Chapter 4
The Materialisation of Data Protection in International Instruments

But one thing is certain: data protection is a reality.

(Hondius 1978)

By the end of the 1970s, various international organisations began to work actively towards the elaboration of international instruments dealing with the processing of information on individuals. International cooperation brought together European and non-European countries, including the United States (US). It eventually led to the parallel and intertwined elaboration of two key international instruments: the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (OECD), adopted in 1980, and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter, 'Convention 108') of the Council of Europe, of 1981.

This initial institutionalised international cooperation resulted in the labelling of existing and upcoming European rules on the processing of data as concerned with 'data protection', and their progressive linkage with the word 'privacy'. The embroilment between these expressions was to expand from the adopted international instruments directly into various European national legal orders. It was also crucially transferred into European Union (EU) law, where it survived during several decades, and where it is arguably not (yet?) completely undone.

This chapter analyses how such 'data protection'/'privacy' connection was incorporated into the OECD Guidelines and Convention 108, to contribute to a deeper understanding of its implications for the shaping of EU personal data protection. It also examines the impact upon national legal instruments of the adoption of Convention 108, and the only partial integration of its terminology and approach in the case law of the European Court of Human Rights (ECtHR).

G. González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Law, Governance and Technology Series 16, DOI 10.1007/978-3-319-05023-2_4,

4.1 The OECD and its Guidelines

The OECD is an international economic organisation established in 1961 to promote economic development and world trade. Initially composed of 18 European countries, together with the United States and Canada, it has nowadays 34 members, including countries of South America and the Asia-Pacific region. Its headquarters are in Paris, and its official languages are English and French. In 1980, the OECD adopted its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, which constituted the first international statement of principles regulating the processing of data—a text agreed upon which agreed both by the US and European countries (Working Party for Information Security and Privacy (WPISP) 2011, p. 12).

4.1.1 From the Computer Utilisation Group to the Data Bank Panel

The OECD started investigating the issue of computers in 1968, when a Ministerial Meeting on Science of OECD Countries was devoted to the issue of *Gaps in Technology*.[1] A few months later, the OECD Committee on Science Policy promoted the launch of a Computer Utilisation Programme, and the setting up of a Computer Utilisation Group to study the subject more deeply (Hondius 1975, p. 57). This Computer Utilisation Group[2] carried out a series of studies on electronic data banks, computers, and telecommunications, leading it to the discussion of issues of privacy and data protection (Hondius 1975, p. 57). In 1971, illustrating the increasing interest of the OECD in the question of privacy, a report on *Digital information and the privacy problem* was published under the Series *OECD Informatics Studies*.[3]

In 1972, the OECD created a board named the Data Bank Panel,[4] directly concerned with reflecting on the regulation of the processing of information about individuals in automated databases. The Data Bank Panel organised in 1974 an *OECD Seminar on Policy Issues in data protection and privacy*,[5] where many of the discussions centred on the notion of privacy as described by Westin (Braibant 1999, p. 8). The event comprised a session titled *Rules for Transborder Data Flows*,[6]

[1] The 3rd Ministerial Meeting on Science of OECD Countries, celebrated in March 1968.

[2] Working in close liaison with the Information Policy Group, and under the supervision of the OECD Committee for Science Policy (Hondius 1975, p. 58).

[3] To which were annexed an English and a French translation of the Hessen Data Protection Act (Gassmann 2010, p. 1). Other studies published as Informatics Studies were *Computerised Data Banks in Public Administration*, and '*Policy Issues in Data Protection and Privacy*' (Working Party for Information Security and Privacy (WPISP) 2011, p. 9).

[4] Chaired by chaired by the Swedish P. Svenonius.

[5] See also Chap. 3, Sect. 3.1.4, of this book.

[6] As well as other sections named *The Personal Identifier and Privacy*, and *Right of Citizen Access to their File*. A Synthesis Report was prepared by the OECD Secretariat in 1976 (Working Party

heralding the identification of what soon became the major issue of concern for the OECD in relation to the regulation of data processing: transborder data flows (Gassmann 2010, p. 1).

The expression 'transborder data flows' referred to the possibility to legally transfer data from a determined country to another. The 1973 Swedish Data Act, based on the idea that, generally, any automated processing operation required previous authorisation by a Data Inspection Board, had established a requirement to obtain an explicit authorisation before exporting any data outside Sweden (Kuner 2011, p. 14). As the 1970s unfolded and national norms on data processing continued to spread, different European countries included in their own legislation disparate mechanisms to restrict the export of data, in the belief that, otherwise, those processing data might be tempted to escape national regulation by surreptitiously transferring data to countries with less stringent protection, so-called 'data havens': this was so in Austria[7] and France,[8] but also in Luxembourg, and in Denmark (Kirby 1980, p. 3).

One of the major objectives of the OECD being the promotion of the expansion of world trade, this organisation worried about the possibility that national provisions would create barriers to the free flow of information, and, in this way, impede growth (Working Party for Information Security and Privacy (WPISP) 2011, p. 10). Some considered that, under the surface of a discourse on the protection of the individual surrounding the national norms on data processing, what was really at stake were measures conflicting with free trade, or what was described as 'data protectionism' (Kirby 1980, p. 4). Transborder data flows were thus rapidly placed high on the agenda. In 1977, the OECD Data Bank Panel organised a new event, this time called *Symposium on Transborder Data Flows and the Protection of Privacy*. During the event, Louis Joinet, at the time President of the French *Commission nationale de l'informatique et des libertés* (CNIL), emphasised the economic value and national interest of transborder data flows (Working Party for Information Security and Privacy (WPISP) 2011, p. 10). The symposium led to the dismantlement of the Data Bank Panel, and the creation, instead, of a new Expert Group.

4.1.2 The OECD Guidelines

Set up at the beginning of 1978,[9] this new OECD Expert Group[10] was immediately entrusted with the task of drafting guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data for the OECD (Michael 1994, p. 34).[11]

for Information Security and Privacy (WPISP) 2011, p. 9).

[7] Österreichisches Datenschutzgesetz von 1978, p. 32, 34.

[8] Article 24 of Loi no. 78–17 relative à l'informatique, aux fichiers et aux libertés.

[9] By the Committee for Scientific and Technological Policy (Kirby 1980, p. 13).

[10] Expert Group on Drafting Guidelines governing the Protection of Privacy and Transborder Data Flows of Personal Data.

[11] It has been argued that the initiative was originally advanced by the French government (Michael 1994, p. 32).

The Expert Group was chaired by Michael Kirby, Chairman of the Australian Law Reform Commission which was at that time preparing new federal laws on privacy protection for Australia (Kirby 2010a, p. 2).[12] Other Expert Group members included the German Spiros Simitis, who had previously contributed to the drafting of pioneering German data protection, and was the *Hessischer Landesbeauftragter für den Datenschutz* (Data Protection Commissioner of the German federal state of Hesse) since 1975 (Kirby 2010a, p. 7), and the Italian Stefano Rodotà.

Among the main common references for discussion inside this Expert Group were the writings by Westin and by one of his former research assistants, the Canadian David Flaherty, as well as existing institutional reports, such as the British 1972 Younger Report, the French 1975 Tricot report, and especially, the report *Personal Privacy in an Information Society* published in 1977 by the short-lived US Privacy Protection Study Commission (The Privacy Protection Study Commission 1977). The OECD Expert Group was instructed to carry out its activities in close co-operation and consultation with both the Council of Europe, already active in the field for some years, and the European Community (EC) (Kirby 1980, p. 14),[13] which was starting to express interest in the field.

The negotiations leading to the elaboration of the OECD Guidelines were rather laborious (Bennett and Raab 2003, p. 74), notably due to contrasting approaches on the question of international data flows. And although there was a consensus on the idea that individuals should generally have access to personal data held about them (Kirby 1980, p. 5), views also diverged on how this should be put into words. European members favoured language similar to two recommendations already adopted by the Council of Europe[14] while US representatives insisted—with success—on referring back to the 1977 report by the US Privacy Protection Study Commission as the main 'conceptual framework' to apply (Kirby 1980, p. 16). Whereas Council of Europe's instruments tied the adoption of measures solely to the protection of individuals,[15] the l977 US report delineated the vision of a need to strike a proper balance between competing values: on the one hand, individuals' interests on their personal privacy, and, on the other, the information needs of an information-dependent society.[16]

In January 1980, US President Jimmy Carter announced in his State of the Union Address that the adoption of the OECD guidelines was imminent. The OECD Council finally adopted its Recommendation concerning Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[17] in September 1980.

[12] Peter Seipel assisted as consultant.

[13] The Expert Group worked in cooperation with representatives of the Commission of the European Communities (EC) (Kirby 2010a, p. 8). The key representative of the Council of Europe was F. W. Hondius (Kirby 2010a, p. 8).

[14] Council of Europe's Recommendations 73 (22) and 74 (29).

[15] European representatives emphasised that for them interferences with privacy from misuse of personal data were not a theoretical danger, but had historical precedents, for instance in relation with the Second World War (Kirby 2010b, p. 5).

[16] See: (The Privacy Protection Study Commission 1977, Chap. 1 "Introduction").

[17] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23 September 1980. Actually, 21 of the then 24 Members of the OECD voted in favour,

The OECD Guidelines target the protection of 'privacy', as expressed in their heading, but, more exactly, 'the protection of privacy and individual liberties'[18] in relation to personal data. The mention of 'individual liberties' in conjunction with privacy echoes the allusion to the same notion among the general purposes of the 1978 French *loi informatique et libertés.*[19] It also translates a tension between the disparate terminological choices existing among OECD countries. The Preface to the OECD Guidelines states that 'privacy protection laws'[20] have been introduced or are to be introduced in many OECD Member countries, including France, Germany, Sweden, Belgium, the Netherlands or Spain, with a view to prevent 'what are considered to be violations of fundamental human rights'[21] in relation to the use of personal data.[22] The Explanatory Memorandum accompanying the Guidelines nevertheless concedes that in continental Europe it is common practice to refer to 'privacy protection laws' not with such terms but rather as 'data laws', or even as 'data protection laws'.[23] It also hints at the different meanings attached to the word privacy, arguing that there has been in the previous years 'a tendency to broaden the traditional concept of privacy', leading to something that 'can perhaps more correctly be termed *privacy and individual liberties'*.[24][25]

Privacy is any case the word in the end privileged by the OECD Guidelines, which repeatedly refer to privacy protection, and to the protection of privacy. Despite the qualifications of the Explanatory Memorandum, in the Guidelines themselves there is no reference whatsoever to data protection. As a matter of fact, they designate any existing norms on the processing of data as privacy laws. This choice was fully consistent with the US perspective, which formally endorsed (informational) privacy while ignoring the 'data protection' tag (a notion still today commonly overlooked both by US law and doctrine),[26] but it represented a novelty from the European standpoint, as in Europe at the time no existing legal instrument portrayed itself as a privacy instrument as such.

