997), 179–197.

51 The Commission opinion in the case is also ambiguous on the issue, though it seems to treat both the secrecy element and the information content as necessary constituents of the interference(s) occasioned by the processing of the information.

police surveillance will tend to undermine one's ability to lead a private (and public) life of one's own choosing.[52] It is also worth noting the case law on prisoners' correspondence which establishes that interception of a person's communications need not be surreptitious in order to amount to an interference with respect to Art 8(1).[53]

As for the refusal of opportunity to challenge the information (ie, the refusal to lift the veil of secrecy *vis-à-vis* Leander), it is sometimes claimed this amounted to a separate (third) interference.[54] The validity of this claim is, at the very least, questionable. The syntax of the above-cited statement would suggest that the Court viewed the refusal as simply aggravating the interferences occasioned by the storage and release of the information (note especially the wording "which were coupled" as opposed to just "coupled"). So too would subsequent case law.[55] However, a later passage in the judgment could be read as indicating otherwise. At para 66, the Court stated:

"The fact that the information released to the military authorities was not communicated to Mr. Leander cannot by itself warrant the conclusion that the interference was not 'necessary in a democratic society ...', as it is the very absence of such communication which, at least partly, ensures the efficacy of the personnel control procedure ...".

Nevertheless, the apparent link between the term "interference" and the "fact" of non-communication of the information to Leander is far from tight, and the passages preceding this statement seem to link "interference" exclusively to the storage and release of the information. Indeed, the Court's discussion of the denial of opportunity to challenge the information appears to arise only in relation to assessing whether or not such denial robbed the interference incurred by the information's storage and release, of justification under Art 8(2).[56]

The Commission has held that "a security check *per se*" will not amount to an interference with the right to respect for private life pursuant to Art 8(1); an interference will only occur "when security checks are based on information about a person's private affairs".[57] Lustgarten and Leigh interpret the Commission's statement here as "reject[ing] the assertion that compilation and retention of a file … [is] in itself an invasion of privacy".[58] With respect, this interpretation may not be entirely accurate, as the process of carrying out a security check need not always involve establishing a file. Nevertheless, read as a whole, the Commission's statement does seem to deny that the mere establishment of a file is not a sufficient condition for interference, at least in the context of security checks. Other conditions must also be met: the information in the file must be actually applied for the purpose of security clearances and it must contain details about a person's private affairs.

---

52 See also Feldman, *supra* n 39, 271 ("overt surveillance might interfere with the right to respect for private life in some circumstances …").

53 See, eg, *Silver and others v United Kingdom* (1983) Series A, No 61. For an overview of case law on prisoners' correspondence, see FG Jacobs & RCA White, *The European Convention on Human Rights* (Oxford: Clarendon Press, 1996, 2nd ed), 197–204.

54 See, eg, K Eggen, *Vernet om ytringsfriheten etter art. 10 i Den europeiske menneskerettighetskonvensjonen* (Oslo: Universitetsforlaget, 1994), 66 (n 100) & 72; R Schweizer, "Europäisches Datenschutzrecht – Was zu tun bleibt" (1989) *Datenschutz und Datensicherung*, 542, 545.

55 See especially *Gaskin v United Kingdom* (1989) Series A, No 160, para 41, in which the Court describes the interferences in *Leander* as arising only from "compiling, storing, using and disclosing private information about the applicant"; no mention is made of the refusal of opportunity to gain access to the information. However, the *Gaskin* judgment opens up the possibility for arguing that denial of access to the information violated a positive obligation on the Swedish state to ensure "respect" for Leander's Art 8(1) right: see the discussion of the judgment (*infra* section 4.4) in connection with informational access and rectification rights.

56 See paras 58ff.

57 *Hilton*, *supra* n 47, 117.

58 L Lustgarten & I Leigh, *In from the Cold: National Security and Parliamentary Democracy* (Oxford: Clarendon Press, 1994), 150.

Regarding the latter condition, it is important to note that the *Leander* judgment is premised on a finding that the records in question contained information concerning Leander's "private life": in the Commission's words, the information "related to the applicant's acts, associations or opinions and must have been based on an assessment of his behaviour and possibly his personality".[59] The Commission contrasted this situation with a hypothetical case in which all that were recorded were "the name and address of an individual": in such a case, the Commission held, the records "would not normally involve any interference with Article 8 § 1".[60] The Court did not explicitly agree or disagree with the latter statement. It is worth emphasising, though, that the processing of such data does not fall outside the ambit of data protection laws – and for good reason, as even data of ordinarily trivial significance can be used in certain contexts to the detriment of the data subjects.

Fortunately, the Court's decision in *Malone* indicates that some data of ordinarily trivial character may be processed in ways that are found to interfere with the data subject's right under Art 8(1). The *Malone* judgment concerned, *inter alia*, the secret disclosure to the police of certain data obtained from the "metering" of Malone's telephone by the British telecommunications authority.[61] The Court found Malone's right under Art 8 to be interfered with by this disclosure. At para 84 of its judgment, the Court ruled:

"The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts ... to an interference with a right guaranteed by Article 8".

It is not entirely clear whether the Court assumed the metering data to be related to Malone's "private life" or simply part of his "correspondence". Either assumption would be justifiable.[62]

The Court also left open the issue of whether or not the practice of metering in itself could be an interference with respect to Art 8(1). In this case, interference was found on the basis of the *non-consensual disclosure* of the metering data to the police. The Commission's above-cited statement in the *Hilton* case[63] would indicate that metering in itself (as opposed to the subsequent use/disclosure of the metering data) could not be sufficient to constitute an interference. Even if we put the Commission's statement in *Hilton* aside, metering would probably only contravene Art 8(1) if the telephone user has a reasonable expectation that such activity does not occur. The notion of "reasonable expectation" was used in *Halford* as a criterion for determining whether or not tapping of the applicant's office telephone contravened Art 8(1). In concluding that the tapping did contravene Art 8(1), the Court laid decisive weight on the fact that the applicant was never given any warning about the possibility of tapping and was, accordingly, able to "have had a reasonable expectation of privacy for … [her] calls".[64] Thus, if the practice of metering is brought to the attention of a telephone user or is otherwise common knowledge (which will often be the case),[65] it will not interfere with the telephone user's right under Art 8(1).

---

59 *Leander v Sweden* (1987) Series B, No 99, para 56.

60 *Id.*

61 "Metering" denotes the registration of data on telephone usage, including numbers dialled and the time and duration of each call, but not the call's content: see *Malone*, *supra* n 42, para 56.

62 In this respect, note *Klass*, *supra* n 41, para 41, in which the Court held that a person's telephone communications are covered by both the notions of "private life" and "correspondence" in Art 8(1).

63 *Supra* n 47.

64 *Halford*, *supra* n 34, para 45.

65 Indeed, telecommunications service providers in the European Union will be *legally* required (pursuant to Art 10 of the EC Directive on data protection) to notify telephone users of what call data are registered.

In a separate, concurring opinion in the *Malone* judgment, Judge Pettiti suggested that the mere application of metering data for purposes other than "accounting" would be sufficient to constitute interference.[66] Here, Pettiti appears to have drawn on the principle of purpose specification laid down in, *inter alia*, Art 5(b) of the CoE Convention on data protection. Pettiti's colleagues, however, failed to signal support for his view on this point. Nevertheless, his view has much to commend it, though what should be upheld here is not so much the purpose specification principle as such but the interests that the principle appears to safeguard. One can read into the principle, together with the principle of use limitation, a concern to ensure, *inter alia*, that personal data are processed in conformity with the reasonable expectations of the data subjects. In other words, the two principles are grounded in a respect for these expectations and, indirectly, a respect for the data subjects' integrity. If this view is accepted, it can scarcely be held that Art 8(1) rights do not require, as a point of departure, personal data to be processed in conformity with the two principles.

