Constitutional Rights and New Technologies

A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States

Edited by
Bert-Jaap Koops
Ronald Leenes
Paul De Hert

Tilburg, February 2007

TILT – Tilburg Institute for Law, Technology, and Society
P.O. Box 90153 • 5000 LE Tilburg • The Netherlands
T +31 13 466 81 99 • **W** www.uvt.nl/tilt • **E** info-tilt@uvt.nl

Constitutional Rights and New Technologies

A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States

Bert-Jaap Koops, Ronald Leenes & Paul De Hert (eds.)

with contributions by

Susan W. Brenner
Fanny Coudert
Anne Debet
Paul De Hert
Thomas Hoeren
Els Kindt
Bert-Jaap Koops
Eleni Kosta
Ronald Leenes
Thomas Leys
Eva Lievens
Cecilia Magnusson Sjöberg
Anselm Rodenhausen
Jason Young

report commissioned by the Dutch Ministry of the Interior and Kingdom Relations

Tilburg, February 2007

Table of Contents

Abbreviations

¶	Randnummer (consecutive number within the commentary of an Article of the German Constitution)
AfP	Archiv für Presserecht
AG	Die Aktiengesellschaft
AöR	Archiv des öffentlichen Rechts
API/PNR	Advance Passenger Information/Passenger Name Record (Canada)
Arbrb.	Arbeidsrechtbank (Labour Court, Belgium)
Arr.Cass.	Arresten Cassatie (decisions Supreme Court, Belgium)
B.S.	Belgisch Staatsblad (Official Journal, Belgium)
BAG	Bundesarbeitsgericht (Federal Labour Court, Germany)
BB	Der Betriebsberater
Bd.	Band (volume)
BGH	Bundesgerichtshof (Federal Court of Justice, Germany)
BGHSt	Amtliche Entscheidungssammlung des Bundesgerichtshofs in Strafsachen (Official compilation of the decisions of the Federal Court of Justice in criminal matters, Germany)
BGHZ	Amtliche Entscheidungssammlung des Bundesgerichtshofs in Zivilsachen (Official compilation of the decisions of the Federal Court of Justice in civil matters, Germany)
BNA	British North America (Canada)
Bull. Civ.	Bulletin des arrêts de la Cour de Cassation, chambres civiles (decisions of the Supreme Court, Civil-Law Section, France)
Bull. crim.	Bulletin des arrêts de la Cour de Cassation, chambre criminelle (decision of the Supreme Court, Criminal-Law Section, France)
BVerfGE	Amtliche Entscheidungssammlung des Bundesverfassungsgerichts (Official compilation of the decisions of the Federal Constitutional Court, Germany)
BVerwG	Bundesverwaltungsgericht (Federal Administrative Court, Germany)
CA	Cour d'Appel (Appeal Court, France)
Cass. Crim.	Cour de Cassation, Chambre criminelle (French Supreme Court, Criminal-Law Section)
Cass. Soc.	Cour de Cassation, Chambre Sociale (French Supreme Court, Labour-Law Section)
Cass.	Cassatie (Supreme Court, Belgium)
CBC	Canadian Broadcasting Corporation
CBS	Canadian Blood Services
CBSA	Canada Border Services Agency
CC	Criminal Code
CCP	Code of Criminal Procedure
CDRP	Canadian Internet Registration Authority Domain Name Dispute Resolution Policy
Ch.	Chambre (section of a court, France)
CIRA	Canadian Internet Registration Authority
CNIL	Commission Nationale Informatique et Libertés (French Data Protection Authority)
cons.	consideration
Corr.Rb.	Correctionele rechtbank (Lower Penal Court, Belgium)
CR	Computer und Recht
DC	Décision du Conseil Constitutionnel (Decision of the Constitutional Council, France)
DÖV	Die Öffentliche Verwaltung
DRM	Digital Rights Management
DuD	Datenschutz und Datensicherung
DVBl	Deutsches Verwaltungsblatt
EC	European Community
ECHR	European Convention of Human Rights
ECPA	Electronic Communications Privacy Act (US)
ECtHR	European Court of Human Rights
EU	European Union
FDA	Food and Drug Administration (US)
FLFE	Fundamental Law on Freedom of Expression (Sweden)
FLIR	Forward Looking Infrared (Canada)
FNR	Fin de non recevoir (case not admitted by the Court, France)
FPA	Freedom of the Press Act (Sweden)
GPS	Global Positioning System
HRDC	Human Resources Development Canada
HStR	Handbuch des Staatsrechts für die Bundesrepublik Deutschland