Concerning their substance, the OECD Guidelines apply to any personal data 'which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties', regardless of whether they are processed in the public or in the private

---

while Australia, Canada and Ireland preferred to abstain, and to postpone the decision the join (Commission nationale de l'informatique et des libertés (CNIL) 1982, p. 158).

[18] First paragraph of the Recommendation.

[19] The official languages of the OECD are English and French. In French, the title of the OECD Guidelines is *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel,* and their objective is described as ensuring protection of '*la vie privée et les libertés individuelles*'.

[20] First paragraph of the Recommendation.

[21] Ibid.

[22] Ibid.

[23] See Explanatory Memorandum, paragraph 4.

[24] Emphasis added.

[25] Ibid. paragraph 2.

[26] Observing such resistance: (Arzt 2005, p. 193).

sector, and of whether they are processed automatically or manually.[27] Personal data are defined as 'any information relating to an identified or identifiable individual (data subject)'.[28] The processing of data of personal data in the signatory countries shall be subject to eight 'principles': the collection limitation principle,[29] the data quality principle,[30] the purpose specification principle,[31] the use limitation principle,[32] the security safeguards principle,[33] the openness principle,[34] the individual participation principle,[35] and the accountability principle.[36]

The protection of privacy and individual liberties is not, however, the only objective pursued by the OECD Guidelines. There is a key second goal, which is the sheltering of transborder flows of personal data by avoiding any disparities in national legislations that could hamper 'the free flow of personal data across frontiers'.[37] Four different principles are put forward to facilitate the free flow of personal data across borders, including a general invitation to refrain from restricting transborder flows of personal data,[38] and a suggestion to avoid developing, in the name of the protection of privacy and individual liberties, any laws that would create obstacles to such flows.[39]

After adopting the 1980 Guidelines, the OECD remained active in the area of the regulation of data processing. For instance, in a Declaration on Transborder Data Flows accepted on 11 April 1985, the OECD Minister Committee reiterated the guidelines, while simultaneously emphasising again the interest of the OECD in unobstructed information exchange.

During all its various activities in the field, the OECD has confirmed its initial approach of subsuming any rules on the processing of data under the privacy tag. In this sense, in 2007 it adopted a Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, and, for the purposes of that Recommendation, any 'national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with the OECD Privacy Guidelines' are to be referred as 'laws protecting privacy'.[40] US literature commonly follows this line of thinking, for instance describing 'data protection' as a phrase 'frequently used' in Europe 'to describe privacy protection' (Solove et al. 2006, p. 870). The OECD Guidelines were an extremely influential instrument globally, but were not legally

[27] Article 2 of the OECD Guidelines.

[28] Ibid. Article 1(b).

[29] Ibid. Article 7.

[30] Ibid. Article 8.

[31] Ibid. Article 9.

[32] Ibid. Article 10.

[33] Ibid. Article 11.

[34] Ibid. Article 12.

[35] Ibid. Article 13.

[36] Ibid. Article 14.

[37] Ibid.

[38] Ibid. Article 17.

[39] Ibid. Article 18.

[40] Point 1 of Annex to OECD *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (2007).

binding. As they were adopted, the Council of Europe was finalising the elaboration of a legally binding instrument, to become even more significant in Europe.

4.2 The Council of Europe and Convention 108

The Council of Europe is an international organisation set up in 1949 by ten European countries,[41] to develop throughout Europe common and democratic principles. It comprises now 47 members. It is based in Strasbourg, and has two official languages: English and French.[42]

4.2.1 Privacy as (Insufficiently) Protected by Article 8 of the ECHR

Already in 1949, the Council of Europe launched negotiations to draft and adopt its own catalogue of human rights, leading to the elaboration of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Signed on 4 November 1950, and entered into force on 3 September 1953, the EHCR soon became the most important European human rights instrument ever. It lists thirteen rights or freedoms that drew heavily upon the Universal Declaration of Human Rights of 1948, both in subject matter and terminologically (Blackburn 2001, p. 9).

Contrary to the Universal Declaration of Human Rights (UDHR), however, the ECHR does not mention privacy at all. Whereas Article 12 of the UDHR, establishes that '(n)o one shall be subjected to arbitrary interference with his *privacy*,[43] family, home or correspondence, nor to attacks upon his honour and reputation', the ECHR provision that is supposed to mirror it, namely Article 8(1) of the ECHR, foresees that '(e)veryone has the right to respect for his *private*[44] and family *life*,[45] his home and his correspondence'.[46] This formal peculiarity of the ECHR could presumably be explained by taking into account the influence of the French expression

[41] The Statute of the Council of Europe was adopted on 5 May 1949, and came into force on 3 August 1949. The initial signatories were Belgium, Denmark, France, Ireland, Italy, Luxembourg, the Netherlands, Norway, Sweden and the UK. They were soon joined by Germany, Greece, Iceland, and Turkey (1949/1950). Austria joined in 1956. Cyprus in 1961, Switzerland in 1963, Malta in 1965 (De Schutter 2010, p. 21).

[42] Article 12 of the Statute of the Council of Europe (London, 5 May 1949).

[43] Emphasis added.

[44] Emphasis added.

[45] Emphasis added.

[46] Article 8(2) of the ECHR adds: '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'.

vie privée, which was the expression used in the French version, consistently with the French version of Article 12 of the UDHR.[47]

In reality, initial English draft versions of the EHCR did include the word privacy, but the term was replaced by the idiom 'private life' a few months before the definitive signing of this instrument. In the documents of the *travaux préparatoires* (preparatory works) of the ECHR the appearance of the expression private life (instead of privacy) in the English draft can be dated to August 1950. Although it was common practice to underline in each subsequent draft the changes proposed in relation to the previous draft, the sudden replacing of privacy with private life was not identified as a change, in the sense that it was not underlined.[48]

As a result of this (not even underscored) move, the English and French versions of Article 8 of the ECHR might be regarded as looking superficially rather similar: one establishes a right to respect for 'private life', and the other for *vie privée*. Nevertheless, while the French text maintains a formal consistency with Article 12 of the UDHR, the consistency is lost in the English version.

Insofar as the ECHR is concerned, the ultimate interpreter of its provisions is the ECtHR, based in Strasbourg. Over the decades, the Court has systematically avoided using the word privacy to refer to any right protected by Article 8 of the ECHR.[49] In reality, no Council of Europe institution appears to have used the word privacy in that sense (i.e., referring to the content of Article 8 of the ECHR) in the period going from the original drafting of the ECHR up until 1967.[50] During those years, the rare documented occurrences of the term took place only anecdotally, for instance in relation to some spatial privacy needed in Council of Europe premises to facilitate free discussions,[51] in the frame of criticism of the secrecy of certain governmental debates,[52] or regarding the isolation of houses as foreseen by a debated housing code.[53]

---

[47] Article 12 of the UDHR: 'Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation'.

[48] Draft Convention adopted by the Sub-Committee on Human Rights (7th August 1950) in (Registry of the Council of Europe 1967, p. 17).

[49] The word tends to appear only exceptionally and only in specific contexts, for each time that the ECtHR considers the possible relevance of the 'reasonable expectations of privacy' doctrine, which originated in the US (see, for instance, *Gillan and Quinton v the United Kingdom* [2010] RJD 2010, App. No. 4158/05, § 61). See also, in relation to 'a sense of privacy' of patients: *Z v Finland* [1997] RJD 1997-I, App. No. 22009/93, § 95.

[50] According to the information available on the electronic repository of the archives of the Council of Europe.

[51] In discussions regarding the possible need to ensure 'the maintenance of the privacy of certain parts of the Assembly premises, so that they would reserved exclusively to Representatives and to competent Assembly services' (Council of Europe's Consultative Assembly 1949, p. 1128).

[52] There are references to 'Governments enveloped in the privacy of diplomatic conference', as well as to 'the privacy in which the Committee's debates are conducted' (Council of Europe's Consultative Assembly 1950a, p. 1430, 1653). The word is also used in alluding to a suggestion by Winston Churchill for an international meeting to be 'held in an atmosphere of privacy and seclusion' (Council of Europe's Consultative Assembly 1953, p. 47).

[53] In describing a draft Housing Code said to contain provisions relating to distribution of space and 'maintenance of the privacy of the home' (Council of Europe's Consultative Assembly 1950b,

The situation started to change in 1967, when Article 8 of the ECHR was indeed characterised as establishing a right to privacy (as opposed to private life).[54] This usage of the word privacy to allude to the right to respect for private life of Article 8 of the ECHR emerged in the specific framework of debates over the impact of scientific and technological developments in the protection of human rights. In April 1967, more precisely, the Consultative Assembly of the Council of Europe referred to its Legal Committee two motions, one for a resolution on human rights and modern scientific and technological developments in general, and another more concretely expressing concern about the spread of technical devices facilitating eavesdropping and other ways of interfering with the right to privacy, which called for a study on how to regulate such devices (Commission on Human Rights of the United Nations Economic and Social Council 1970, p. 24).

In January 1968, the Council of Europe's Legal Committee responded to these two motions by submitting a report to its Parliamentary Assembly (Committee on Legal Affairs and Human Rights 1968). The report generally reviewed the dangers to individual's rights inherent in developments of the time, ranging from illegitimate use of official surveys to manipulation by electric shocks and drugs, and brainwashing.[55] Presenting the report to the Council of Europe's Parliamentary Assembly,[56] Mr. Czernetz, an Austrian representative, noted that the Legal Committee argued it was necessary to study 'the question whether Article 8 of the Convention on Human Rights as well as national legislation in the member States adequately protect the right to *privacy*[57] against violations which may be committed by the use of modern scientific and technical methods' (Council of Europe's Consultative Assembly 1968, p. 754). The terminological inclination of the members of the Legal Committee to use the word privacy in this context was presumably connected with their familiarity with the work of Alan F. Westin, cited twice by Czernetz during his speech (Council of Europe's Consultative Assembly 1968, pp. 751–752).

Following this intervention, the Parliamentary Assembly of the Council of Europe adopted an influential Recommendation addressed to the governments of its Member States: Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments.[58] Recommendation 509 (1968) proclaimed that 'modern scientific and technical methods'[59] were 'a threat to the rights and

p. 153, 209).