Both principles figure in the Court's recent judgment in *MS v Sweden*.[67] The case concerned the communication by a hospital, without the applicant's consent, of medical data on the applicant to the Swedish Social Insurance Office so that the latter could settle a compensation claim by the applicant. The Court found the communication to be an interference with the applicant's right under Art 8(1) but held it justified under Art 8(2). In finding interference, the Court stated:

"Although the records remained confidential, they had been disclosed to another public authority and therefore to a wider circle of public servants …. Moreover, whilst the information had been collected and stored at the clinic in connection with medical treatment, its subsequent communication had served a *different purpose*, namely to enable the Office to examine her [the applicant's] compensation claim. It did not follow from the fact that she had sought treatment at the clinic that she would consent to the data being disclosed to the Office …."[68]

From this statement, it is apparent that the Court did not view the "re-purposing" of the medical data as solely constitutive of the interference; rather, the Court seems to have placed primary weight on the factor of consent, with the "re-purposing" of the data serving merely to establish the parameters of the consent. Nevertheless, the Court was apparently alert to, and respectful of, the applicant's reasonable expectations as to what would happen with the data, inasmuch as the parameters of the applicant's consent reflected the parameters of these expectations. Also noteworthy was the Court's rejection of an argument by the Swedish government that the applicant, by applying for compensation from the Social Insurance Office, had waived her right to confidentiality with regard to the medical data. According to the government, the applicant should have known that the Office would legally be required to request the data from the hospital and that the latter would have to comply with the request. The Court sensibly held that since it was exclusively up to the Office to assess which data would need to be communicated, and that since the applicant had no right to be notified or consulted about this assessment beforehand, the applicant's request for compensation could not be interpreted as unequivocally waiving her right to the privacy of the medical records.[69]

The registration of data on a person taken into custody, and the retention of these data after the person's release, may interfere with his/her right to respect for private life under Art 8(1). The leading case on this point is *Murray v United Kingdom*.[70] In this case, the Court was

---

66 *Ibid*, 47.
67 (1997) Reports 1997-IV, 1437.
68 *Ibid*, para 35 (emphasis added).
69 *Ibid*, para 32.
70 (1994) Series A, No 300-A.

called upon to consider, *inter alia*, the lawfulness of military authorities' registration and continued storage of information on a woman who had been arrested for alleged involvement in terrorist activities, but released after a short interrogation. During the interrogation, the authorities had photographed the woman and registered other information on her, all without her consent. The Court (along with the Commission) had little difficulty in finding both the recording and retention of this information (including the photographs) as interferences with the woman's right to respect for private life under Art 8(1).[71] However, the interference was found to be justified pursuant to Art 8(2).

The decision in *Murray* can be contrasted with earlier opinions of the Commission which demonstrate greater reluctance to find an interference with respect to Art 8(1) in situations where police record and retain information on arrested persons. An example here is *X v United Kingdom*,[72] a case in which police photographed the applicant upon her arrest for participating in a political demonstration. The photographs were taken without her consent and stored by the police for future identification of the woman should she become involved in subsequent unlawful demonstrations. The Commission held that these measures did not constitute an interference with the applicant's rights under Art 8(1). The exact grounds for this decision are unclear, though a central factor was that, in the Commission's view, "the taking of her photographs was part of and solely related to her voluntary public activities".[73] The decision may be criticised not just for its ambiguity but also for its failure to problematise the fact that the photographs were taken without the applicant's consent and revealed aspects of the applicant's political persuasion, information on which is typically regarded as sensitive.[74] In the opinion of some scholars, the above decision may well be an outdated aberration in the case law of the Strasbourg organs.[75] Certainly, in the light of the problems of the decision identified above, there are good grounds for holding that it ought to be accorded little weight in present and future interpretation of Art 8(1). There is, however, no case law directly overruling the decision. The *Murray* judgment, for instance, does not directly overrule it, as the applicant in *Murray* was not arrested and photographed on account of voluntarily participating in public activities. And, in the recent case of *Friedl v Austria*,[76] the Commission did not explicitly distance itself from the approach it took in the decision.

In *Friedl*, the Commission refused to find that the photographing of the applicant by police whilst he took part in a public demonstration, along with the subsequent retention of the photographs, interfered with the applicant's right to respect for private life under Art 8(1). In reaching this finding, the Commission laid weight upon the same three kinds of factors as those mentioned in *X v United Kingdom*.[77] At the same time, it also attached weight to assurances that the photographs taken "remained anonymous in that no names were noted down, the ... photographs taken were not entered into a data-processing system, and no action

---

71 Indeed, the point was not even contested: *ibid*, para 86; see also para 79 of the Commission report, annexed to the Court judgment.

72 (1973) Appl 5877/72, 16 *Yearbook of the European Convention on Human Rights*, 328.

73 *Ibid*, 338. The Commission listed two other factors too, but without indicating clearly their relative weight. These factors were (i) that the applicant had not been photographed in her own home but in a public area, and (ii) that the photographs would not be disclosed to the general public but kept by the police solely for the purposes of future identification of the applicant.

74 See, eg, Art 6 of the CoE Convention on data protection (listing personal data that reveal "political opinions" as a "special category" of data in need of extra protection).

75 Falck, *supra* n 39, 35; LA Rehof & T Trier, *Menneskerett* (Copenhagen: Jurist- og Økonomforbundets Forlag, 1990), 193, n 34. Cf D Gomien, D Harris & L Zwack, *Law and Practice of the European Convention on Human Rights and the European Social Charter* (Strasbourg: Council of Europe, 1996), 231, where the case is cited uncritically as authority for the proposition that "[w]hatever the state's intended use for ... collected information might be, the Convention organs will not find any interference under Article 8(1) if the individual has placed himself or his activities in the public domain". With respect, the premises of the case decision are too uncertain and narrow to support such a broad proposition.

76 (1995) Series A, No 305-B (not treated by the Court on the merits due to friendly settlement).

77 *Ibid*, paras 49–50 of the Commission's opinion.

was taken to identify the persons photographed".[78] In this respect, the Commission could be interpreted as either introducing additional criteria to be met in such cases (thus implying that the outcome of *X v United Kingdom* is problematic on account of the fact that the applicant's anonymity in that case was not assured *vis-à-vis* the police) or as simply underscoring the fact that future use of the photographs would not of itself compromise the privacy of the data subject *vis-à-vis* the general public. In any case, interference with respect to Art 8(1) was found to have been incurred by the police's questioning of the applicant and recording of his personal details (independent of the photographs).[79] But the Commission characterised this interference as "relatively slight",[80] and had little trouble in finding it justified pursuant to Art 8(2).