HTML	HyperText Markup Language
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications Technology
IG	Instrument of Government (Sweden)
IMSI	International Mobile Subsciber Identity
ISP	Internet Service Provider
JA	Juristische Ausbildung
JCP Ed. G	Jurisclasseur, édition Générale
JO	Journal Officiel (French Official Journal)
JuS	Juristische Schulung
K&R	Kommunikation und Recht
k.	kamer (section of a court, Belgium)
KG	Kammergericht (Court of Appeal for the district of Berlin, Germany)
LG	Landgericht (county court, Germany)
MITA	Modernization of Investigative Techniques Act (Canada)
MMR	MultiMedia und Recht
NJA	Nytt Juridiskt Arkiv (decisions of the Supreme Court, Sweden)
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OLG	Oberlandesgericht (Higher Regional Court, Germany)
P2P	peer-to-peer
Parl.St.	Parlementaire Stukken (Parliamentary Documents, Belgium)
PDA	Personal Data Act (Sweden)
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PKI	Public Key Infrastructure
R.W.	Rechtskundig Weekblad
RÅ	Regeringsrättens Årsbok (decisions of the Supreme Administrative Court, Sweden)
Rb.	Rechtbank (Lower Court, Belgium)
RCMP	Royal Canadian Mounted Police
RDV	Recht der Datenverarbeitung
Rec.	Recours (Judicial Process, France)
ref.	Referat (review, Sweden)
RFID	Radio Frequency Identification
s.	section
SEK	Svensk Krona (Swedish Crown)
SFS	Svensk FörfattningsSamling (Swedish Code of Statutes)
SMS	short message service
SOIA	Security of Information Act (Canada)
StPO	Strafprozessordnung (Code of Criminal Procedure, Germany)
SuP	Sozialrecht + Praxis
TGI	Tribunal de Grande Instance (French Higher District Court)
TJK	Tijdschrift voor Jeugdrecht en Kinderrechten
TKG	Telekommunikationsgesetz (Telecommunications Act, Germany)
TSP	Telecommunications Service Provider
UDRP	Uniform Domain Name Dispute Resolution Policy
US	United States of America
VGH	Verwaltungsgerichtshof (Higher Administrative Court, Germany)
viWTA	Vlaams Instituut voor Wetenschappelijk en Technologisch Aspectenonderzoek (Flemish Parliamentary Technology Assessment Institute)
VoIP	Voice over Internet Protocol
WIPO	World Intellectual Property Organization
WRP	Wettbewerb in Recht und Praxis
XML	eXtensible Markup Language
ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht

1. Introduction[1]

Ronald Leenes,[2] Bert-Jaap Koops,[3] Paul de Hert[4]

1.1. Digital constitutional rights in the Netherlands

The introduction of the Internet for ordinary citizens, businesses, and governments in the early 1990s has had serious consequences for society. The issue of protecting fundamental human rights in the digital era was placed firmly on scientific and political agendas in the mid-1990s.

This was particularly the case in the Netherlands, where a dissertation on secrecy of communications by Hofman, for instance, spurred much debate in 1995.[5] A subsequent proposal for a limited amendment, confined to Article 13, of the Dutch Constitution was proposed and subsequently withdrawn during parliamentary deliberation.[6] This was not only the result of problems with respect to the content of the proposal itself, but also of the hasty process used in trying to amend the Constitution. Public debates had not been held, and also advice by a state committee was lacking, both of which were deemed inappropriate for a constitutional amendment.[7] To address these shortcomings, the government instituted a Committee for Constitutional rights in the digital era (*Commissie Grondrechten in het digitale tijdperk*), which was given the task of analyzing the consequences for fundamental human rights of the introduction of the digital era, and to propose amendments to the Constitution where necessary or appropriate. The committee's final report was presented to the government in 2000,[8] with proposals for amending Articles 7, 10, and 13 of the Dutch Constitution, as well as for introducing the right to access government documents as a new constitutional right. This new constitutional right would introduce an obligation for the state to actively disseminate public-sector information. The Committee also proposed smaller amendments to other provisions affected by ICT developments.

The report triggered some parliamentary debate[9] and gave rise to four government draft proposals for constitutional reform, which were submitted to the Council of State in 2001. In these drafts, the government adopted the majority of the Committee's proposals, putting aside considerable criticism by various, largely academic, sources about the Committee's proposals.

It has been relatively quiet since then. The draft proposals were not submitted to parliament, and the process of changing the constitution in light of ICT has come to a halt, or so it seems. This pause was partly due to international developments with respect to fundamental rights in the digital era. The Committee of Ministers of the Council of Europe had adopted the *Declaration on freedom of communication on the Internet* in 2003,[10] which affects the policy developments with respect to freedom of speech and anonymity. The possible implementation of the declaration is subject of a study of the Group of Specialists on Human Rights in the Information Society (MC-SIS). The World Summits on the Information Society in Genève (2003) and Tunis (2005) has