[54] In relation to Article 8 and Article 10(2) of the ECHR, it is alluded to 'the need for protection of the right to privacy', allegedly 'often not taken adequately into consideration by the Press' (Council of Europe's Consultative Assembly 1967, p. 15).

[55] But also eavesdropping, phone-tapping, surreptitious observation, subliminal advertising, propaganda and the use of mass media, and lie detectors (Commission on Human Rights of the United Nations Economic and Social Council 1970, p. 24).

[56] Presentation of 31 January 1968.

[57] Emphasis added.

[58] Council of Europe, Recommendation 509 (1968) on Human Rights and Modern Scientific and Technological Developments, adopted by the Assembly on 31st January 1968 (16th Sitting).

[59] Recommendation 509 (1968) paragraph 8(i).

freedoms of individuals and, in particular, to the right to *privacy*[60] which is protected by Article 8' of the ECHR,[61] and called for a study on the subject.[62] As a result, Council of Europe's Committee of Ministers included[63] this subject matter in the intergovernmental Programme of Work of the Council of Europe for 1968–1969,[64] and the Committee of Experts on Human Rights was set to work on it.

Somehow surprisingly, the Committee of Experts on Human Rights judged that all of the technological developments mentioned in Recommendation 509 (1968) were reasonably under control. But, the Committee pointed out, there was something that had not been mentioned in the Recommendation that was actually giving rise to serious problems, and required urgent action: the issue of computers (Hondius 1978, p. 2). The Committee of Experts on Human Rights regarded as particularly doubtful whether Article 8 of the ECHR offered any satisfactory safeguards in this area, particularly because, in its view, Article 8 of the ECHR was only applicable to interferences by public authorities, and not by private parties,[65] leaving the issue only partly uncovered.

By the beginning of the 1970s, thus, the Council of Europe had reframed its original interest in the problem of the protection of individuals in the face of technological developments by apprehending it as a (computers and) (informational) privacy problem, encapsulated by a need to, first and foremost, regulate the use of computers—very much echoing formally the framing of the issue in the US, therefore. And it had also set off the use of the word privacy to refer to the content of Article 8 of the ECHR.

4.2.2 Council of Europe's Recommendation 73 (22) and Recommendation 74 (29)

Following Recommendation 509 (1968), the Council of Europe continued to work on the protection for the citizen against intrusions on privacy by technical devices. A special Sub-Committee,[66] charged with studying the civil, criminal and constitutional issues related to the subject, suggested that the Council of Europe should

[60] Emphasis added.

[61] Ibid.

[62] Ibid. paragraph 8(ii).

[63] In April 1968, having considered Recommendation 509 (1968).

[64] Explanatory report to the Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series, no. 108 of 28 January 1981, p. 2.

[65] Explanatory Report accompanying Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of Ministers of the Council of Europe on 26 September 1973 at the 224th meeting of the Ministers' Deputies, paragraph 2.

[66] Working under the supervision of the European Committee on Legal Cooperation and in consultation with the European Committee on Crime Problems, and chaired by Gerald Pratt (Hondius 1975, p. 66).

concentrate on investigating the issue of electronic data banks, temporarily leaving aside any other aspects of privacy (Hondius 1975, p. 66).

As a result of this focused effort, the Council of Europe's Committee of Ministers adopted in 1973 Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector.[67] One of the major arguments grounding its adoption was that it was urgent to act in order to prevent the surfacing of divergences between upcoming national laws.[68] The 1973 Resolution's Explanatory Report noted that only very few Member States of the Council of Europe had already enacted legislation 'on *data privacy*',[69] but that, in addition to existing laws,[70] it was necessary to consider that there were important bills providing indications of possible solutions, among which was highlighted a 1972 Belgian bill.[71] The Explanatory Report also observed that the US 1970 Fair Credit Reporting Act equally provided an interesting model for discussion.[72]

Resolution 73 (22) took the form of a recommendation to Member States to take the steps necessary to give effect to ten principles applying to personal information stored in electronic data banks in the private sector. Elaborated in its Annex and further expounded in the Explanatory Report, these ten principles related to: quality of the information stored; the purpose of information; ways in which information is obtained; period during which data should be kept; authorised use of information; informing the person concerned; correction and erasing of information; measures to prevent abuses; access to information; and statistical data.

Resolution 73 (22) mentioned privacy in its very title, sustaining the idea that the regulation of automated data processing serves the protection of privacy, even if it failed to define or delimit the notion. It also alluded to the notion of 'intimate private life', stating that, generally, 'information relating to the intimate private life of persons' should not be recorded, and that in any case it should not be disseminated.[73] For the purposes of Resolution 73 (22), the terms 'information' and 'data' were used as interchangeable words, in an attempt to overcome that some European countries appeared to be focusing on the protection of 'data', while others referred to their object as 'information' (Hondius 1975, p. 85).[74]

Whereas Resolution 73 (22) covered data banks in the private sector, in 1974, the Council of Europe adopted a new Resolution which applied, this time, to the public

[67] Committee of Ministers of the Council of Europe, Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, adopted by the Committee of Ministers on 26 September 1973 at the 224th meeting of the Ministers' Deputies.

[68] Explanatory Report of Resolution (73) 22, paragraph 2.

[69] Emphasis added.

[70] Such as the 1970 Data Protection Act of the federal state of Hesse, and the Swedish 1973 *Datalag*.

[71] Explanatory Report of Resolution (73) 22, paragraph 8.

[72] Ibid.

[73] The French version refers to the protection of *vie privée* in the title, and to '*informations concernant l'intimité des personnes'* in para 1 of the Annex.

[74] See also: The Explanatory Memorandum of Resolution 74 (29) 12.

sector: Resolution 74 (29) on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector.[75] Resolution 74 (29) likewise took the form of a recommendation to the governments of Member States to take the steps to give effect to the principles applying to personal information set out in an Annex.[76]

By the end of 1974, experts at the Council of Europe considered that the body of law created across Europe for the protection of individuals against computerised records had acquired a name of its own, and that such name was 'data protection' (Hondius 1978, p. 3).[77] This body of law was nevertheless portrayed as an element of 'privacy', a term sometimes linked to its understanding as 'information(al) privacy' (Hondius 1975, p. 4), but sometimes used to refer to the content of Article 8 of the ECHR.

4.2.3 Council of Europe's Convention 108

Having adopted Recommendation 73 (22) and Recommendation 74 (29), the Council of Europe decided to pursue its work by reviewing how they were implemented and, in general, the state of advancement of national legislation in the area. A comparative study carried out in 1975 by the Secretariat of the Council showed that all national data protection regimes in Europe shared fundamental principles related with the quality of information, obligations imposed on the record-keepers, the rights of the persons whose data are stored (the 'data subjects'), public supervision (generally by a special authority), and the existence of procedural rules and sanctions (Hondius 1978, pp. 4–5). Nonetheless, the study also highlighted the existence of disparities, and presented them as a potential problem justifying further action.

In 1976, a Committee of Experts on Data Protection was set up, and placed under the authority of the European Committee on Legal Co-operation (CDCJ).[78] Its objective was to prepare a Convention for the protection of privacy in relation to data processing, to be ready for 1980 (Hondius 1978, p. 8). The Committee of Experts

[75] Committee of Ministers of the Council of Europe, Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, adopted by the Committee of Ministers on 20 September 1974 at the 236th meeting of the Ministers' Deputies.

[76] These principles, although extremely similar to those of Recommendation 73 (22) (Kirby 1980, p. 10), were however formally presented in a slightly different fashion. The Explanatory Memorandum accompanying Resolution 74 (29) only mentions the existence of eight principles.

[77] Data protection had been described as the 'legal rules and instruments designed to protect the rights, freedoms and interests of individuals whose personal data are stored, processed and disseminated by computers against unlawful intrusions, and to protect the information stored against accidental or wilful unauthorised alteration, loss, destruction or disclosure' (Hondius 1975, p. 1). For Hondius, an especially unfortunate terminological choice was the repeated mention by English speakers of the words computers and computer science. He called English speakers to adopt the word *informatics* instead of computer science, and of *informatician* instead of computer scientist, imploring the acceptance of this words by English speakers as 'a sacrifice asked of them for the sake of international cooperation' (Hondius 1975, p. 56).

[78] Explanatory Report of Convention 108, paragraph I.

on Data Protection worked from November 1976 to May 1979,[79] and was renamed the Project Group on Data Protection (CJ-PD) during 1978.[80]

The first meeting of the Committee of Experts on Data Protection resulted in an exchange of letters with the OECD, agreeing on cooperation and mutual assistance (Michael 1994, p. 33). Since that very initial stage, there was a common view on the need for the future Convention drafted by the Council of Europe to respect the principle of free international flow of information as supported by the OECD, and to refrain from laying obstacles in the way of international trade and commerce (Hondius 1978, p. 8).

Following a proposal by one of Council of Europe's experts, Frits W. Hondius, it was decided to draft a Convention that could be ratified not only by European countries, but also by countries outside Europe. The instrument was thus not named European Convention, but simply Convention.[81] This search for openness was confirmed and sustained by the direct participation in the preparatory works of observers from the OECD, and from four of its non-European states (Australia, Canada, Japan and the US). Observers from the EC, concretely the EC Commission, also took part.[82]

As the Convention was being drafted, exchanges between the Council of Europe and EC institutions increased. In 1979, the Secretary General of the European Parliament sent a letter to the Secretary General of the Council of Europe to inform him of the European Parliament's interest in progress in the field, illustrated by an attached Resolution on the subject endorsed soon before by the European Parliament.[83] In February 1980, the Parliamentary Assembly of the Council of Europe adopted a Resolution[84] welcoming European Parliament's interest,[85] and inviting it 'to direct its attention to how action within the framework of the European Communities could most effectively strengthen the principles and provisions to be embodied in the convention on data protection of the Council of Europe',[86] as well as to call on national parliaments to press for the introduction of legislation on data protection.[87]

On the same day that it approved such Resolution encouraging further work by EC institutions, Council of Europe's Parliamentary Assembly also adopted a

[79] First under the chairmanship of Louis Joinet (France), and subsequently of R. A. Harrington (Explanatory Report of Convention 108, paragraph 17).

[80] A working party, composed of the experts from Austria, Belgium, France, Germany, Italy, Netherlands, Spain, Sweden, Switzerland and the UK, met several times between the plenary committee meetings (ibid.).

[81] Explanatory Report to Convention 108, paragraph 24.

[82] As well as from Finland, and of the Hague Conference on Private International Law (ibid. paragraph 15).