Interference of a more serious character (at least in the view of the Commission) was found to have occurred in the case of *Chave née Jullien v France*.[81] Here the Commission was called upon to consider a refusal by French authorities to accede to a request by the applicant that her name and personal particulars be deleted from a register over persons who suffered from psychiatric illness. The request was made in the wake of a court action in which it had been found that the applicant's compulsory confinement in a psychiatric hospital had been illegal. Citing the *Leander* judgment as support, the Commission held that the storage of the information in question could amount to interference with her right to respect for private life under Art 8(1). Characteristically, the Commission was somewhat imprecise when specifying exactly what constituted the interference: was it the initial registration of the disputed information or the continued storage of the information subsequent to the applicant's release from illegal confinement? And how significant was the factor of consent (or, rather, non-consent)?[82] The Commission referred simply to "the storing" of the information as constitutive of the interference.[83] But, given the importance of the (non-)consent factor in other case law, there are strong grounds for arguing that the Commission viewed the interference as being occasioned not by "the storing" *per se* of the information but by its *non-consensual* storing. In any case, there is little doubt that the Commission viewed the interference as fairly serious.[84] Nevertheless, the Commission went on to find it justified pursuant to Art 8(2).

Finally, mention should be made of two other cases which have particular relevance for data protection and which, like *Chave née Jullien*, do not directly concern state security or crime control. The first of these cases is *Lundvall v Sweden*,[85] in which the Commission held that the applicant's right to respect for private life under Art 8(1) was interfered with by his registration in a public register over defaulting taxpayers when there was pending an appeal against his tax assessment. To quote the Commission:

---

78 *Ibid*, para 51 of the Commission's opinion.

79 *Ibid*, para 53 of the Commission's opinion.

80 *Ibid*, para 67 of the Commission's opinion. Cf *McVeigh, O'Neill and Evans v United Kingdom* (1981) Appl 8022/77, 8025/77 & 8027/77, 25 DR 15, which concerned the lawfulness of the searching, questioning, fingerprinting and photographing of the applicants during their temporary detention by police. The Commission found that interference with their Art 8(1) rights was occasioned by "some at least" of the disputed measures, but did not go into more detail: *ibid*, 49. The Commission found it "open to question" as to whether the police retention of the records after the applicants' release from custody also constituted an interference but commented that if it did, it would be "at most ... relatively slight": *ibid*, 50–51.

81 (1991) Appl 14461/88, 71 DR 141.

82 The Commission did not specifically mention the consent factor, but it seems reasonable to assume that the initial registration of information, in addition to its retention after the applicant's release, was done without the consent of the applicant, given that her confinement was compulsory.

83 *Ibid*, 155.

84 In the words of the Commission, "[t]he interference complained of was all the more serious because it concerned information relating to the applicant's compulsory placement in a psychiatric hospital the illegality of which was recognised in a judgment of the Paris Court of Appeal ... It caused the applicant distress which was all the more keenly felt because she was well-known in Carpentras, where she had worked as a teacher": *ibid*, 156.

85 (1985) Appl 10473/83, 45 DR 121.

"the fact that the applicant was registered in a register on taxes in arrears, a tax which was based on an assessment and still subject to appeal, and that this register became public and available *inter alia* to credit information companies, can as such be regarded as an interference ...".[86]

It seems from this statement that the Commission viewed the interference as being essentially occasioned by the public disclosure of potentially inaccurate personal information. But, given that the data subject apparently had not consented to the registration and disclosure, it is, once again, arguable that the (non-)consent factor was an implied, necessary precondition for the Commission's finding of interference. In contrast to *Chave née Jullien*, the Commission viewed the interference as "minor".[87] Not surprisingly, the interference was found to be justified under Art 8(2) as lawful and necessary "*inter alia* for the economic well-being of the country and for the protection of the rights and freedoms of others".[88]

In the same case, the Commission observed that the use of personal identity numbers is not expressly or implicitly prohibited by any provision in the Convention.[89] Nevertheless, the Commission added that it is "conceivable that the use of personal identity numbers as a way of storing data in different registers and the matching of such registers could raise an issue under Article 8 of the Convention".[90] The Commission did not elaborate on this last comment. It shows, however, that the Commission is aware of the privacy-invasive potential of matching and exchange of personal data. It also signals a preparedness to give serious consideration to future applications centering on data-matching practices. We are given no hint, though, as to why data-matching practices might interfere with the right to respect for private life under Art 8(1). On the basis of previous case law, the Court is most likely to judge such practices as interfering with the right to respect for private life when the matching occurs without the consent of the data subjects and/or, by implication, when the matching occurs contrary to the data subjects' reasonable expectations. It could also be argued that matching practices ought to be judged as problematic in the context of Art 8(1), independent of the factors of consent and expectations: after all, such practices tend to increase the transparency of data subjects *vis-à-vis* other persons and organisations – a development that can threaten, in turn, the bases for democratic, pluralist society.

The second case is *X v United Kingdom*,[91] which concerned a compulsory public census carried out in the UK in 1981. In this case, the Commission held that:

"a compulsory public census, including questions relating to the sex, marital status, place of birth and other personal details of the inhabitants of a particular household may constitute a *prima facie* interference with the right guaranteed by Article 8, paragraph 1 of the Convention to respect for private and family life, which falls to be justified under the terms of Article 8, paragraph 2 …".[92]

The Commission's statement fails to clarify the degree to which interference was occasioned by the *compulsory* nature of the census as opposed to the simple registration of personal details. Given the other case law of the Commission and the Court in which the (non-)consent

---

86 *Ibid*, 131.

87 *Id.* In reaching this view, the Commission emphasised that taxes in Sweden are legally required to be paid even if they are subject to subsequent appeal, and that Sweden has a long-standing Constitutional principle of making official documents available to the public.

88 *Id.*

89 *Ibid*, 130.

90 *Id.*

91 (1982) Appl 9702/82, 30 DR 239.

92 *Ibid*, 240.

factor is prominent, the interference was most likely seen by the Commission as partially occasioned by the compulsory (ie, non-consensual) registration of the data. In other words, without the element of compulsion it is doubtful that the registration of the data would have been sufficient to interfere with the right to respect for private and family life under Art 8(1).

To sum up, the case law on Art 8(1) presented above is considerable but somewhat confusing. The confusion arises largely because of the frequent failure by the Commission and Court to indicate exactly which elements of the contested data-processing practices have constituted an interference with respect to Art 8(1). Nevertheless, some fairly stable guidelines do emerge. Thus, it appears that whether or not the collection, registration or other processing of personal data will incur an interference with the right under Art 8(1) will depend on a consideration of various factors, the most important of which are: (i) the nature of the data in question (eg, to what extent do the data concern "private life"?); (ii) the manner in which the data are processed (eg, are they processed with the knowledge or consent of the data subject?); and (iii) the context for the data processing (eg, are the data found in a register that allows potentially negative assessments to be made of the data subject's character?). Generally speaking, interference is likely to be found when the data in question reveal details about the data subject's personality (eg, his/her preferences), are processed without the latter's knowledge or consent, *and* the processing potentially casts the data subject in a negative light or could result in a restriction of the data subject's freedom of choice. These principles would seem to apply regardless of whether the information is processed automatically or manually.

At the same time, sight should not be lost of the possibility that some data-processing activities could constitute an interference even if they are consented to by the data subjects. However, this possibility has not yet been squarely addressed by the Strasbourg organs.

The fact that a person is denied an opportunity to gain access to, and challenge the validity of, data on him/her kept by others, would seem ordinarily not to constitute an interference. Denial of such an opportunity, though, may be in breach of a state's positive obligations under Art 8(1).[93] Denial of such an opportunity may also aggravate the seriousness of an interference incurred by the processing of the data.

In general, the gravity of an interference will tend to be lessened the more the data processing in question occurs with the knowledge of the data subject, accords with the data subject's reasonable expectations, anonymises the data subject's identity, or relates to public activities voluntarily entered into by the data subject. Other factors may also play a role.