[1] This report was commissioned by the Dutch Ministry of the Interior and Kingdom Relations. The research for this report was finalised by 1 December 2006; later developments have been included only incidentally. The text of the report was finalised on 1 February 2007.
[2] Ronald Leenes is Associate Professor in Law & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands.
[3] Bert-Jaap Koops is Professor in Regulation & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands.
[4] Paul de Hert is Associate Professor in Law & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands, and Professor at Law, Science, Technology & Society (LSTS), Free University of Brussels, Belgium.
[5] J.A. Hofman, *Vertrouwelijke communicatie: een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht* (Zwolle, W.E.J. Tjeenk Willink 1995).
[6] *Kamerstukken II* [Dutch Parliamentary Series, Second Chamber] 1996/97, 25 443, Nos. 1-2 et seq.
[7] *Kamerstukken I* [Dutch Parliamentary Series, First Chamber] 1998/99, 25 443, No. 40.
[8] Commissie Grondrechten in het digitale tijdperk, *Rapport*, May 2000, available at http://www.min-bzk.nl/gdt/artikelen/rapport_gdt_5-00.pdf.
[9] *Kamerstukken II* [Dutch Parliamentary Series, Second Chamber] 2000/01, 27 460, No. 2.
[10] Council of Europe, Committee of Ministers, *Declaration on freedom of communication on the Internet*, 28 May 2003, available at http://www.unesco.nl/images/freedcominternet.pdf.

addressed fundamental rights in the digital era, including freedom of speech and privacy, although not in detail. Moreover, a small number of academic studies have been published in the Netherlands, for instance with respect to the communication rights,[11] the impact of ICTs on other fundamental human rights,[12] and anonymity.[13]

1.2. Developments in technology

Meanwhile, technical developments have continued. Mobile phones have become common in the late 1990s and are currently replacing traditional fixed telephones as the principal means of telephony. Mobile communication differs from traditional telephony in a number of ways. Mobile phones are, for instance, personal instead of bound to a location where they are likely to be shared by multiple individuals, like in a family. This implies that conversations involving a mobile phone are likely conducted by the owner of the device. Furthermore, the approximate location of the device is known to the communication service provider, which means that also the current location of the device's owner is known. And finally, mobile phones contribute to 24x7x365 availability of their users. Telephony is also moving across the Internet, with Voice over IP (VoIP). Whereas traditional telephony, including GSM, can easily be wiretapped, this is not the case with most VoIP systems, such as Skype. VoIP therefore differs from other forms of telecommunication with respect to confidentiality of the communication.

These types of developments affect discussions with respect to a constitutional right to anonymity and the protection of so-called traffic data – two controversial issues in the late 1990s debate over amending the Dutch Constitution. These issues have received new input since; new arguments in favour of a right to anonymity have been put forward,[14] and also arguments favouring equal treatment (i.e., equal protection) of traffic data and content have been issued.[15] As a result of technological developments, possibilities for monitoring telecommunication, as well as the scope thereof, change. This calls for a reflection on the fundamental rights to confidential communication and privacy protection.

Also with respect to other Internet applications, significant changes can be witnessed since the end of the 1990s that may affect constitutional rights. Peer-to-peer (p2p) networks facilitate information exchange without easy means to reveal sender and recipient. Google has become synonymous with searching the Internet. The flipside is that Google retains an enormous amount of information on the content of the Internet, as well as on the information needs of its users. Both Google's search capabilities and the possibilities to use its logfiles to study the information needs, and thereby the preferences, of its users, raises serious questions with respect to their privacy. The US government, for instance, in early 2006, requested search engine providers, including Google, Yahoo, and AOL, to provide large amounts of search queries to establish how easy it is for users of search engines to locate online porn. Moreover, Google and other search engines also play a role in the debates on other constitutional rights. They filter information on request of the Chinese government which aims to ban politically sensitive material and porn, which practically means that they operate as a censor. The considerable effects on society and the economic interests of search engines, such as Google, call for critical reflection.[16]

The means to enter the individual's private sphere also evolve in the physical world. Communication by individuals is increasingly carried out by means of electronic devices, such as computers, (mobile) phones, and PDAs. These devices communicate by means of cables and also wireless. Both can (unobtrusively) be monitored remotely. This means that private communication in the home can be monitored from the outside without the subjects being aware

[11] Lodewijk Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2002.
[12] Bert-Jaap Koops, Hanneke van Schooten and Merel Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004, 221 p.
[13] Anton Ekker, *Anoniem communiceren: van drukpers tot weblog*, Den Haag, Sdu Uitgevers 2006, available at http://dare.uva.nl/document/19656.
[14] Ibid.
[15] A.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen: Wolf Legal Publishers 2006.
[16] See N.A.N.M. Van Eijk, *Zoekmachines: zoekt en gij zult vinden? Over de plaats van zoekmachines in het recht*, inaugural lecture Amsterdam (UvA) (Amsterdam, Otto Cramwinckel Uitgever 2005).

of this. This kind of unobtrusive eavesdropping is possibly not covered by the constitutional right to inviolability of the home.[17]

Advanced equipment, such as microwave scanners, can see through clothing to reveal weapons carried on the body of the subject. These devices are currently being tested in airports. TNO – a Dutch governmental research institute – is developing terrahertz scanners that can see right through walls. This allows the detection of people in a room. These uses again pose questions with respect to the constitutional rights to inviolability of the body and inviolability of the home.[18]

1.3. Scope and research question

These examples show some technical developments that may affect fundamental human rights of individuals in the digital era. This is compounded by the fact that other technologies, notably biotechnology, also impact human rights, triggering the question whether the Constitution should be adapted not only in the light of ICT but also with a view to other technological developments. The issue of adapting the Dutch Constitution is therefore even more relevant today than it was a few years ago.