[83] Parliamentary Assembly of the Council of Europe, *Protection of the rights of the individual in the face of technical developments in data-processing*, Doc. 4377, 11.6.1979.

[84] Resolution 721 (1980) on data processing and the protection of human rights, Assembly debate on 1 February 1980 (27th Sitting), text adopted by the Assembly on 1 February 1980 (27th Sitting).

[85] Resolution 721 (1980) paragraph 6.

[86] Ibid. paragraph 10(a).

[87] ibid. paragraph 10(b).

Recommendation on the possible inclusion in the very text of the ECHR of a right to the protection of personal data. In January 1980, had indeed been submitted to the Parliamentary Assembly an Opinion on *Data processing and the protection of human rights* (Lewis 1980), where it was stressed that Portugal,[88] Spain,[89] Austria and the German federal state of North Rhine-Westphalia had incorporated 'data protection' into their respective constitutional texts. The Opinion was based on a Report that stated that 'the idea of privacy is very difficult to define', but argued that, nevertheless, 'it is possible to tell when and who it may be infringed by the computerised use of personal data' (Parliamentary Assembly of the Council of Europe 1980, p. 5).

In response to that Opinion, Council of Europe's General Assembly, through its Recommendation 890 (1980) on the protection of personal data,[90] commenting that some states had 'made the protection of personal data a constitutional right',[91] and declaring that others planned to do so, recommended its Committee of Ministers to consider 'as part of the extension of the rights in the (ECHR), the desirability of including (…) a provision on the protection of personal data, by amending Article 8 or 10, or by adding a new article'.[92] Council of Europe's Committee of Ministers transmitted this Recommendation for opinion to two different committees, the Steering Committee for Human Rights, and the European Committee for Legal Co-operation.

A final version of the Convention on data protection was published in April 1980 (Michael 1994, p. 33). The Convention, to be commonly known as Convention 108,[93] was adopted by the Committee of Ministers on 17 September 1980, and it was decided to open it for signature only during a Session of the Parliamentary Assembly (Commission nationale de l'informatique et des libertés (CNIL) 1982, p. 157). This happened on 28 January 1981, when seven states already signed it.[94]

Convention 108 identifies as its object to secure for all individuals in the territory of the countries Party to the Convention respect for their rights and fundamental freedoms, and in particular (in the French version, *notamment*) for their right to privacy, with regard to automatic of personal data relating to them,[95] which is advanced as corresponding to the substance of the notion of 'data protection'.[96] Convention 108 thus marks a key step in the norms on the processing of personal

[88] Portugal had become of Member of the Council of Europe in 1976.

[89] Spain had become of Member of the Council of Europe in 1977.

[90] Text adopted by the Assembly on 1 February 1980 (27th Sitting).

[91] Resolution 890 (1980) paragraph 2.

[92] Ibid. paragraph 3.

[93] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, European Treaty Series No. 108.

[94] Austria, Denmark, France, Germany, Luxembourg, Switzerland and Turkey (ibid.). See also: Explanatory Report to Convention 108, paragraph 17.

[95] Article 1 of Convention 108.

[96] Ibid. The Explanatory Report to Convention 108 defines data protection as 'the legal protection of individuals with regard to automatic processing of personal information relating to them' (paragraph 1).

data, for at least three reasons: first, it inscribes in a legally binding international instrument the English idiom 'data protection' (in the French version, *protection des données*), moving it beyond its previously strictly German context; second, it formally links such data protection to the safeguarding of 'rights and fundamental freedoms' in general; and, third, it articulates a special linkage of data protection with a 'right to privacy'—to be understood as enshrined by Article 8 of the ECHR (mentioned in the Explanatory Memorandum), and thus as equivalent to the right to respect for private life. From its perspective, thus, it can be supported that there exists, for the purposes of Convention 108, something called 'data protection' which is implemented to preserve something designated as 'privacy' (Flaherty 1989, p. xiv).

Contrary to the OECD Guidelines, which openly pursue two conflicting objectives that they aim to reconcile ('privacy and the free flow of information', the latter overtly related to OECD's support of the free market),[97] Convention 108 has, formally, one single purpose: ensuring data protection.[98] Nevertheless, Convention 108 is also directly concerned with securing the free flow of data. In this sense, it devotes various provisions to 'Transborder data flows',[99] and prohibits in general any restriction to flows of personal data going to the territory of another Party taken 'for the sole purpose of the protection of privacy'.[100]

Convention 108's backing of the free flow of personal data is connected in a rather indeterminate way both to the notion of free market and to freedom of expression, concretely through a renaming of the established human rights principle of freedom of circulation of information (Lageot 2008, p. 338) in terms of 'free flow' (which was the terminology applied by the OECD to refer to the lifting of barriers to free trade). The preamble to Convention 108 identifies 'the free flow of information between peoples' as a fundamental value, linking it to 'the freedom of information across frontiers'.[101] The Explanatory Report to the text explicitly links the Convention's provisions on transborder data flows to 'the principle of free flow of information, regardless of frontiers, which is enshrined in Article 10' of the ECHR,[102] proclaiming that the 'free international flow of information' is of fundamental importance for individuals as well as for nations.[103] The same Explanatory Report also asserts that the preamble aims at underlining the Convention 'should not be interpreted as a means to erect non-tariff barriers to international trade'.[104] Despite not being formally as overtly directed towards ensuring the free flow of

[97] Described as fundamental and competing values in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

[98] Article 1 of Convention 108.

[99] Chapter III of Convention 108.

[100] Article 12(2) of Convention 108; see also Articles 12(1) and 12(3).

[101] Article 10(1) of the ECHR establishes in its first sentences: 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers'.

[102] Explanatory Report to Convention 108, paragraph 62.

[103] Ibid. paragraph 9.

[104] Ibid. paragraph 25.

data as the OECD Guidelines, Convention 108 has been portrayed as at least as equally concerned with such objective (Jacqué 1980, p. 779).

The scope of application of Convention 108 covers 'automated personal data files and automatic processing of personal data in the public and private sectors'.[105] Contrary to the OECD Guidelines, it thus focuses on the processing of data which is automated. Personal data are defined as 'any information relating to an identified or identifiable individual ('data subject')'.[106] In the French version, the notion of 'personal data' is referred to as '*données à caractère personnel*', or 'data of personal nature', a wording underlining the peculiarity of the meaning of 'personal' in this context. The provisions of a Chapter titled '*Basic principles for data protection*' (which do not include any further references to such idea of principles) address, notably, the notion of quality of data,[107] special categories of data,[108] data security,[109] and additional safeguards for the data subject (which are to generate subjective rights in domestic law).[110] The notion of quality of data is particularly important: it refers to the idea that personal data automatically processed must be processed 'fairly and lawfully',[111] 'stored for specified and legitimate purposes and not used in a way incompatible with those purposes',[112] 'adequate, relevant and not excessive' in relation to such purposes;[113] 'accurate and, where necessary, kept up to date',[114] and preserved in a form allowing for identification of individuals only as long as it is necessary.[115] Under the 'additional safeguards for the data subject' heading are recognised the right to information on the existence of automated personal data files, and on the controller of the files;[116] the right to access data stored,[117] the right to obtain rectification or erasure of the data if unduly processed,[118] and the right to have a remedy in case of lack of compliance.[119]

Convention 108 created a Consultative Committee (T-DP), consisting of representatives of Parties to the Convention and complemented by observers, which was entrusted with the interpretation of its provisions, their insurance, and the

[105] Article 3(1) of Convention 108.

[106] Ibid. Article 2(a).

[107] Ibid. Article 5.

[108] Ibid. Article 6.

[109] Ibid. Article 7.

[110] Ibid. Article 8.

[111] Ibid. Article 5(a).

[112] Ibid. Article 5(b).

[113] Ibid. Article 5(c).

[114] Ibid. Article 5(d).

[115] Ibid. Article 5(e).

[116] Ibid. Article 8(a).

[117] More concretely, 'to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form' (Article 8(b) of Convention 108).

[118] Ibid. Article 8(c).

[119] Ibid. Article 8(d).

improvement of their application.[120] Decades later this T-DP was merged with the Project Group on Data Protection set up in 1978.[121]

One of the first effects of the adoption of Convention 108 was to put over the possible inclusion in the ECHR of a special provision on data protection. The two committees to which the Committee of Ministers had transmitted Recommendation 890 for opinion, namely the Steering Committee for Human Rights, and the European Committee for Legal Co-operation, agreed shortly after the Convention's approval that it was not appropriate at the time to draft a provision on the protection of personal data for incorporation in the ECHR (Committee of Ministers of the Council of Europe 1981, p. 27). They suggested that it was preferable to first acquire more experience on the application of Convention 108, while at the same time working towards sector-specific Recommendations complementing it (Committee of Ministers of the Council of Europe 1981, pp. 28–29). The Steering Committee for Human Rights also pointed out the importance of the case law of the ECtHR confirming that States had positive obligations in relation to Article 8 of the ECHR,[122] asking to consider the possible implications of such case law as regards the provision of sufficient safeguards against interference with privacy resulting from the use of automatic processing of personal data—an argument that, in reality, could have been used to question also the need to adopt Convention 108.

Convention 108 entered into force on 1 October 1985, obliging participating countries to adopt their own legislation. It immediately generated much interest in the EC Commission, which did not only promote the Convention's ratification by Member States, but also expressed its intention to accede to the instrument. In 1999, Convention 108 was amended to allow the accession of the European Communities.[123] In 2001, an Additional Protocol was open to signature, with supplementary provisions on supervisory authorities and on transborder data flows.[124] The Additional Protocol took Convention 108 closer to the EC regime, which was already developed by then: it had put on the table the requirement of an independent data protection authority as a key element of data protection enforcement, and had refined the approach to requirements for restrictions on personal data exports.

The 1981 Convention is currently under reconsideration. The review process, conducted by the T-PD, started formally in January 2011 (Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to

[120] Chapter V of Convention 108.

[121] The merge occurred in 2003, and the resulting committee kept the name of Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.

[122] It referred notably to *Marckx v Belgium* [1979] Series A No. 31, App. No. 6833/74 (Committee of Ministers of the Council of Europe 1981, p. 27).

[123] Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, 15.6.1999.

[124] Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) regarding supervisory authorities and transborder data flows, Strasbourg, 8.11.2001. See, notably: (Pavón Pérez 2002).

Automatic Processing of Personal Data (T-PD) 2011, p. 5).[125] In its context, the possibility is being discussed to include in the revised instrument an explicit reference to a 'right to data protection', more recently advanced as a right to the protection of personal data.