In light of the above, the major point of difference between the basic principles of data protection laws and the case law regarding what is an interference with respect to Art 8(1) is that whereas the former usually cover the processing of all data from which individual persons can reasonably be identified, the latter leaves open the possibility that some such data (ie, those that do not relate to a person's "private life") will fall outside the protective ambit of Art 8. Fortunately, though, this possibility has been cut back somewhat by the Strasbourg organs' preparedness to interpret the notion of "private life" in a fairly broad, open-ended way.

### *4.3. Justification under Article 8(2)*

Most instances of interference with respect to Art 8(1) by state authorities' collection, storage or other processing of personal data have been held by the Strasbourg organs as justified under Art 8(2). Indeed, the Commission has sometimes skipped taking a conclusive view on whether or not the action complained of has been an interference with an Art 8(1) right, by

[93] See further section 4.4 below.

finding justification in Art 8(2) for the putative interference.[94] It is, therefore, important to describe the scope of Art 8(2), as interpreted by the Court and the Commission.

Article 8(2) sets out three main criteria for justifying an interference with a person's right under Art 8(1). The interference must be: (i) "in accordance with the law"; (ii) "necessary in a democratic society"; and (iii) in furtherance of at least one of the aims listed in paragraph 2 (ie, "national security", "public safety", "economic well-being of the country", "prevention of disorder or crime", "protection of health or morals" or "protection of the rights and freedoms of others").

The requirement that an interference be "in accordance with the law" means that there must be some sort of legal basis for the interference. This basis does not have to be found in statutes; it may also be found in rules made pursuant to delegated powers, or in judicial practice.[95] In addition, the legal measure concerned must be of a certain quality that satisfies the ideals of "rule of law"; that is, it must be accessible to the person concerned and sufficiently precise to allow the person reasonably to foresee its consequences.[96] Thus, the legal measure "must indicate the scope of any ... discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity ... to give the individual adequate protection against arbitrary interference".[97]

As a general rule, the stringency of the above requirements of the quality of a legal measure will be linked to the seriousness of the interference with the right under Art 8(1). For instance, the Court emphasised in *Kruslin* that

"interception of telephone conversations represent[s] a serious interference with private life and correspondence and must accordingly be based upon 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".[98]

At the same time, it has also been held that the requirement of foreseeability may be relaxed for the purposes of police investigations and the safeguarding of national security. As the Court stated in para 67 of its judgment in *Malone*,

"the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly".

---

94 See, eg, *X v Federal Republic of Germany* (1962) Appl 1307/61, 9 *Collection of Decisions of the European Commission of Human Rights* (hereinafter "CD") 53 (concerning police retention of records on applicant's previous criminal convictions); *X v Federal Republic of Germany* (1963) Appl 1216/61, 11 CD 1 (regarding police seizure of applicant's files during investigation of his criminal activities); *X v Federal Republic of Germany* (1973) Appl 5339/72, 43 CD 156 (on disclosure in open court of sexually explicit photographs of the applicant, during his criminal trial); *X v Austria* (1979) Appl 8170/78, 16 DR 145 (concerning collection of information on applicant as a child and subsequent use of this information in criminal proceedings against him); and *X v Norway* (1978) Appl 7945/77, 14 DR 228 (on disclosure in open court of applicant's criminal record).

95 See, eg, *Kruslin v France* (1990) Series A, No 176-A, para 29; *Huvig v France* (1990) Series A, No 176-B, para 28.

96 *Sunday Times v United Kingdom* (1979) Series A, No 30, para 49; *Malone*, *supra* n 42, paras 66–68. See, eg, *Silver v United Kingdom* (1983) Series A, No 61, in which parts of the legal regime for the screening of prisoners' correspondence in the UK were found not to satisfy the "accessibility" requirement.

97 *Malone*, *supra* n 42, para 68.

98 *Kruslin*, *supra* n 95, para 33; *Huvig*, *supra* n 95, para 32.

Similar statements on the foreseeability requirement in the context of vetting prospective employees for national security purposes have been made by the Court in para 51 of its *Leander* judgment.

Nevertheless, the outcome of cases such as *Malone*, *Kruslin* and *Huvig* show that the Court may still find that the quality of the legal measures relied upon by the state party concerned are inadequate to justify police telephone-tapping practices pursuant to Art 8(2). In *Kruslin* and *Huvig*, for instance, serious deficiencies were identified with the quality of French law regulating the surreptitious tapping of telephones by the police. The Court pointed out, *inter alia*, that the law failed to specify safeguards against possible abuses of the telephone-tapping system. There were, for instance, insufficiently detailed rules defining whose telephones should be tapped and under which circumstances, and the conditions upon which the recordings should be destroyed.[99] The judgments in these cases highlight that when interference with rights under Art 8(1) is serious, there is a need for comprehensive regulation of the activities that incur the interference. With regard to surreptitious telephone tapping, it would seem necessary to have fairly detailed rules specifying *when* tapping is permitted, *who* has competence to permit it and to carry it out, *how* the tapping is to be conducted, for *what purposes* its results may be applied and for *how long* the resulting information may be kept.[100]

The above judgments raise the question of whether or not equally comprehensive rules are required under Art 8(2) for other forms of processing personal data. It is obvious that equally comprehensive rules would be required for other forms of data processing which involve, in the opinion of the Court, an equally serious interference with an Art 8(1) right as surreptitious telephone tapping involves. As for data processing incurring less serious forms of interference, the answers must be partly speculative since it is sometimes difficult to determine exactly how serious the Court or Commission has judged an interference to be. Some idea of what the Court requires may be gathered from case law assessing the necessity – or, more particularly, the proportionality – of a given interference with an Art 8(1) right. This case law is described further below. Ideally, the principles in the CoE Convention on data protection, as developed in the Council's various sectoral recommendations in the field, should be viewed as constituting a model set of basic rules for all processing of personal data, but the Strasbourg organs have rarely made express reference to these.

In order to be justified under Art 8(2), the interference must not only have a sufficient legal basis; it must also have been carried out in order to achieve one or more of the aims listed in paragraph 2. In cases where the interference has been incurred by the processing of personal data, the Strasbourg organs have rarely found that the processing has not been in pursuance of at least one of these aims.

Greater dispute has often arisen over the requirement that the interference in question be "necessary in a democratic society". The criterion of necessity has been interpreted by the Strasbourg organs as satisfied when the interference "corresponds to a pressing social need"

---

[99] *Kruslin*, *supra* n 95, para 35; *Huvig*, *supra* n 95, para 34. The latest case (as of June 1998) in which the Court has found legal measures inadequate to justify telephone tapping is *Kopp v Switzerland*: see judgment of 25.3.1998, available over the Internet via URL <http://www.dhcour.coe.fr>, otherwise unpublished as yet. Here, case law permitting the tapping of a lawyer's telephone communications was found not to delineate sufficiently clearly the circumstances in which such tapping could occur in the face of relatively clear statutory rules on legal professional privilege. The Court also criticised the lack of judicial supervision of the process of determining which elements of the applicant lawyer's communications fell outside the scope of this privilege: *ibid*, paras 73–75.