The Dutch government has acknowledged this and has decided that constitutional changes may be required to update the Constitution to the requirements of new technologies. This is a complex task, and because relevant developments are global rather than neatly confined to the Netherlands, it is useful to study other countries to see which questions have arisen there and how developments in new technologies are dealt with in light of constitutional rights. As a result, the Dutch Ministry of the Interior and Kingdom Relations has commissioned a comparative study of six countries with respect to a number of fundamental rights that are affected by technological developments. The findings will be used to develop recommendations for modifying the Dutch Constitution.

This report offers the result of the comparative study. It is a sequel to an earlier study carried out in 1999-2000 under supervision of Alis Koekkoek of Tilburg University,[19] which was used by the Committee for Constitutional rights in the digital era. The present study contains the same six countries – Belgium, Canada, France, Germany, Sweden, and the US – and builds on the findings of the Koekkoek report. The goal of this study is to study changes in constitutional rights and human-rights policy related to developments in ICT and new technologies. It focuses in particular on the constitutional rights to freedom of expression, privacy and data protection, inviolability of the body, inviolability of the home, and secrecy of communication.[20]

The **research question** central to this study is twofold.

> Which developments have taken place in Belgium, Canada, France, Germany, Sweden, and the US with respect to constitutional rights and new technologies, in particular since 2000? And which recommendations for the Dutch legislator can be distilled from these developments?

The emphasis in this report is on the first question. To answer this question, experts in the six countries have written country reports, showing the state of affairs in their countries as of late November 2006. The central research question was decomposed in a number of sub-questions that have guided the country reporters in writing their chapters.

a. Have significant changes to the constitutional system taken place, in particular since 2000, for instance with respect to constitutional review, horizontal effect, or influence of international law?
b. Are there any changes with respect to freedom of expression, privacy, inviolability of the body, inviolability of the home, and freedom of communication, in particular since 2000?

---

[17] Koops et al. 2004, op. cit. n. 12.
[18] Ibid.
[19] A. Koekkoek, P. Zoontjens, et al., *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport* [Protection of fundamental rights in the digital age. A comparative study to the freedom of information and of communication and privacy in Sweden, Germany, France, Belgium, The United States of America and Canada], Tilburg, Katholieke Universiteit Brabant, 2000, 255 p.
[20] The rights laid down in Articles 7, 10, 11, 12, and 13 of the Dutch Constitution, respectively.

c. What are the policy developments in the country at issue with respect to constitutional rights and new technologies?
d. What are the most relevant issues with respect to constitutional rights in legislative, legal academic, and public debates? For instance, are debates focused on the 'traditional' rights, or do debates concern new fundamental rights, for instance regarding biotechnology?

The second question was addressed by means of an international workshop with the country reporters, which was held on 1 December 2006 in The Hague, the findings of which have been used to write the conclusion and recommendations of this report.

1.4. Background: the Koekkoek report of 2000

As mentioned, this study builds on an earlier study commissioned by the Dutch Ministry of Justice to a Tilburg University research group headed by Alis Koekkoek in 1999. In this section, we provide a brief overview of the findings of this study, which we will refer to as the Koekkoek report.[21]

The Koekkoek report started from the following research question.

> Have developments with respect to information and communication technologies led to amendments in constitutional rights and/or legislation bearing on constitutional rights in the countries in the sample?

The research was limited to privacy (art. 10 Dutch Constitution), freedom of expression (art. 7 Dutch Constitution), freedom of communication (related to art. 13 Dutch Constitution), and the right to access government information. The constitutional rights relating to inviolability of the body and inviolability of the home were not part of the study. In each of the countries in the study, Sweden, Germany, France, Belgium, the United States of America, and Canada, the following topics were addressed:

- policy developments regarding the protection of constitutional rights in relation to ICT developments;
- the system of constitutional rights;
- public debates relating to constitutional amendments in the light of ICT developments;
- the constitutional protection of freedom of expression/freedom of communication and privacy;
- the protection of freedom of expression/freedom of communication and privacy in legislation;
- the protection of freedom of expression/freedom of communication and privacy by courts; and
- the impact of International and European law on the protection of freedom of expression/freedom of communication and privacy.

In this section, we provide a summary of the findings of the 2000 report to offer a springboard for the current country reports of 2006.

Policy developments

ICT developments in the 1980s and 1990s have spurred debates with respect to freedom of expression and new media, the impact of ICTs on privacy and data protection, hate speech on the Internet, and online distribution of child pornography in all countries in the study.

On the brink of the new millennium, many countries have issued policy documents for promoting the information society, e-commerce, e-government, and stimulating new media. Noticeable in these initiatives are an emphasis on facilitating universal access (e.g., Sweden, France, the US, Canada), guaranteeing and promoting access to public information (Sweden, Germany, France, the US), and self-regulation as an important way of regulating the Internet and new media (France, US), implying a limitation for state intervention.