Concretely, it has been proposed that the future instrument should mention in its preamble that everybody has 'the right to control one's own data and the use made of them', and that the future Convention's opening provision should define its purpose as to secure for every individual 'the right to the protection of personal data, thus ensuring the respect for their rights and fundamental freedoms, and in particular their right to privacy, with regard to the processing of their personal data' (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 9). To justify the allusion to the right to the protection of personal data, it has been argued that the right 'has acquired an autonomous meaning over the last 30 years', both through the case law of the ECtHR, and in the Charter of Fundamental Rights of the EU (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 32).

Some Members of the Council of Europe, however, have manifested their reticence. German representatives have contended that the German government 'finds it difficult to draw the line between the 'right to data protection' and the 'right to privacy'' because '(i)n the German understanding, the right to data protection is derived from the right to privacy'.[126] And the Swedish delegation to the T-PD has expressed its uneasiness with the aforementioned sentence on the right of individuals to control their own data, observing that 'it is unclear what it means',[127] and it also advocated that any reference to 'data protection' shall be replaced with 'personal data protection' (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 107).

4.2.4 Impact of Convention 108 on National Laws

The adoption in 1981 of Convention 108 set a milestone in the development of norms on the processing of personal data in European countries.[128] This does not

[125] Works towards the review at started at T-PD level in 2009 (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 4).

[126] Comments of the German Federal Government regarding the planned overhaul of Council of Europe Convention 108 (30 May 2012) in (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 86).

[127] See (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 107); in a similar vein, the European Data Protection Supervisor (EDPS) warned that 'there is not, literally speaking, a right to control one's data in the text' (of Convention 108) (Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) 2012, p. 135).

[128] According to the chronology by Spiros Simitis, it marked the beginning of a second phase in the development of data protection: (Simitis 2006).

mean that it was the sole reference for (or the sole reason behind) national norms approved after 1981. Nonetheless, its principles certainly served as basis for all subsequent European legislation (Zerdick 1995, p. 81), and inspired the review of instruments already in force (Prieto Gutiérrez 1998, p. 1140). Its ratification was openly supported by the EC,[129] and was eventually configured by a prior condition to access some instruments emerging in the context of increased European integration. Nowadays, all EU Member States have ratified Convention 108. The instrument is what is technically described as non self-executing, in the sense that it imposes on those countries wishing to ratify it the integration in their own legal systems of measures in compliance with its content.

The 1981 Convention appears to have been the decisive factor conducting the United Kingdom (UK) to finally adopt an Act on the automated processing of data (Prieto Gutiérrez 1998, p. 1145), in 1984.[130] It was entitled the Data Protection Act 1984, a name that already illustrates the influence of Council of Europe's framing of the issue (in terms of 'data protection' as opposed to 'privacy'). The Act's provisions do not mention any right to privacy (Flaherty 1989, p. 377), the existence of which was still a contested issue in British law, even if this absence was not an obstacle for some to assert that, for the purposes of the Act, data protection was essentially another name for privacy.[131] Like Convention 108, the Data Protection Act of 1984 focused on the regulation of automated data processing. Its basic approach was to require public and private organisations with access to computer-held personal data to register with a Data Protection Registrar. Very much influenced by both Convention 108[132] and the UK Data Protection Act of 1984, Ireland passed in 1988 its own Data Protection Act.[133]

In 1987, Finland, the last Nordic country to enact a statute on the processing of data (Blume 1991, p. 1), finally adopted its Personal Data File Act,[134] which came into force in 1988.[135]

In the Netherlands, the Koopmans Commission, which had been reflecting on the issue of privacy and personal information since 1971,[136] published its final findings in 1976. On this basis, in 1981 a bill was put forward, but it was later withdrawn due to criticism on potential implementation problems. In 1985, a new bill was submitted, this time taking into account a major revision of the Dutch Constitution that had taken place in 1983, and which had incorporated in the constitutional text a general right to respect of the *persoonlijke levenssfeer* ('personal sphere of

[129] Commission Recommendation of 29 July 1981 relating to the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data [1981] OJ L246/31.

[130] The UK signed Convention 108 in 1981, and ratified it in 1987.

[131] For instance: (Sizer and Newman 1984, p. 9).

[132] Ireland signed Convention 108 in 1986, and ratified it in 1990.

[133] Adopted on 13 July 1988, it came into force on 19 April 1989.

[134] Act 471/1987.

[135] Finland only signed and ratified Convention 108 in 1991.

[136] See Chap. 2, Sect. 2.2.1, of this book.

life')[137] together with a mandate to protect this right in relation to the recording and dissemination of personal data,[138] and on the rights to access to and rectification of such data.[139] The 1985 bill was enacted in 1989 as the *Wet persoonsregistraties* (WPR) (Overkleeft-Verburg 1995, p. 571).

Belgium signed Convention 108 already in 1982, but ratified it only in 1993. During many years it witnessed the drafting of unsuccessful bills (Robben and Dumortier 1992, p. 59), initially focusing on the regulation of the protection of private life in general,[140] later moving to certain aspects of such private life,[141] and later still centred on the protection of private life in relation to the processing of personal data.[142] In 1992, Belgium enacted the *Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.*[143]

4.3 European Court of Human Rights Case Law

As described, at the beginning of the 1970s, in order to justify Council of Europe's activity in the field of automated data processing that eventually resulted in the adoption of Convention 108,[144] it had been argued that Article 8 of the ECHR did not offer enough protection for individuals in the light of the advent of computers. A decade later, it was conversely contended that the very same Article, as developed in the case law of the judiciary of the Council of Europe,[145] was possibly effective enough to offer satisfactory protection, and that it was thus unnecessary to incorporate into the ECHR the recognition of an additional right.[146] In reality, both propositions might be regarded as open to debate.

The Council of Europe's Court that hears applications of alleged breaches of rights enshrined in the ECHR is the ECtHR. Over the decades, the ECtHR has been developing a broad interpretation of Article 8 of the ECHR. This interpretation certainly covers at least partially the scope of application falling under Convention 108, although it is still debatable whether it encompasses, or can encompass, the entirety of such scope (European Union Network of Independent Experts in

[137] Article 10(1) of the Dutch Constitution.

[138] Ibid. Article 10(2).

[139] Ibid. Article 10(3).

[140] Period 1970–1971 (Centre d'Informatique pour la Région Bruxelloise (C.I.R.B.) 2004, p. 4).

[141] Period 1975–1976 (Centre d'Informatique pour la Région Bruxelloise (C.I.R.B.) 2004, p. 4).

[142] 'Gol project', 1984–1985 (Centre d'Informatique pour la Région Bruxelloise (C.I.R.B.) 2004, p. 4). See also: (De Hert and Gutwirth 2013, pp. 19–20).

[143] 08/12/1992 (B.S., 18.03.1993). Describing it as largely inspired by French law: (Reidenberg and Schwartz 1998, p. 12).

[144] See Sect. 2.1 of this chapter.

[145] The European Commission and the Court of Human Rights, which were dissolved with the coming into force in November 1998 of Protocol No. 11 to the ECHR.

[146] See Sect. 2.3 of this chapter.

Fundamental Rights 2006, p. 90)—and to what extent it grants, or can grant, an equivalent level of protection.

Article 8 of the ECHR, titled 'Right to respect for private and family life', has a binary structure. It reads as follows:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

In its first paragraph, Article 8 of the ECHR establishes the existence of a series of rights: a right to respect for private life, a right to family life, a right to inviolability of the home, and a right to confidentiality of correspondence. The ECtHR however often mentions these rights in conjunction with each other, for instance by referring jointly to the right to respect for private and family life, or to respect for private life and confidentiality of correspondence in combination (Nardell 2010, p. 46). The second paragraph of Article 8 of the ECHR details the requirements of lawful interferences by public authorities with the described rights, which need to be 'in accordance with law' and 'necessary in a democratic society', and to pursue one of the explicitly enumerated aims.

When adjudicating on Article 8 of the ECHR, the ECtHR typically follows a two-step approach: first, it examines whether the issue at stake shall be regarded as an interference with any of the rights mentioned; second, it appraises whether the interference is to be considered legitimate or not.[147]

4.3.1 A Broad Interpretation of the Right to Respect for Private Life

The ECtHR has given to the wording of Article 8(1) of the ECHR a wide, generous interpretation (Nardell 2010, p. 46), as an element of its general approach of regarding the ECHR as a living instrument to be interpreted each time in light of 'present-day conditions'.[148] This broad reading has allowed the Strasbourg Court to consider as interferences with the rights enshrined by the provision measures related to the processing of data about individuals, and, vice versa, adjudication on this kind of measures has contributed to the progressive extension of ECtHR's construal of Article 8 of the ECHR.

The Court's broad conception of private life was notably put forward in the *Niemietz* ruling.[149] In this judgment, the ECtHR stressed that the right to respect for

[147] As a landmark case, see: *Klass and others v Germany* [1978] Series A no. 28, App. No. 5029/71.

[148] *Tyrer v United Kingdom* [1978] Series A No. 26, App. No. 5856/72.

[149] *Niemietz v Germany* [1992] Series A No. 251-B, App. No 13710/88.

private life ex Article 8 of the ECHR includes to a certain degree the right for individuals to develop relationships with other human beings.[150] The Court declared that it regarded as both impossible and unnecessary to attempt to define the notion of private life, but that in any case it would be too restrictive to limit the notion to an 'inner cycle' in which the individual may live his own personal life as he chooses', excluding entirely the outside world. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings'.[151]

The *Niemietz* case concerned the search of a lawyer's office in the context of criminal proceedings against a third party, raising the issue of the protection granted to profession or business activities. During the search, various cabinets and files had been examined, but no relevant documents had been found. In its judgment, the ECtHR made it clear that there was no reason of principle why the notion of private life should be taken to exclude professional or business activities, since it is precisely in the course of their working lives that the majority of people have a significant opportunity of develop relationships with others.[152] In addition, the Court noted, in some cases it is not even possible to clearly distinguish which activities are part of a professional or business life, and which are not.[153] The ECtHR has since then regularly emphasised the wideness of the notion of private life, portraying it as a term 'not susceptible to exhaustive definition'.[154]

4.3.2 Protection of Information Relating to Private Life

The cornerstone of the Strasbourg's case law on the processing of information about individuals is possibly the 1987 *Leander* judgment.[155] Previously, the question of whether the Court should rely or not on the provisions of Convention 108 had already been touched upon in the *Malone* judgment of 1984, in relation to the monitoring of telephone communications by the police, within the context of criminal investigations, through a technique called 'metering', and the related storage of information.[156] In *Malone* the Court concluded that there had been a violation of

[150] *Niemietz* § 29. See also: (Sudre 2005, p. 402). This broad conception was partly based in a special use of the expression 'right to respect for private and family life' as referring to a nebulous notion that covers the right to develop interpersonal relations (Sudre 2005, pp. 403–404).