[100] In his separate but concurring opinion in *Malone*, Judge Pettiti claimed that it is also necessary, even in the case of "justified and properly controlled telephone interceptions", to provide the data subjects with rights of access and erasure in relation to the interception records, once the data subjects have been cleared of suspicion: *Malone*, *supra* n 42, 45. Pettiti appears to have partly derived these requirements from the provisions and spirit of the CoE Convention on data protection: *ibid*, 46. However, Pettiti's views here did not receive explicit endorsement from the other members of the Court in the *Malone* case. Neither did the Court make any mention of a need for access and erasure rights in its *Kruslin*, *Huvig* and *Kopp* judgments. Such rights were available, though, in the latter case, and were regarded by the Court as being of "value": *Kopp*, *supra* n 99, para 72.

and is "proportionate to the legitimate aim pursued".[101] In applying the necessity criterion, the Court and the Commission accord state parties a "margin of appreciation", allowing the judgment of what is necessary in the circumstances of the particular case to be determined to some extent by the national authorities. The extent of this margin of appreciation varies from case to case and depends on the Strasbourg organs' appraisal of a variety of factors. These include the seriousness of the interference with the right concerned, the importance of this right, the importance of the "legitimate aim" for the interference, and the conformity of the interference to a relevant pan-European practice.[102]

In cases involving surreptitious surveillance of persons, the Court has viewed the criterion of necessity more stringently than in other cases. According to the Court in *Klass*:

"Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only insofar as *strictly* necessary for safeguarding the democratic institutions".[103]

At the same time, the Court has held that when the aim of such surveillance is to safeguard national security (as it often is), the margin of appreciation available to state parties in assessing what is necessary for fulfilling that aim is wide.[104] It could be argued, though, that in cases involving the processing of personal data for *other* purposes, the existence of a large body of European data protection laws based on common principles is a factor that would tend to reduce state parties' margin of appreciation.[105]

In assessing the necessity/proportionality of a data-processing operation that interferes with an Art 8(1) right, the Strasbourg organs pay regard to the nature of the data in question. Generally speaking, the more intimate or sensitive the data are judged to be, the more stringent will be the application of the necessity/proportionality criterion. For example, in *Z v Finland*[106]– a case concerning the non-consensual disclosure of information on the applicant's HIV status in the course of court proceedings against her husband – the Court stated:

"In view of the highly intimate and sensitive nature of information concerning a person's HIV status, any State measures compelling communication or disclosure of such information without the consent of the patient call for the *most careful scrutiny* on the part of the Court, as do the safeguards designed to secure an effective protection".[107]

In this case, the Court found that Art 8 was violated firstly by the Finnish courts' decision to place the HIV-status information under a confidentiality order of only ten years (despite the applicant's wish for a longer period), and secondly by the disclosure of the applicant's name and medical condition in the appeal court's published judgment. The Court had little trouble in deciding that both actions failed to meet the necessity/proportionality criterion, in light of the sensitive nature of the data.[108]

---

[101] See, eg, *Leander*, *supra* n 48, para 58. Cf the minimality principle in data protection laws as defined in the Introduction to the paper. An example of legal manifestation of this principle is Art 6(1)(c) of the EC Directive on data protection which provides, *inter alia*, that personal data must be "not excessive" in relation to the purposes for which they are processed.

[102] For a detailed discussion of these and other factors, see, eg, Harris *et al*, *supra* n 26, 290–301, 344–353.

[103] *Klass*, *supra* n 41, para 42 (emphasis added).

[104] *Leander*, *supra* n 48, para 59.

[105] On this point, see Falck, *supra* n 39, 70. See also Judge Pettiti's opinion in *Malone*: "the right to respect for private life against spying by executive authorities comes within the most exacting category of Convention rights and hence entails a certain restriction on ... domestic 'discretion' and on the margin of appreciation. In this sphere ... it is possible ... to identify European standards of State conduct in relation to surveillance of citizens. The shared characteristics of statutory texts or draft legislation on data banks and interception of communications is evidence of this awareness": *Malone*, *supra* n 42, 47.

[106] (1997) Reports 1997-I, 323.

[107] *Ibid*, para 96.

[108] The Court also expressed doubt that the purpose of the second-mentioned action could satisfy any of the "legitimate aims"

When assessing the necessity/proportionality of a given interference with an Art 8(1) right, the Strasbourg organs also pay regard to the existence or otherwise of sufficient safeguards against abuse of the measure(s) leading to the interference:

"The court must be satisfied that, whatever system of surveillance is adopted, there exist adequate and effective guarantees against abuse. This assessment has only a relative character: it depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the national law".[109]

To a great extent, this assessment is similar to, and overlaps with, the assessment of the quality of the legal basis for the interference (see above).

One safeguard is the existence of rules to ensure data confidentiality.[110] This safeguard is seen as especially important with respect to medical data:

"[t]he protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention".[111]

Interestingly, the Court recognises that confidentiality of health data is important not just in order to respect the patient's privacy but also for wider policy reasons to do with preserving public confidence in medical services and, ultimately, preserving community health.[112] At the same time, it goes without saying that the need for confidentiality measures extends to other types of data as well. For example, in *X v United Kingdom* (on the lawfulness of a compulsory public census), the Commission held that "where the information gathered by the census is treated with care and confidentiality, the interference thereby occasioned with the applicant's right to respect for his private and family life is necessary in a democratic society".[113]

Another safeguard that is often emphasised in the case law is the existence of an independent control body to monitor activities contravening Art 8(1). Thus, searches of persons' homes conducted by state authorities in order to enforce criminal law, are likely to require prior court authorisation.[114] Such authorisation, however, is not a sufficient condition

---

listed in Art 8(2): *ibid*, para 78. As for the first-mentioned action, the Court accepted this could be aimed at protecting the "rights and freedoms of others" but not the "prevention of crime": *ibid*, para 77.

109 *Klass*, *supra* n 41, para 50.

110 Cf the security principle in data protection laws as defined in the Introduction to the paper; see also *supra* n 16.

111 *Z v Finland*, *supra* n 106, para 95. See also *MS v Sweden*, *supra* n 67, para 41. See also *Chave née Jullien*, *supra* n 81, 156, where the Commission stressed that the information in question was "protected by the appropriate confidentiality rules". Similarly, in *T V v Finland* (1994) Appl 21780/93, 76-A DR 140, the Commission found that disclosure to prison staff of the fact that a prisoner was HIV-positive was justified in a situation where the staff must observe a strict duty of confidence in relation to such information.

112 "Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community": *Z v Finland*, *supra* n 106, para 95.

113 *X v United Kingdom*, *supra* n 91, 241.

114 See, eg, *Funke v France* (1993) Series A, No 256-A, especially para 57 (search-and-seizure operation directed at applicant's house by French customs authorities held not to be justified under Art 8(2) on account of, *inter alia*, lack of prior court approval of operation).

for the search to be deemed justified under Art 8(2);[115] neither will it always be a necessary condition.[116]

With regard to secret surveillance systems involving, for example, the interception of citizens' communications, the Court has held that supervision should, "in principle", be entrusted to the judiciary.[117] The Court has also stated that, on the basis of the "rule of law", *any* interference by the executive with a person's rights "should normally be assured by the judiciary, at least in the last resort", since the judiciary offers "the best guarantees of independence, impartiality and a proper procedure".[118] But in both *Klass* and *Leander*, the Court accepted non-judicial systems for the control of secret surveillance activities, on the ground that the control systems were sufficiently autonomous of the authorities responsible for surveillance and had sufficiently effective powers. The Court appears to have been especially impressed by the participation of parliamentary bodies in the control systems concerned.[119] At the same time, the Strasbourg organs have rarely acknowledged that the existence of privacy/data protection commissioners may be significant for determining the extent to which the necessity criterion is satisfied. No doubt this is due partly to the fact that much of the Art 8 case law centers upon the activities of police and national security agencies, the regulation of which often falls outside the competence of privacy/data protection commissioners.