Constitutional systems and the position of 'digital rights'

To understand whether ICT developments have, or should have, an impact on constitutional rights, it is necessary to understand the constitutional systems in the various countries, for

[21] Koekkoek et al. 2000, op. cit. n. 19

example, whether there is constitutional review by a constitutional court or (lower) courts, and how international and European law relate to national law.

In the decentralised unitary states – Sweden and France – constitutional rights are addressed in a limited set of documents. In federal states – Belgium, Germany, Canada, and the US – constitutional rights are vested on the federal level as well as on the level of 'Bundesländer', provinces, or states. The federal constitution determines the jurisdiction of the lower levels. The **Swedish** set of constitutional documents (the Regeringsform, the Act of Succession, the Freedom of the Press Act, and the Fundamental Law on Freedom of Expression) contain the rights to privacy, freedom of expression/communication, inviolability of the body, and inviolability of the home, as well as access to public information. In **France**, the constitution itself does not mention fundamental rights. According to the constitution's preamble, these can be constructed from the 1789 'Déclaration des droits de l'homme en du citoyen' and the preamble of the 1946 Constitution. As a result of this, the protection of fundamental rights is a matter of the (non constitutional) legislator and the courts. The **German** Grundgesetz plays a pivotal role in the protection of fundamental rights. It contains a system of rights (order) and assigns powers to the Bund (postal affairs, telecommunications, competition law, intellectual property, and copyright) and the Länder (most culture-related topics, such as media and the press). The **Belgian** constitution contains provisions relating to information, communication, and privacy, resembling the Dutch constitution. The **US** constitution sees to freedom of speech (1st Amendment) and, by virtue of Supreme Court decisions, also to privacy (5th and 14th Amendment). Privacy protection concerns vertical relations only. In horizontal relations, regulation is left to self-regulation in the market. Access to public information is guaranteed by the Freedom of Information Act. In **Canada**, fundamental rights are included in the Charter of Rights and Freedoms, which contains freedom of thought, belief, opinion, and expression. Privacy protection is thought to be entailed by article 8, which reads 'Everyone has the right to be secure against unreasonable search and seizure'.

The conclusion that can be drawn from this summary is that fundamental rights are protected on the constitutional level in most countries in the study. The role of protection at this level partly depends on whether there is constitutional review by the courts. There appears to be much variance between the countries in the study in this respect. Constitutional review can be *ex ante* (by the legislator, e.g., Sweden) or *ex post* (by the Constitutional Court, e.g., Germany, or by any court, e.g., Canada). Review can be abstract (not related to a particular case, e.g., Germany) or case-based (e.g., the US). Constitutional review allows affected individuals to address the court in order to correct encroachments, or it allows unconstitutional legislation to be questioned before a court. Constitutional review therefore plays a role in the actual enforcement of constitutional rights. Especially in countries without constitutional review, this function has to a large extent been performed on the basis of lower legislation and international law. In all countries, legislation dealing with the various 'digital' rights on the level of ordinary legislation can be found.

All countries in the study are signatory to the International Covenant on Civil and Political Rights (ICCPR), and the European countries are signatory to the European Convention on Human Rights (ECHR). These conventions cover freedom of expression (art. 19 ICCPR, art. 10 ECHR) and privacy (art. 17 ICCPR, art. 8 ECHR). In Sweden, conventions have to be implemented into national law. The ECHR, however, has received constitutional status by means of a clause in the Regeringsform. Conventions also have to be implemented into national law in Germany and Canada. In Germany, the ECHR has the status of normal legislation, subordinate to the Grundgesetz. In Canada, the ECHR plays a role in the interpretation of the Charter. France, Belgium, and the US have a monist system, meaning that conventions have equal or higher standing than the constitution if they are self-executing. The US considers the ICCPR not to be self-executing, whereas France and Belgium have taken both the ICCPR and the ECHR to be self-executing, thus placing them above their constitutions. In monist countries, especially if they lack constitutional review, such as the Netherlands, or have only limited constitutional review, conventions allow for a pseudo-constitutional review.

The European Data Protection Directive, 95/46/EC, which covers informational aspects of privacy protection, has been implemented in national legislation in Sweden and Belgium, whereas the implementation was not yet completed in Germany and France in 2000.

Changes in legislation prior to 2000

Technical and societal developments have led to changes in 'ordinary' legislation as well as to forms of self-regulation. Self-regulation is promoted by Article 27 of Directive 95/46/EC, which marks a radical change in mode of regulation for countries such as Sweden and Germany. Self-regulation is typical in the US, whereas Canada has a mixed mode; a code (PIPEDA) proposed by industry was adopted by the Standards Council of Canada and practically serves as proper legislation.

In a number of countries, e.g., Germany and the US, legislation was adopted with respect to civil and criminal liability of access, service, and content providers, and to protect children against harmful online content, although several attempts were deemed unconstitutional in the US (*UCLA* v. *Reno I & II*).