[151] *Niemietz* § 29.

[152] Ibid.

[153] Ibid.

[154] *Bensaid v United Kingdom* [2001] RJD 2001-I, App. No. 44599/98, § 47.

[155] *Leander v Sweden* [1987] Series A No. 116, App. No. 9248/81. See also: (Peers 2006, p. 507).

[156] *Malone v the United Kingdom* [1984] Series A No. 82, App. No. 8691/79. Concerning 'metering', the Court took note of the fact that a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, and that metering is therefore to be distinguished from interception of communications. The Court did not accept, however, that the use of data obtained from metering cannot give rise to an issue under Article 8 of the ECHR, as the records of metering contain information which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of

Article 8 of the ECHR in connection with these practices, but without explicitly referring to Convention 108. The judgment was however accompanied by the concurring opinion, signed by Judge Pettiti, in whose view it was impossible to isolate the issue of the interception of communications from the issue of data banks, because interceptions give rise to storing of the information obtained; in this context, Judge Pettiti referred to the principles established by Convention 108 as criteria relevant to assess whether or not a measure constitutes a violation of Article 8 of the ECHR.

In *Leander*, the ECtHR did not refer either to Convention 108 (Martínez Martínez 2004, p. 196), but declared that the mere storing by the police of information relating to the private life of an individual amounts to an interference with the right to respect for private life,[157] and that this is so independently of the possible subsequent use of the data in question.[158] The case concerned a Swedish carpenter who wished to work at a museum adjacent to a restricted military security, but, after a personnel control procedure, and seemingly on the basis of a secret police file, was refused the job.

The *Leander* judgment was important insofar as it advanced that the mere storage by the police of some information relating to the private life of individuals amounts to an interference with the rights established under Article 8 of the ECHR. The Court, however, critically failed to explain in what was grounded such qualification of data as relating to somebody's private life. In *Leander*, the ECtHR merely declared that it was uncontested that the data at stake in the particular case related to the private life of the individual,[159] which was true, because precisely one of the concerns raised by the applicant was that he had not been able to access the content of the secret file (De Schutter 2001, p. 153),[160] and this impossibility to access the data prevented any contestation regarding their nature.

Leander opened up the question of whether the category of 'information relating to private life' the mere storage of which can amount to an interference with Article 8 of the ECHR corresponded or not to the category of 'personal data' recognised in Convention 108, which covers any automated processing of personal data, including their storage. Convention 108 applies to personal data qualified as pertaining to 'special categor(ies)' of data, such as personal data 'revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life', or relating to criminal convictions,[161] but also, generally, to data not falling under any of such categories, which are nonetheless 'personal' data, defined as any information relating to an identified or identifiable individual.[162]

What appeared to generate major ambiguities, especially at the beginning, was the issue of whether in the expression information 'relating to the private life' of

---

the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Article 8 of the ECHR (§ 84).

[157] *Leander* § 48.

[158] In *Leander,* the ECtHR was additionally concerned with the release of information.

[159] *Leander* § 48.

[160] See also: (De Hert 1998, p. 1998).

[161] Article 6 of Convention 108.

[162] Ibid. Article 2(a).

individuals the adjective private shall be read as opposed to public, or not. In 1994, the Commission of Human Rights looked into the case of an Austrian citizen who had participated in a demonstration to draw attention to the plight of the homeless, *Friedl*.[163] The police had taken pictures of him, and stored them. The Commission of Human Rights, noting that there had been no intrusion of the 'inner circle' of the applicant's private life in the sense that he was not at home when the pictures where taken; that the photographs related to a public event, that he was attending freely; that they were taken to record the sanitary conditions of the demonstration;[164] that no names were noted on the pictures, with participants remaining unidentified, and that no personal data or images had been entered into a data processing system,[165] concluded that the measure did not amount to an interference with Article 8 of the ECHR.[166] The Commission did not assert, however, that any of these criteria excluded by itself the possible qualification of the measure as an interference with the right to respect for private life.

In 2000, the ECtHR put forward that the category of information 'relating to private life' (the storage of which can amount to an interference with the right protected by Article 8 of the ECHR) shall be understood in line with its broad reading of the notion of private life, which, it argued, corresponded also to the view sustained by Convention 108. In *Amann*,[167] the Court indeed recalled the principle established in *Niemietz* according to which there is no reason of principle to justify excluding activities of a professional or business nature from the notion of private life,[168] and maintained that this broad interpretation corresponds with that of Convention 108.[169]

The *Amann* case concerned a seller of depilatory appliances, who once received a telephone call from the Soviet embassy in Berne for the order of a machine called Perma Tweez. The call was intercepted by the public prosecutor's office, who requested the intelligence service to draw up a file about the seller. Recalling its *Leander* case law, and after connecting it to *Niemietz* and Convention 108, the Court concluded in the judgment that storing a card on the seller, on which he was described as 'a contact with the Russian embassy', and where it was pointed out that he did 'business of various kinds' with a certain company,[170] was to be regarded as containing details that 'undeniably' amounted to data relating to the applicant's private life.[171]

The matter was further developed in another judgment of the same year, *Rotaru,*[172] where the defendant tried to argue that Article 8 of the ECHR was not

[163] Commission (Plenary) *Friedl v Austria* [1994] RJD 31.

[164] Ibid. § 49.

[165] Ibid. § 50.

[166] Ibid. 51.

[167] *Amann v Switzerland* [2000] RJD 2000-II, App. No. 27798/95.

[168] *Niemietz* § 29, and *Halford v United Kingdom* [1997] RJD 1997-III, App. No. 20605/92, § 42).

[169] Amann § 65.

[170] Ibid. § 66.

[171] Ibid. § 67.

[172] *Rotaru v. Romania* [2000] RJD 2000-V, App. No. 28341/95.

applicable to the case on the grounds that the information stored related not to the applicant's private life, but to his public life.[173] In *Rotaru*, the applicant was a Romanian national complaining about information seemingly in possession of the Romanian Intelligence Service, and which he considered false and defamatory. The information had been revealed in a letter, and generally concerned his youth, covering also his political activities. The intelligence service had notably claimed he had participated to an extreme right-wing movement in the 1930s, apparently mistaking him with another individual of the same name.

In its judgment in *Rotaru*, the Court referred to *Leander* and *Amann,* and explicitly pointed out that 'public information' can also fall with the scope of 'private life', concretely when systematically collected and stored in files held by the authorities, and that this 'is all the truer where such information concerns a person's distant past'.[174] The ECtHR then noted that the letter in question 'contained various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than 50 years earlier',[175] and declared that 'such information, when systematically collected and stored in a file held by agents of the State', fell within the scope of private life for the purposes of Article 8 of the ECHR. *Rotaru* thus made clear that the category of information relating to private life shall not be read as opposed to public information. As this was clarified, the question remained of determining what is exactly information relating to private life, the mere storage of which can deserve qualification as an interference with the rights established by Article 8 of the ECHR.

Since then, the ECtHR has been throwing further light on the issue, often making use of criteria implicitly or explicitly associated to Convention 108.[176] In *P.G. and J.H.*,[177] for instance, the Court alluded to Convention 108 to develop the case law of *Rotaru* and to apply it to the recording of the applicants' voices when being charged and when in their police cell, commenting that '(p)rivate-life considerations may arise (…) once any systematic or permanent record comes into existence of (…) material from the public domain'.[178]

The 2008 *S and Marper* judgment[179] illustrates particularly well the variety of grounds that can justify the qualification of information as relating to private life for the purposes of considering that its mere storage amounts to an interference with

[173] Ibid. § 42.

[174] Ibid. § 43. See also: *Cemalettín Canli v Turkey* [2008] App. No. 22427/04, § 33. The case concerned a man who appeared in registers held by the police as former member of illegal organisations, despite having been acquitted of that offence.

[175] Ibid. § 44.

[176] The ECtHR generally takes into account the context and the way in which information is used, and its nature. See also, for example: *Peck v the United Kingdom* [2003] RJD 2003, App. No. 44647/98.

[177] *P.G. and J.H. v the United Kingdom* [2001] RJD 2001-IX, App. No. 44787/98.

[178] Ibid. § 57. See also: *Segerstedt-Wiberg and Others v Sweden* [2006] RJD 2006-VII, App. No. 44787/98 (in particular, § 72).

[179] *S. and Marper v the United Kingdom* [2008] RJD 2008, App. Nos. 30562/04 and 30566/04.

the rights of Article 8 of the ECHR.[180] In *S and Marper*, the applicants complained about the retention by UK authorities of their fingerprints, cellular samples and DNA profiles after criminal proceedings against them were terminated. The Court found that the three types of data deserved protection, but for different reasons.

Concerning cellular samples, the ECtHR noted that their retention had to be regarded 'per se' as interfering with the right to respect for private life, given the 'nature' (labelled as 'highly personal')[181] and the 'amount' of 'sensitive'[182] personal information they contained.[183] DNA profiles were described as containing less information, but as being able, nonetheless, to generate information going 'beyond neutral identification' (for instance, touching upon genetic relationships between individuals) when submitted to automated processing.[184] Finally, the storage of fingerprints was described as giving rise to important private-life concerns because they constituted data regarding identified or identifiable individuals held by public authorities with the aim of being permanently kept and regularly processed by automated means for criminal-identification purposes;[185] thus, not because of the nature of the data, but because of storage conditions.

The Strasbourg Court later affirmed in *Khelili*[186] that *Marper* had detailed some of the principles applying to the storage of 'personal' information, 'personal' being advanced here as in 'personal data protection':[187] the judgment was issued in French, and the words used by the Court (*à caractère personnel*)[188] were words ostensibly rooted in European data protection.[189] The qualification of data as 'personal' did not, however, trigger immediately the qualification of their memorisation as an interference under Article 8 of the ECHR: the Court declared that, in order to determine whether personal data engaged any aspects of private life, it was necessary to take into account the context in which the data had been collected and stored, their nature, the way they were used and treated and the results obtainable from the processing.[190]

The ECtHR case law built over the years upon *Leander* certainly appears to move towards the incorporation of the substance of Convention 108 into the

[180] See, for instance: (González Fuster 2009).

[181] *Marper* § 73.

[182] Ibid. § 72.

[183] Ibid.

[184] Ibid. § 75.