In neither *Klass* nor *Leander* did the Court require as a safeguard that authorities notify data subjects of surveillance measures, either before or after surveillance takes place.[120] In the Court's view, such a notification requirement would have been incompatible with the efficacy and purpose of the surveillance. In such a situation, it appears also that a requirement of notification may not be read into Art 13 of the Convention which guarantees victims of violations of the Convention "an effective remedy before a national authority".[121] Even in other contexts, there is a dearth of case law promoting as a necessary or desirable safeguard that persons be given a right of access to information kept on them in order that they may verify or challenge the accuracy of the information (see below). There is also a dearth of case law promoting as a necessary or desirable measure that such information be erased after the expiry of a certain period or after its storage is no longer necessary relative to the purposes for which it was originally registered.[122]

To sum up, the case law above sets out a multiplicity of hurdles that must be cumulatively cleared before an interference with an Art 8(1) right may be regarded as justified pursuant to Art 8(2). Though great in number, however, none of these hurdles has proved

---

115 See, eg, *Niemitz v Germany* (1992) Series A, No 251-B (police search-and-seizure operation directed at applicant's business premises held not to be justified despite existence of prior judicial warrant).

116 In the *Funke* case, for example, it appears that the Court might have accepted the French regulatory regime in dispute, but for the fact that the rules operating in the the absence of judicial warrants were "too lax and full of loopholes for the interferences ... to have been strictly proportionate to the legitimate aim pursued": *Funke*, *supra* n 114, para 57.

117 *Klass*, *supra* n 41, para 56.

118 *Ibid*, para 55.

119 *Ibid*, para 56; *Leander*, *supra* n 48, para 65. See also *L v Norway* (1990) Appl 13564/88, 65 DR 210 (acceptance by Commission of control system whereby police tapping of telephones is subject to prior authorisation by court but *ex post facto* review of tapping is undertaken by non-judicial body); *Mersch and Others v Luxembourg* (1985) Appl 10439/83, 10440/83, 10441/83, 10452/83, 10512/83 & 10513/83, 43 DR 34 (acceptance by Commission of control system in which police surveillance of communications to be first authorised by non-judicial body but where *ex post facto* review by a court possible). In the two latter cases, the non-judicial bodies in question were found by the Commission to afford guarantees of impartial control similar to the guarantees afforded by ordinary courts of law.

120 *Leander*, *supra* n 48, para 66; *Klass*, *supra* n 41, para 58. The same line has been taken by the Commission in *Mersch*, *supra* n 119; *MS & PS v Switzerland* (1985) Appl 10628/83, 44 DR 175; *Spillmann v Switzerland* (1988) Appl 11811/85, 55 DR 182; and *L v Norway*, *supra* n 119.

121 *Klass*, *supra* n 41, para 68. See also *Mersch*, *supra* n 119, 118.

122 Cf the Commission opinions in *Friedl v Austria*, *supra* n 76, para 67 and *McVeigh, O'Neill and Evans v United Kingdom*, *supra* n 80, 50–51 where the Commission indicates – albeit indirectly – that personal data gathered by police for the purpose of investigating a crime should be destroyed after the data subject is no longer suspected of having committed the crime, unless special considerations require otherwise.

especially difficult to jump with respect to most of the interferences occasioned by the collection or other processing of personal data. The most difficult hurdles have been the requirements read into the phrases "in accordance with the law" and "necessary in a democratic society". These are likely to be the most difficult hurdles in the future as well. But, where all or most stages of the contested data-processing activity are subject to detailed regulation in accordance with the basic principles of data protection laws, it is safe to assume these hurdles will normally be cleared.

### *4.4. Access and rectification rights under Art 8*

The leading case on a person's right of access under Art 8 to information on him-/herself kept by a public authority is *Gaskin v United Kingdom*.[123] The applicant in this case complained about the refusal of a local authority to allow him access to confidential records kept on him during the period he spent as a teenager in the authority's foster-care. The authority's practice was to grant access only upon the consent of the persons who were responsible for contributing the information in question. No system was in place by which an independent body could hear and determine appeals against denial of access. Against this background, the Court ruled that the state had violated its obligations under Art 8:

"In the Court's opinion, persons in the situation of the applicant have a vital interest, protected by the Convention, in receiving the information necessary to know and to understand their *childhood* and *early development*. On the other hand, it must be borne in mind that confidentiality of public records is of importance for receiving objective and reliable information, and that such confidentiality can also be necessary for the protection of third persons. Under the latter aspect, a system like the British one, which makes access to records dependent on the consent of the contributor, can *in principle* be considered to be compatible with the obligations under Article 8, taking into account the State's margin of appreciation. The Court considers, however, that under such a system the interests of the individual seeking access to records relating to his private and family life must be secured when a contributor to the records either is not available or improperly refuses consent. Such a system is only in conformity with the principle of proportionality if it provides that an *independent authority* finally decides whether access has to be granted in cases where a contributor fails to answer or withholds consent".[124]

It is clear from this judgment that Art 8(1) protects a person's interest in gaining access to certain types of information concerning him-/herself, but that the degree to which state authorities must secure this interest will depend on the importance of the information for the applicant's private and family life.

The right of access established in *Gaskin* arises as a "positive" obligation on the state party; for the Court, the failure by British authorities to grant the applicant full access to his case records was not an "interference" with the applicant's rights under Art 8(1) but a breach of the authorities' positive obligation to secure respect for those rights.[125] Accordingly, the Court did not find it strictly necessary to apply Art 8(2). In drawing the extent of positive obligations deemed necessary in the case, the Court stated that: (i) a "fair balance" has to be struck between the interests of the community and those of the individual; (ii) regard must be

---

[123] (1989) Series A, No 160.

[124] *Ibid*, para 49 (emphasis added). Cf *X v Austria* (1974) Appl 5416/72, 46 CD 88, in which the Commission held that the applicant was not entitled under Art 8 to be given information on the welfare of his daughter after losing custody of her.

[125] *Ibid*, para 40. The Commission, however, treated the refusal to allow access as an "interference" with the applicant's Art 8(1) right which fell to be justified pursuant to Art 8(2).

had to the margin of appreciation enjoyed by a state party when striking this balance; and (iii) the aims listed in Art 8(2) "may be of a certain relevance" in the balancing process.[126]

One should be cautious when drawing conclusions about the general applicability of the outcome in *Gaskin*.[127] The information at dispute in the case was found to be of special importance for the psychological well-being and identity of the applicant, such that a refusal of access to it would seriously hinder the applicant's personal development. Thus, the case should not be seen as establishing a right of access which covers all sorts of personal data. At the same time, the Court's judgment in *Gaskin* builds upon the premise that the importance to a person of gaining access to information on him-/herself is only a necessary condition for enforcing access, not a sufficient condition. This premise also seems to be manifest in the case of *Leander*, in which the Court refrained from placing Swedish authorities under a duty to provide the applicant with access to information on his personal affairs, despite this information having been used to deny him employment.[128]

In the aftermath of *Gaskin*, the Court has handled several noteworthy cases dealing with access to information pursuant to Art 8. The first is *McMichael v United Kingdom*.[129] In this case, the applicants were parents to a child who was taken from their custody by a child-welfare agency. During the proceedings for determining custody, the applicants were denied the opportunity of acquainting themselves with certain documents considered by the adjudicatory body. The Court held that the lack of access to these documents breached both applicants' right to respect for "family life" under Art 8(1), even though only one of the applicants was formally a party to the custody proceedings.[130] In other words, the Court found that Art 8 embodied a right of access in the circumstances of the case, independent of the applicants' entitlement or non-entitlement to such a right under Art 6 of the ECHR.[131]

Of broader significance is the case of *Guerra and Others v Italy*.[132] Here, the Court unanimously found that the failure by state authorities to fulfil certain legislative obligations to inform the citizens of a town about serious nearby environmental hazards was in violation of the authorities' positive obligation to secure the citizens' right to respect for private and family life pursuant to Art 8. The decision is particularly noteworthy for showing that Art 8 may require, in some circumstances, that state authorities pass over certain information to citizens independent of actual requests by the latter for such information. The decision is also noteworthy for showing that Art 8 may require procedures for access to a broader range of information than was stipulated in *Gaskin*: access procedures may need to encompass not only information which is necessary for citizens' understanding of their "childhood and early development", they may also need to encompass non-personal information that can increase

---

126 Here the Court cited its decision in *Rees v United Kingdom* (1986) Series A, No 106, para 37. For presentation of the *Rees* judgment, see below.