Access to public information is guaranteed at the constitutional level only in Sweden (extensively) and in Belgium. Swedish, French, and Belgian (federal) legislation pertaining to public information include access to electronic documents. The Freedom of Information Act (FOIA) in the US was amended in 1996 to include electronic access and electronic documents. The Canadian Access to Information Act of 1983 applies to electronic documents as well. No access right to public information exists in Germany.

Constitutional revision up to 2000

Up to 2000, there has been little discussion on constitutional revisions in the light of ICT developments in the countries studied. In some countries, e.g., the US, the constitutional provisions are so abstract or broad that changes are deemed unnecessary. The existing constitution is considered to offer courts sufficient guidance for protecting fundamental rights in the digital era. In other countries, e.g., Sweden and Belgium, provisions have been amended to make them more technology-neutral. With respect to the various rights, the following developments can be witnessed.

- *Freedom of information and freedom of communication.* Sweden has amended Article 2:1 of the Regeringsform 1974 to read 'The freedom to communicate information and to express ideas opinions and emotions, whether orally, in writing, in pictorial representations, *or in any other way'* [emphasis added]. This italicized addition makes the provision technology-neutral. Sweden also introduced the Fundamental Law on Freedom of Expression in 1991 as part of their constitution. Germany, France, and the US consider changing their constitution unnecessary in this respect. The German Article 5 Grundgesetz and the US freedom of speech provision (1st Amendment) are sufficiently abstract to accommodate new technologies, whereas the French protection of freedom of speech is based on lower legislation and active courts. The Conseil d'État (high advisory board to the government), in a 1998 advice, proclaimed that radical changes in legislation as a result of Internet developments were unnecessary. Belgium is preparing a change of Article 25 of the Constitution to incorporate a technology-neutral catch-all. The Canadian Charter of Rights and Freedoms of 1982, in Art 2(b), also contains an open technology-neutral formulation: 'freedom of the press and *other media of communication*' [emphasis added].
- *Privacy.* Also with respect to the constitutional protection of privacy, different reactions to ICT developments can be witnessed in the six countries. In France and the US, case law provides sufficient guidance to handle new kinds of privacy breaches. Article 8 of the Canadian Charter (protection against unreasonable searches and seizures) is considered capable of handling new kinds of breaches. Sweden has modified Art. 2:3 Regeringsform to incorporate 'by means of electronic data protection', and Article 2:6 to read 'Citizens shall likewise [in their relation with the public administration] be protected against physical search, house searches, or other similar encroachments and against examination of mail or other confidential correspondence and against eavesdropping, telephone-tapping or recording of other confidential communications'. ICT developments have given rise to changes in German Art. 13 Grundgesetz (inviolabilty of the home) to allow for direct eavesdropping in houses in serious crimes. Human dignity (Art. 1 Grundgesetz) and free development of one's personality (Art. 2 Grundgesetz) are formulated abstractly and are considered to give

guidance with respect to new technological developments. These rights are the foundations for the German approach of informational self-determination. The German provision safeguarding secrecy of communication (Art. 10 Grundgesetz: 'Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich') is considered to be in need of broadening its scope to include all forms of communicationunder the term 'Fernmeldegeheimnis'.

- *Access to public information.* Sweden's Freedom of the Press Act has provided a technology-neutral provision since the 1970s. Documents can have any form according to Art. 2:3. The IT Commission has advised to replace 'public document' by 'public data' to make it even more technology-neutral. Belgium also has a technology-neutral provision: Article 32 of the Constitution relates to the right to access any public document (*bestuursdocument*). 'Public document' is defined in a federal law to encompass all available information, therefore including automatically processed data. The other countries do not have a constitutional right to access public information, although – with the exception of Germany – this right is present in lower legislation.

References

Lodewijk Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2002.

Commissie Grondrechten in het digitale tijdperk, *Rapport*, May 2000, available at http://www.min-bzk.nl/gdt/artikelen/rapport_gdt_5-00.pdf.

Anton Ekker, *Anoniem communiceren: van drukpers tot weblog*, Den Haag, Sdu Uitgevers 2006, available at http://dare.uva.nl/document/19656.

J.A. Hofman, *Vertrouwelijke communicatie: een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht* (Zwolle, W.E.J. Tjeenk Willink 1995).

A. Koekkoek, P. Zoontjens, et al., Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport [Protection of fundamental rights in the digital age. A comparative study to the freedom of information and of communication and privacy in Sweden, Germany, France, Belgium, The United States of America and Canada], Tilburg, Katholieke Universiteit Brabant, 2000, 255 p.

Bert-Jaap Koops, Hanneke van Schooten and Merel Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004, 221 p.

A.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen: Wolf Legal Publishers 2006.

N.A.N.M. Van Eijk, *Zoekmachines: zoekt en gij zult vinden? Over de plaats van zoekmachines in het recht*, inaugural lecture Amsterdam (UvA) (Amsterdam, Otto Cramwinckel Uitgever 2005).