[185] Ibid. § 78–86. See also: (De Beer de Laer et al. 2010, p. 141).

[186] *Khelili v Switerland* [2011] App. No. 16188/07.

[187] See also, for references to both personal data and sensitive data as in Convention 108: *M.M. v UK* [2012] App. No. 24029/07 § 188.

[188] See, for instance, *Khelili* § 55.

[189] The case concerned a woman who contested her description as prostitute in a police database, and asked for the data to be rectified. In its assessment of whether there had been an interference, the ECtHR took notably into account the fact that the information was accessible in an automated database (§ 64).

[190] *Khelili* § 55.

interpretation of Article 8 of the ECHR. The degree of such incorporation is nevertheless debatable.[191] Ultimately, the case law evidences Strasbourg Court's reluctance to apprehend the assessment of whether a measure constitutes or not an interference with Article 8 of the ECHR in terms other than those present in that provision. The ECtHR has never declared that any automated processing of personal data shall per se be considered as an interference with Article 8 of the ECHR, but it remains unclear whether this should be interpreted as indicating that some processing activities are excluded from the scope of Article 8 of the ECHR (Kranenborg 2008, p. 1093), or, perhaps, simply not included yet.

4.3.3 Health Data

A category of data unquestionably portrayed by the ECtHR as deserving protection under Article 8 of the ECHR is data related to health. In this area, the ECtHR has been particularly keen to vocalise the importance of 'data protection', and of Convention 108. It is highly questionable, nonetheless, to which extent health data have been granted protection in the name of general 'data protection' (understood as the legal notion developed by Convention 108, applicable to any automated processing of personal data), or in the name of special provisions on special categories of data deserving reinforced protection (which are also covered by Convention 108).

An eloquent instance of these ambiguities is *Z v Finland*,[192] related to the disclosure of the medical condition of the applicant, who was infected with HIV, in the context of proceedings concerning a sexual assault. In its judgment, the ECtHR underlined that 'the 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 ECHR.[193] Despite this formal endorsement of 'the protection of personal data', eventually the Court justified the level of protection deserved by the information disclosed[194] not because it constituted 'personal data' in the sense of Convention 108, but because it was sensitive data, the disclosure of which 'may dramatically affect' the private and family life of individuals.[195] Additionally, the Court associated the protection in question with a principle 'of confidentiality',[196] and described it as consisting in safeguards to

[191] On the partial recognition of data protection under Article 8 of the ECHR by the ECtHR, see also: (De Hert and Gutwirth 2009, p. 24 ff).

[192] *Z v Finland* [1997] RJD 1997-I, App. No. 22009/93.

[193] Ibid. § 95. See also *M. S. v Sweden* [1997] RJD 1997-IV, App. No. 20837/92, § 51.

[194] In *Z v Finland*, the Court enters into these considerations when examining whether the interferences with Article 8 of the ECHR can be considered 'necessary in a democratic society'. It was undisputed that the various measures of which the applicant complained constituted interferences (*Z v Finland* § 71).

[195] Ibid. § 96.

[196] Ibid. § 95.

prevent some types of communication or disclosure,[197] even though 'data protection' in the sense of Convention 108[198] encompasses principles that go beyond confidentiality obligations.

I v Finland,[199] about the protection of patient records, added a new dimension to what is known as the doctrine of positive obligations in relation to the protection of personal data (De Hert 2009, p. 25). The case concerned an applicant, also diagnosed as HIV-positive, whose confidential patient records had been unlawfully consulted by her colleagues. The applicant complained that the district health authority had failed to provide adequate safeguards against unauthorised access of medical data. In this ruling, the ECtHR recalled that according to its own case law Article 8 of the ECHR does not merely compel States to abstain from interferences with the right to respect for private life, but that there may also be positive obligations inherent in an effective respect for private or family life,[200] and that these obligations may involve the adoption of measures designed to secure the respect for private life even in the sphere of the relations of individuals between them.[201]

4.3.4 Access to Data and Article 8 of the ECHR

Cases such as *Leander* and *Rotaru* concerned not only the storage of information by public authorities, but also the refusal to grant individuals access to the information stored,[202] thus depriving them of the opportunity to refute it.[203] Such refusal of access is also regarded by the ECtHR as an interference with the rights enshrined by Article 8 of the ECHR.[204]

A landmark judgment regarding access to information is *Gaskin*,[205] of 1989. In *Gaskin*, the applicant, who had been taken into care as a child, wished to find out about his past to overcome some personal problems, but had been refused access to his file on the ground that it contained confidential information. The Strasbourg Court found that the applicant had an essential interest in accessing the information at stake, described as relating to the applicant's childhood and formative years and, thus, to his 'private and family life', and eventually established there had been a violation of Article 8 of the ECHR because the decision on denial of access had not been taken by an independent authority (Sudre 2005, p. 409).

---

[197] Ibid.

[198] Some articles of which are expressly mentioned (in particular, Article 6 of Convention 108 on special categories of personal data), stating they are applicable *mutatis mutandis (Z v Finland § 95)*.

[199] *I. v. Finland* [2008] App. No. 20511/03.

[200] *Airey v Ireland* [1979] Series A No. 32, App. No. 6289/73, § 32.

[201] *X and Y v the Netherlands* [1985] Series A No. 91, App. No. 8978/80, § 23.

[202] See, for instance: *Leander* § 48.

[203] *Rotaru* § 46.

[204] See also: *M.G. v the United Kingdom* [2002] App. No. 39393/98.

[205] *Gaskin v the United Kingdom* [1989] Series A No. 160, App. No. 10454/83.

Some regard *Gaskin* as a leading case on the right of individuals, under Article 8 of the ECHR, to access information about them held by public authorities.[206] As a matter of fact, however, in that judgment the ECtHR did not focus its assessment on whether the information was *about* the applicant (in the sense of it being data related to him as an identified individual, or his 'personal data'), but rather on the issue of the impact on his life of not being able to access the information. The Court considered the refusal of access as amounting to an interference not because of the nature of the data, or of the way in which the data were used, but because of the denial of access' potential impact on the life of the applicant, and because the act of accessing the data served an essential interest. In this sense, the Court explicitly emphasised that its judgment shall not be interpreted as providing general guidance on the question of whether general access rights to personal information could be derived from Article 8 of the ECHR.[207]

4.3.5 Integration Through Article 8(2) of the ECHR

Further incorporation into the reading of Article 8 of the ECHR of principles related to the protection of personal data has been developed by the ECtHR in relation to the interpretation of the second paragraph of Article 8 of the ECHR, which describes the requirements for any interference to be legitimate (Nardell 2010, p. 46). In *Liberty*,[208] a case concerning the use of information gathered through the interception of communications, the Strasbourg Court detailed the substance of the requirement of legality (or of being 'in accordance with the law' as per Article 8(2) of the ECHR) in relation to further data processing of intercepted data (Nardell 2010, p. 46).[209] The Court notably connected the compliance with the legality requirement with the need to set out in detail rules on the storing and destroying of data, with a periodical assessment of the necessity to keep data stored, and with special supervision of these rules.[210]

In *S and Marper*, the ECtHR linked the application of personal data protection principles to the compliance with the requirement of measures being regarded as 'necessary in a democratic society'. In this sense, it framed data protection constraints as elements to be taken into account to assess whether data processing measures can be deemed proportional.[211]

[206] Lee A Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' 6 (1998) *International Journal of Law and Information Technology* 247.

[207] *Gaskin* § 37. See also: (Sudre et al. 2004, p. 343).

[208] Liberty and others v the United Kingdom [2008] App. No. 58243/00.

[209] On *Liberty* and legality, see also: (De Hert 2009, pp. 24–25).

[210] Liberty § 68.

[211] Ibid. 49. On proportionality, see also: *Segerstedt-Wiberg*, and (De Hert 2009, p. 26).

4.4 Summary

The activities of OECD and of the Council of Europe in the area of the regulation of data processing can be traced back to the 1960s, and are closely intertwined.

The main outcome of the OECD efforts was the adoption of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These guidelines are concerned with balancing the protection of the privacy of individuals with what was described as the 'free flow' of personal data across frontiers, even if such 'balancing' de facto privileges the promotion of such 'free flow' in the name of free trade. In the OECD context, national norms on the regulation of data processing are typically denominated 'privacy laws'.

The Council of Europe's main instrument is Convention 108, adopted in 1981. Convention's 108 basic approach can be synthesised as establishing a series of rules, labelled as 'data protection', which are presented as serving rights and freedoms in general, but, in particular, a right to privacy. In connection with Convention 108, national norms on data processing are 'data protection' rules, which serve (first and foremost) something called 'privacy'. The right to privacy pursued by data protection rules is, according to Convention 108, the right to respect for private life enshrined by Article 8 of the ECHR.

Under the direct influence of the OECD, Convention 108 echoed the notion of a 'free flow' of data, concretely as in 'free flow of information'. The notion's transposition into a Council of Europe's instrument marked a slight shift in its conception: it became now vaguely linked to the human right to freedom of expression.

The OECD Guidelines and Convention 108 promoted a way of framing the issues at stake that the ECtHR has only followed reluctantly. The ECtHR has over the years expanded its interpretation of Article 8 of the ECHR to encompass the protection of individuals in the face of some information practices, but has never openly and fully embraced the entire scope of application of Convention 108.[212] The Strasbourg Court has avoided the designation of any of the rights established by Article 8 of the ECHR as 'the right to privacy'. So, if it has confirmed by its practice of referring to Convention 108 when discussing Article 8 of the ECHR the perception that 'data protection' is related to the right to respect for private life, it has not clearly delimited how.

Convention 108 obliges ratifying countries to adopt their own legislation in accordance with its provisions. As a result, the notion of 'data protection' spread across Europe, and was notably championed by the UK, which adopted in 1984 its first Data Protection Act, after years of sterile deliberations on the possible acknowledgement of a right to privacy.

As they unfolded, the activities of the OECD and of the Council of Europe increasingly intersected with those of another organisation that began to be active in the field in the early 1970s: the European Communities, later known as the European Union. Chapter 5 is devoted to the involvement of the EU.

[212] Constituting what some have described as a 'somewhat confusing' case law (Bygrave (1998) op. cit. 17).

References

Arzt, Clemens. 2005. Data protection versus Fourth Amendment privacy: A new approach towards police search and seizure. *Criminal Law Forum* 16:183–230.

Bennett, Colin J., and Charles D. Raab. 2003. *The Governance of Privacy: Policy Instruments in Global Perspective*. Aldershot: Ashgate.