127 Note particularly the Court's comment in para 37 that it "is not called upon to decide *in abstracto* on questions of general principle in this field but rather has to deal with the concrete case of Mr Gaskin's application".

128 The judgments in *Leander* and *Gaskin*, however, are not completely analogous with respect to information access. The claims for access in each case were raised in very different factual contexts – police surveillance for national security purposes as opposed to child foster-care. Moreover, in contrast to its assessment of the situation for Mr Gaskin, the Court found that, apart from being denied employment, the detriment suffered by Mr Leander as a result of not being given access to the contested information "did not constitute an obstacle to his leading a private life of his own choosing": *Leander*, *supra* n 48, para 59. Further, in contrast to *Gaskin*, the *Leander* case concerned a claim of access to personal information which had been held and used in such a way as to 'interfere' with the data subject's Art 8(1) rights; accordingly, the Court considered enforceability of the access claim solely by reference to Art 8(2). It is questionable, though, whether the latter factor was of any decisive consequence. The Commission in *Gaskin* assessed the refusal of access by reference to Art 8(2) and ended up applying much the same "proportionality" criterion as the Court did. But, given the different factual contexts in which the claims for access were raised in each case, one cannot be sure of the exact effect of Art 8(2) on the different case outcomes.

129 (1995) A 307-B.

130 *Ibid*, paras 91–93.

131 If a person who is party to judicial proceedings is denied the opportunity of gaining access to the case documents, his/her right to a fair trial under Art 6 may be breached. See, eg, *McMichael*, *supra* n 129; *Kerjojärvi v Finland* (1995) A 322.

132 Judgment of 19.2.1998, available over the Internet via URL <http://www.dhcour.coe.fr>, otherwise not yet officially published.

citizens' understanding of their health situation, at least in circumstances where their health is seriously endangered. In this respect, Art 8 may require access procedures that are more typical of legislation on freedom of information (FOI) than data protection.

In *McGinley and Egan v UK*,[133] the Court followed up the line taken in *Guerra* by holding that state authorities engaged in nuclear testing are required under Art 8 to establish "effective and accessible" procedures for enabling citizens involved in such activity "to seek all relevant and appropriate information" about the possible effects of the testing on their health:

"Where a Government engages in hazardous activities, such as those in issue in the present case, which might have hidden adverse consequences on the health of those involved in such activities, respect for private and family life under Article 8 requires that an effective and accessible procedure be established which enables such persons to seek all relevant and appropriate information".[134]

Also noteworthy is the Commission decision in *Martin v UK*.[135] The Commission was called upon to determine the compatibility with Art 8 of a procedure whereby the applicant's access to his medical records was conditional upon a medical advisor, appointed by the applicant, first deciding which of the information could be accessed without causing harm to the applicant or others. In this case, the applicant sought access to medical records made in connection with his treatment by psychiatric consultants over a four-year period beginning when he was 19 years old. The Commission distinguished the case from *Gaskin*, finding that the records to which access was sought did not relate to his childhood and had not been shown to be the only available means of ascertaining information about the period of his psychiatric treatment. The Commission found also that the access procedure fulfilled a legitimate aim ("protection of health") pursuant to Art 8. It further noted that the records were not required for medical purposes or in connection with any dispute or litigation, and that the applicant was able to appoint the medical advisor who would determine which information could be accessed. On the basis of all these factors, the Commission held that the access procedure "strikes a fair balance between the legitimate aim sought to be realised and the applicant's wish to have access ...".[136] Accordingly, the application was found inadmissible.

A limited right of access to personal information may be derived from the right to receive information under Art 10 of the ECHR. The leading case in this regard is that of *Leander*, in which the Court held that "the right to freedom to receive information basically prohibits a Government from restricting a person from receiving information that others wish or may be willing to impart to him".[137] However, the Court added that "Article 10 does not, *in circumstances such as those of the present case*, confer on the individual a right of access to a register containing information on his personal position, nor does it embody an obligation on the Government to impart such information to the individual".[138] This view was re-affirmed by the Court in *Gaskin*.[139]

At the same time, one should be careful about generalising from the judgments in *Leander* and *Gaskin* that Art 10 cannot provide for any right of access to information held by state authorities. Both judgments concern demands for access to information that was only of

---

[133] Judgment of 9.6.1998, available over the Internet via URL <http://www.dhcour. coe.fr>, otherwise not yet officially published.
[134] *Ibid*, para 101.
[135] (1996) Appl 27533/95, 21 EHRR CD 112.
[136] *Ibid*, 115.
[137] *Leander*, *supra* n 48, para 74.
[138] *Id* (emphasis added).
[139] *Gaskin*, *supra* n 123, para 52.

personal character and only of importance for the data subjects. As several writers have argued, the Court may well reach a different decision if the information in question is of a matter of general public concern. Hence, if the case of *Gaskin* had involved a demand for access to information revealing alleged abuses of power by the social welfare authorities which affected more persons than just Gaskin himself, the Court might have allowed for a right of access pursuant to Art 10.[140] The strength of this supposition is not weakened by the recent decision of the Court in *Guerra*.[141] Here, the Court held that the state authorities' failure to take, *of their own accord*, steps to inform citizens about serious nearby environmental hazards did not amount to a violation of the citizens' right to information under Art 10.[142] However, the Court did not thereby rule that the state authorities could have no duty, pursuant to Art 10(1), to give out such information *upon request*.[143]

As for a putative right for data subjects to rectify data registered on them, one of the very few cases in point is *Chave née Jullien* in which the applicant sought erasure of the record of her illegal confinement in a psychiatric ward. Her action failed, with the Commission finding the continued storage of the disputed record to be in accordance with the law and necessary in a democratic society for the protection of health.[144] Nevertheless, the Commission arguably recognised that Art 8(1) embodies, in the circumstances of the case, a *prima facie* claim for rectification/erasure of data.