Chapter 2. Constitutional Rights and New Technologies in Belgium

Els Kindt,[1] Eva Lievens,[2] Eleni Kosta,[3] Thomas Leys,[4] Paul De Hert[5]

2.1. Introduction[6]

The Belgian Constitution provides a limited catalogue of constitutional rights, drafted in very general terms. Due to historical factors, a lot of attention in the Constitution is oriented towards freedom of expression and related values. The fundamental rights of privacy and access to documents have only been added in the Constitution in 1994. A true Constitutional Court was erected just recently, in 2003. Due to this, the general constitutional framework has remained rather abstract, a situation that has given the legislator a considerable amount of discretion. The adaptation of Belgian law to the new circumstances has therefore been relatively easy and has not required constitutional modifications. Besides, concerns raised by new technologies are not usually addressed at a constitutional level, but at a lower level, by administrative or judicial authorities, when it comes to the application of the rules.

Since the report directed by Alis Koekkoek in 2000 (hereinafter: the Koekkoek report of 2000),[7] many interesting legal and non-legal developments have occurred with direct or indirect consequences for our theme:

- the establishment of a true constitutional court and the rediscovery of existing constitutional rights in a legal system that had established a tradition of referring to international sources such as the European Convention of Human Rights (hereinafter: ECHR) and its dynamics due to the work of the European Court of Human Rights;
- the recognition of horizontal effect of constitutional privacy-rights in case law;
- the federal system entering a more mature phase;
- a long period of a liberal-led coalition focusing on technological progress, development of the information society and liberalization of ethical constraints (abortion, euthanasia); and
- the confrontation with technology not in terms of digital constitutional rights, but rather in terms of governance, money, and democracy.

2.2. History of digital constitutional rights

2.2.1. Before 2000

Belgium is a federal state that was formed as a constitutional monarchy in 1830, with a civil-law system strongly influenced by French law. It has had a written Constitution since 7 February 1831. The Constitution contains general principles of the federal system, including provisions protecting individuals from abuse of power. It also lays down the principal functions of legislative,

[1] Els Kindt is a legal researcher at the Interdisciplinary Centre for Law & ICT of the K.U. Leuven (ICRI) in Leuven – IBBT (Institute for BroadBand Technology), Belgium.
[2] Eva Lievens is a legal researcher at ICRI – IBBT. She is preparing a PhD on the protection of minors in new media and the regulatory instruments used to deal with this issue.
[3] Eleni Kosta is a legal researcher and PhD candidate at ICRI – IBBT.
[4] Thomas Leys is a legal researcher at ICRI – IBBT.
[5] Paul de Hert is Associate Professor in Law & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands, and Professor at Law, Science, Technology & Society (LSTS), Free University of Brussels, Belgium.
[6] The ICRI researchers were responsible for sections 2.4.1, 2.5, and 2.6.1–3. The TILT researcher was responsible for sections 2.1-3, 2.4.2–3, 2.6.4–5, and 2.7.
[7] A. Koekkoek, P. Zoontjens, et al., *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport* [Protection of fundamental rights in the digital age. A comparative study to the freedom of information and of communication and privacy in Sweden, Germany, France, Belgium, The United States of America and Canada], Tilburg, Katholieke Universiteit Brabant, 2000, 255 p.

executive and judicial powers in the state. The original Constitution from 1831, revised several times since, was replaced by a new version on 17 February 1994. The original Constitution contained primarily classic civil and political rights. In the 1993/1994 reform, a number of social, economic, and cultural rights have been inserted. In 2000, a clause on the rights of the child has been added. Since then, minor changes have taken place.[8]

Belgium started in the form of a unitary decentralized state with provinces and communes by the Constitution of 7 February 1831. The 1993 revision redefined Belgium as a federal state (Article 1). The resulting institutional structure is highly complicated, with a federal level (House of Representatives, Senate, King), the community level (Flemish, French, and German Community Council, Joint Commission), the state-region level (Flemish and Walloon Region, Brussels-Capital), and finally the language-region level (Dutch-, French-, German-speaking, and Bilingual Region). Communities and regions have their own legislative and executive bodies. There is no hierarchy between national statutes, and the statutes enacted by the communities and regions are of equal authority. The so-called Court of Arbitration [*Arbitragehof/Cour d'Arbitrage*], founded by the 1980 revision and inaugurated on 1 October 1984, was established to resolve conflicts between legislators. We will see that this court will develop into a Constitutional Court.

The guarantees of the civil liberties are ensured by the control of on the one hand the Constitutional Court and on the other hand the judicial and administrative courts. The Supreme Court [*Hof van Cassatie/Cour de Cassation*] is the highest civil and criminal court and is composed of three chambers, one for civil and commercial matters, one for criminal and police matters, and one for labor matters. In general, the Supreme Court does not reconsider the facts of a case, but only reviews the issues of law raised in a decision of a lower court. If it upholds an appeal, this renders the original decision null and void and the case is referred back to an appropriate court for retrial. Five judges normally render Supreme Court decisions. There is an Attorney-General in the Supreme Court who acts as a Public Prosecutor. In principle, case-law precedents have no legally binding force. In practice, decisions of the highest courts have strong persuasive authority, especially when confirmed repeatedly.