Blackburn, Robert. 2001. The institutions and processes of the Convention. In *Fundamental rights in Europe: The European Convention on Human Rights and its Member States, 1950–2000*, eds. Robert Blackburn and Jörg Polakiewicz, 3–29. Oxford: Oxford University Press.

Blume, Peter. 1991. Introduction. In *Nordic studies in information technology and law*, ed. Peter Blume. Deventer: Kluwer.

Braibant, Guy. 1999. Introduction. *Revue française d'administration publique* 89 (janvier- mars) 5–8.

Bureau of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (T-PD). 2011. Modernisation of Convention 108: Proposals, Council of Europe Directorate General of Human Rights and Legal Affairs, T-PD-BUR (2011) 19_en, Strasbourg.

Bygrave, Lee A. 1998. Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology,* 6, 247–284.

Centre d'Informatique pour la Région Bruxelloise (C.I.R.B.). 2004. La protection de la vie privée et le traitement de données à caractère personnel. N°28. Bruxelles.

Commission nationale de l'informatique et des libertés (CNIL). 1982. Rapport au Président de la République et au Parlement 1980–1981, Prévu par l'art. 23 de la Loi du 6 Janvier 1978. La Documentation Française.

Commission on Human Rights of the United Nations Economic and Social Council. 1970. Human rights and scientific and technological developments: Report of the Secretary-General (Addendum 1). E/CN.4/102.

Committee of Ministers of the Council of Europe. 1981. Conclusions of the 336th meeting of the Ministers' Deputies held in Strasbourg from 9 to 11 September 1981, CM/DEL/CONCL(81)336, Strasbourg.

Committee on Legal Affairs and Human Rights. 1968. Human rights and modern scientific and technological developments, Doc. 2326.

Consultative Committee on the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). 2012. Final document on the modernisation of Convention 108, T-PD (2012) 04 Mos., Strasbourg.

Council of Europe's Consultative Assembly. 1949. First session, 10th August—8th September 1949, Part IV, Sittings 16–18, Strasbourg.

Council of Europe's Consultative Assembly. 1950a. Second session, II, 18th-24th November 1950, Reports Part V, Sittings 22–28, Strasbourg.

Council of Europe's Consultative Assembly. 1950b. Ordinary session 1950 (August 1950), Documents: Working papers, Part I, Doc. No. 1, Strasbourg.

Council of Europe's Consultative Assembly. 1953. Committee on General Affairs, fourth session, political review of the years 1945–1953, Documentary Note submitted by the Secretariat-General in relation to the report submitted by M. Spaak (Doc. AS/AG (5) 23) Strasbourg.

Council of Europe's Consultative Assembly. 1967. Eighteenth ordinary session (third part), 23rd–27th January 1967, Documents: Working Papers: Volume VI: Docs. 2160–2169, Strasbourg.

Council of Europe's Consultative Assembly. 1968. Nineteenth ordinary session (third part), 29th January–2nd February 1968, Official Report of Debates, Volume III, Sittings 577–948, Strasbourg.

De Beer de Laer, Daniel, Paul De Hert, Gloria González Fuster, and Serge Gutwirth. 2010. Nouveaux éclairages de la notion de "donnée personnelle" et application audacieuse du critère de proportionnalité, Cour Européenne des Droits de l'Homme, Grande Chambre, S et Marper c. Royaume Uni, 4 décembre 2008. *Revue trimestrielle des droits de l'homme* 81:141–161.

De Hert, Paul. 1998. Mensenrechten en Bescherming van Persoonsgegevens. Overzicht en Synthese van de Europese Rechtspraak 1955–1997. In *Jaarboek ICM 1997*. Antwerpen: Maklu.

De Hert, Paul. 2009. *Citizen's Data and Technology: An Optimistic Perspective*. The Hague: Dutch Data Protection Authority.

De Hert, Paul, and Serge Gutwirth. 2009. Data protection in the case law of Strasbourg and Luxem-bourg: Constitutionalisation in action. In *Reinventing Data Protection*?, eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne, and Sjaak Nouwt, 3–44. Dordrecht: Springer.

De Hert, Paul, and Serge Gutwirth. 2013. *Anthologie de la vie privée*: *Compilation d'articles, de législation et de jurisprudence concernant la protection de la vie privée et des données à caractère personnel pour la Belgique jusque 1998*. Bruxelles: Academic and Scientific Publishers (ASP) & Commission Protection de la Vie Privée.

De Schutter, Olivier. 2001. Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel. *Revue trimestrielle des droits de l'homme* 45:148–183.

De Schutter, Olivier. 2010. *International Human Rights Law*. Cambridge: Cambridge University Press.

European Union Network of Independent Experts in Fundamental Rights. 2006. Commentary of the Charter of Fundamental Rights of the European Union.

Flaherty, David H. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States*. Chapel Hill: University of North Carolina Press.

Gassmann, Hans Peter. 2010. 30 years after: The impact of the OECD Privacy Guidelines. Address to the OECD Joint Roundtable of the Committee for Information, Computer and Communications Policy (ICCP), and its Working Party on Information Security and Privacy (WPISP). www.oecd.org/sti/interneteconomy/44945922.doc. Accessed 10 March 2013.

González Fuster, Gloria. 2009. TJCE—Sentencia de 04.12.2008, S. y Marper c. Reino Unido. *Revista de Derecho Comunitario Europeo* 33 (mayo-agosto): 619–633.

Hondius, Frits W. 1975. *Emerging Data Protection in Europe*. Amsterdam: North-Holland Publishing Company.

Hondius, Frits W. 1978. The Council of Europe's work in the area of computers and privacy (Discussion paper for the round table on the use of data processing for parliamentary work, Strasbourg, 18–19 May 1978). Strasbourg: Parliamentary Assembly of the Council of Europe.

Jacqué, Jean-Paul. 1980. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. *Annuaire Français de Droit International* 26:773–789.

Kirby, Michael Donald. 1980. International guidelines to protect privacy in transborder data flows. Australian & New Zealand Association for the Advancement of Science, Jubilee Congress, Adelaide, 15 May 1980.

Kirby, Michael Donald. 2010a. The OECD Privacy Guidelines @ 30. Organisation for Economic Co-operation and Development.

Kirby, Michael Donald. 2010b. The history, achievement and future of the 1980 OECD Guidelines on privacy. Presentation at round table on the 30th anniversary of the OECD Guidelines on privacy. Paris: Organisation for Economic Co-operation and Development.

Kranenborg, Herke. 2008. Access to documents and data protection in the European Union: On the public nature of personal data. *Common Market Law Review* 45 (4): 1079–1114.

Kuner, Christopher. 2011. Regulation of transborder data flows under data protection and privacy law: Past, present and future. OECD Digital Economy Papers No. 187. OECD Publishing.

Lageot, Céline. ed. 2008. *Dictionnaire plurilingue des libertés de l'esprit (Bruylant 2008)*. Bruxelles: Bruylant.

Lewis, Arthur. 1980. Opinion of the Committee on legal affairs and human rights on data processing and the protection of human rights, Doc. 4484.

Martínez Martínez, Ricard. 2004. *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson Civitas.

Michael, James. 1994. *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*. Aldershot: Dartmouth/UNESCO.

Nardell, Gordon Q. C. 2010. Levelling up: Data privacy and the European Court of Human Rights. In *Data protection in a profiled world*, eds. Serge Gutwirth, Yves Poullet, and Paul De Hert, 43–52. Dordrecht: Springer.

Ooverkleeft-Verburg, Margriet. 1995. De Wet Persoonsregistraties Norm, toepassing en evaluatie. Tilburg: Katholieke Universiteit Brabant. http://www.overkleeft-verburg.nl/publicatiesproefschrift.htm. Accessed 10 March 2013.

Parliamentary Assembly of the Council of Europe. 1980. Report on data processing and the protection of human rights. (Rapporteur: Mr Holst), Doc. 4472.

Pavón Pérez, Juan Antonio. 2002. La protección de datos personales en el Consejo de Europa: El Protocolo Adicional al Convenio 108 relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos Personales. *Anuario de la Facultad de Derecho* 19–20:235–252.

Peers, Steve. 2006. *EU Justice and Home Affairs Law*. 2nd ed. Oxford: Oxford University Press.

Prieto Gutiérrez, Jesús María. 1998. La Directiva 95/46/CE como criterio unificador. *Informática y Derecho (Revista Iberoamericana de Derecho Informático)* 23–26:1091–1173.

Registry of the Council of Europe. 1967. Travaux préparatoires de l'article 8 de la Convention européenne des droits de l'homme—European Court of Human Rights: Preparatory work on Article 8 of the European Convention on Human Rights (Bilingual Information Document), CDH (67) 5, Strasbourg.

Reidenberg, Joel, and Paul M. Schwartz. 1998. *Data Protection Law and On-Line Services: Regulatory Responses*. European Commission.

Robben, Frank, and Jos Dumortier. 1992. General consideration of the Belgian data protection bill of May 1991. In *Recent developments in data privacy law (ICRI N°2)*, 59–78. Leuven: Leuven University Press.

Simitis, Spiros. 2006. Einleitung: Geschichte—Ziele—Prinzipien. In *Bundesdatenschutzgesetz*, ed. Spiros Simitis, 61–153. Baden Baden: Nomos.

Sizer, Richard, and Philip Newman. 1984. *The Data Protection Act: A Practical Guide*. Aldershot: Gower.

Solove, Daniel J., Marc Rotenberg, and Paul M. Schwartz. 2006. *Information Privacy Law*. 2nd ed. New York: Aspen Publishers.

Sudre, Frédéric. 2005. *Droit européen et international des droits de l'homme*. 7th ed. Paris: Presses Universitaires de France.

Sudre, Frédéric, Jean-Pierre Marguénaud, Joël Andriantsimbazovina, Adeline Gouttenoire, and Michel Levinet. 2004. *Les grands arrêts de la Cour européenne des Droits de l'homme*. 2nd ed. Paris: Presses Universitaires de France.

The Privacy Protection Study Commission. 1977. *Personal privacy in an information society: The report of the Privacy Protection Study Commission*. Washington, D.C.: US Government Printing Office, 1977.

Working Party for Information Security and Privacy (WPISP). 2011. The evolving privacy landscape: 30 years after the OECD Privacy Guidelines. Directorate for Science, Technology and Industry—Committee for Information, Computer and Communications Policy, DSTI/ICCP/REG(2010)6/FINAL,6.4.2011. DSTI/ICCP/REG(2010)6/FINAL.

Zerdick, Thomas. 1995. European aspects of data protection: What rights for the citizen? *Legal Issues of European Integration* 2:59–86.