Other cases in point concern the refusal by state authorities to rectify official records, particularly birth certificates, so as to reflect accurately the changed sexual identities of transsexuals.[145] In these cases, the Commission has consistently found such refusal to violate a transsexual's right to respect for private life under Art 8(1). In doing so, it has recognised Art 8(1) as protecting the interest of transsexuals in being able to determine for themselves their sexual identity, both in relation to themselves and to others. And it has recognised that this interest – described by Harris *et al* as one of "self-identification"[146] – is significantly affected by the way in which transsexuals are represented in personal data registers.[147]

The Court has been more conservative. In *Rees* and *Cossey*, the refusal by British authorities to alter the applicants' respective birth certificates to reflect their changed sexual identities was found by the Court not to breach Art 8. The Court held that to accede to the applicants' requests would require the United Kingdom to undertake extensive modification of its existing system of birth registration, creating problematic consequences for the rest of the population.[148] The Court emphasised that states parties enjoy a wide margin of appreciation with regard to recognising the legal status of transsexuals, given the lack of "common ground between the Contracting States in this area".[149] It noted also that transsexuals in the United Kingdom are free to change their forenames and surnames at will, and that their sexuality as registered in their birth certificates does not have to appear on many of the official documents with which they are issued.[150] In *B v France*, however, the Court

---

[140] Eggen, *supra* n 54, 67. See also S Weber, "Environmental Information and the European Convention on Human Rights" (1991) 12 *HRLJ*, 180; LG Loukaides, *Essays on the Developing Law of Human Rights* (Dordrecht/Boston/London: Martinus Nijhoff Publishers, 1995), 22.

[141] *Supra* n 132.

[142] The Commission, by a majority vote, took the opposite view: see *Guerra and Others v Italy* (1996) Appl 14967/89, reported at [1996] VII HRCD 878.

[143] Indeed, seven judges indicated they view Art 10 as embodying such a duty.

[144] *Chave née Jullien*, *supra* n 81, 156.

[145] See, eg, *Van Oosterwijck v Belgium* (1979) B 36; *Rees v United Kingdom* (1986) Series A, No 106; *Cossey v United Kingdom* (1990) Series A, No 184; and *B v France* (1992) Series A, No 232-C. Note that the Court did not consider the merits of the *Van Oosterwijck* case as the applicant was found not to have exhausted all remedies available to him pursuant to domestic law.

[146] Harris *et al*, *supra* n 26, 307.

[147] See especially *Van Oosterwijck*, *supra* n 145, paras 46 & 52.

[148] *Rees*, *supra* n 145, paras 42–44; *Cossey*, *supra* n 145, para 38.

[149] *Rees*, *supra* n 145, para 37; *Cossey*, *supra* n 145, para 40.

[150] *Rees*, *supra* n 145, para 40.

found for the applicant, distinguishing the case from those of *Rees* and *Cossey* on the grounds that the position of transsexuals in France was more difficult than in the UK and that the administrative changes necessary to accede to the applicant's request were not as major.[151]

In all three cases, the Court stressed that the issue in dispute concerned the extent of a state party's positive obligations flowing from the notion of "respect" in Art 8(1), rather than the extent to which there had been "interference" with Art 8(1) rights. For the Court, the "mere refusal" of a state party to rectify the official records in question could not amount to interference.[152] Accordingly, the Court did not find it strictly necessary to apply Art 8(2). As noted above in relation to the *Gaskin* judgment, the Court commented, nevertheless, that the aims listed in Art 8(2) could be of some relevance in striking a fair balance between the interests of the community and those of the individual.[153]

The majority decisions of the Court in *Rees*, *Cossey* and *B v France* seem simply to have characterised transsexuals' relevant interests in terms of avoidance of harm suffered when transsexuals are forced to disclose to others their transsexuality. The majority decisions have refrained from explicitly recognising transsexuals' interest in "self-identification". This interest is intimately connected with a more general interest in freely developing one's personality. When the latter interest has received considerable recognition in other Court judgments on Art 8, it is incongruous that transsexuals' interest in "self-identification" does not figure more prominently in the majority decisions here.

To sum up, the case law above shows that Art 8(1) provides some protection for a person's interest in being able to gain access to, and challenge, information on him-/herself held by others. However, the case law on Art 8 does not as yet champion a broad principle of individual participation (as defined in the introduction to this article). It does not establish a right of access that *prima facie* embraces all sorts of personal data. This is in contrast to data protection laws, which do establish such a right. However, the latter right is never absolute. Moreover, its strength in a particular case also depends partly on how important access to the data is for the well-being of the data subject. Accordingly, the difference here between Art 8 case law and data protection laws may not be so great in practice as it appears to be in principle. At the same time, the Art 8 case law goes further than data protection laws by requiring access procedures that encompass certain types of *non-personal* information – notably information that can enlighten citizens about serious dangers to their health.

## 5. Concluding remarks

At present, the case law developed around the right to privacy in Art 17 of the ICCPR and Art 8 of the ECHR falls short of explicitly stipulating data protection guarantees as comprehensive as those found in instruments concerned specifically with data protection. Moreover, the case law is somewhat confusing: the principles for processing personal data which emerge from it are often sketchy and of little prescriptory value. This is so even with the relatively extensive body of relevant case law developed around Art 8 of the ECHR. Too often there has been a failure by the Commission and/or Court to make clear exactly which element of the contested data-processing practice has interfered with the right under Art 8(1);

---

151 *B v France*, *supra* n 145, paras 49–63.

152 *Rees*, *supra* n 145, para 35; *Cossey*, *supra* n 145, para 36. The majority judgment of the Court in *B v France* appears also to have accepted this approach. Cf para 3.4 of Judge Martens' dissenting judgment in *Cossey* ("it is at least questionable whether the Court rightly held ... that in the Rees case only the existence and the scope of the *positive* obligations flowing from Article 8 were at stake: the very essence of Mr Rees' complaints was ... that the *legal system* in force in the United Kingdom ... was inconsistent with his rights under Article 8"). Cf also para 6 of Judge Walsh's concurring judgment in *B v France* ("The respondent State has not shown any valid justification within the terms of Article 8 § 2 of the Convention").

153 *Rees*, *supra* n 145, para 37.

too often has there been a concomitant failure to describe the threatened interest. But the limited prescriptory value of Art 8 case law in the field of data protection is not simply due to the Commission and Court. It is also due to the fact that a large proportion of the case law concerns data processing in a rather special context (ie, secret surveillance activities by police or intelligence agencies), while almost none of it deals with private entities' data-processing practices.

Perhaps the most positive aspect of the case law on Art 8, along with that on Art 17 of the ICCPR, is that it demonstrates a willingness of the Strasbourg organs and Human Rights Committee to adapt the provisions to take account of the potential dangers that new or uncontrolled forms of data processing create for the liberties of individuals and the life of democratic societies. To some extent, this willingness remains at the level of rhetoric. But, as the body of data protection laws grows nationally and internationally, it may reasonably be expected that these organs will increasingly expand the right to privacy in the light of these laws. In this regard, it is instructive to note comments by the former President of the European Court of Human Rights, Rolv Ryssdal:

"In decisions such as *Klass*, *Malone*, *Leander*, *Huvig* and *Kruslin*, our Court has demonstrated the continuing resilience of the protection afforded by Article 8 when it comes to technological innovations and data processing. The decided cases suggest that this Article may develop towards a right of informational self-determination, in that the collection, storage and processing of personal information by public powers may constitute an interference with the right enshrined in the first paragraph of Article 8".[154]

However, an important challenge for the European Court of Human Rights in the future will be the data-processing practices of private sector entities: how the Court tackles these practices will determine to a large extent the long-term utility of Art 8 as an instrument for data protection. Just as important is the degree to which the Court will be prepared to restrict data-processing developments which, although justified in isolation and perhaps even consented to by the data subjects, nevertheless combine to erode the bases for pluralist, democratic society. This latter challenge will be equally pertinent for the Human Rights Committee in its application of Art 17 of the ICCPR.

[154] Ryssdal, *supra* n 31, 41.