According to the official doctrine, primary legislation is still immune from judicial control, although in 1971, the Supreme Court introduced the monistic theory, stating that international provisions with direct effect can be invoked by all citizens before a Belgian court and is superior to Belgian law.[9]

The Constitution delineates the power of the legislator and of the regulatory power in the definition of the exercise of the public liberties. The Belgian Constitution is less precise regarding the criteria for restricting fundamental rights when compared to the text of the ECHR. The Constitution was a reaction to the (Dutch) King William I's government. This explains why most of the attention goes to restricting executive authorities powers and the many references to the necessity for the legislator who needs to define by law the rights and liberties in the Constitution.[10]

The Belgian Constitution is monist and integrates international norms directly into the legal system, as long as the international convention is provided with provisions with a direct effect.[11]

---

[8] All changes are incorporated in the official version of the Belgian Constitution at the website of the Senate: www.senate.be/doc/const_nl.html (Dutch) or www.senate.be/doc/const_fr.html (French) (last visited 10 October 2006). There are not many English written sources available regarding Belgian Law. See Ch. Malliet, *Research Guide to Belgian Law*, available at http://www.llrx.com/features/belgian.htm (published December 1, 2000) and at http://www.nyulawglobal.org/globalex/Belgium.htm (published August 2005).

[9] Cass. [*Hof van Cassatie/Cour de Cassation*], 27 May 1971, *Journal des Tribunaux*, 1971, 460. In this case, with the parties Belgium v. S.A. Fromagerie Franco-Suisse Le Ski, the Supreme Court held that a self-executing treaty (here the EC Treaty) prevails over acts adopted before and after the ratification of the treaty and hence, that the courts should give effect to the treaty. See J. Wouters & D. Van Eeckhoutte, 'The Enforcement of Customary International Law Through EC Law', in: J.M. Prinssen & A. Schrauwen (eds.), *Direct Effect. Rethinking a Classic of EC Legal Doctrine*, Groningen, Europa Law Publishing, 2002, (181), 215-223.

[10] A. Alen & J. Clement, 'Fundamental Rights and Liberties', in A. Alen (ed.), *Treatise on Belgian Constitutional Law*, Deventer, Kluwer Law and Taxation Publishers, 1992, (181-209), at 186.

[11] J. Vande Lanotte & Y. Haeck, 'Implementing human rights in Belgium: Sources, Monism – Dualism, Hierarchy, Direct effect, Third-party applicability and implementation mechanisms', in J. Vande Lanotte, J. Sarkin & Y. Haeck (eds.), *Resolving the tension between crime and human rights. An evaluation of European and South-African issues*, Antwerp-Apeldoorn, Maklu Uitgevers, 2001, 1-66.

Hence, and this contrary to most other states (such as the United States and the United Kingdom), Belgium recognizes the primacy of international law over all domestic legislation, including the Constitution, which explains the overall focus of Belgian lawyers on European human rights, rather than Belgian human rights embedded in the Constitution. Due to the open nature of the European human-rights system and its ability to adapt to new developments and new threats created by technology through its case law, debates about adapting the Belgian Constitution are almost never fueled by human-rights problems. Article 32 of the Constitution was amended in 1993 to include a right of access to government documents, a right absent in the human-rights system of the Council of Europe. Article 22 relating to privacy was also added to the Belgian Constitution in 1993 (1994), but this occurred without proper debate and with the general comment that its content had to be defined according to the case law of the European Court. Prior to the constitutional amendment, the Supreme Court had ruled that Article 8 of the European Convention applied directly to the law and prohibited government violation of the private life of individuals.[12]

Finally, the Constitution does not contain any clause relating to the horizontal effect of fundamental rights. This matter has not been discussed either during the 1993 reform. Direct application of fundamental rights in horizontal relations has received some sympathy in legal doctrine, but not in case law. In practice, under Article 1382 of the Civil Code, any individual may claim compensatory damages when one of his constitutional rights has been violated by another individual, on the condition that the general principles of civil liability are fulfilled, i.e., fault, damage, and a relationship between fault and damage.[13] Usually, courts only consider reference to these specific principles and omit a discussion of constitutional rights. Hence the direct horizontal effect remains subject to the intervention of the legislators. For some matters, the legislation indeed converts the interests protected by fundamental rights into specific legal norms, which apply also to relations between private persons.

2.2.2. Since 2000

Since World War II, Christian Democrats had continually been in power. On 6 March 1992, Jean-Luc Dehaene became the last Christian Democrat Prime Minister. In 1999, a new 'rainbow' coalition was sworn in, comprising parties across the political spectrum (the Flemish Liberals, Socialists and Greens and their French-speaking counterparts) without Democrats. One of the priorities of the new Prime Minister, Guy Verhofstad, a Flemish Liberal, was to deal with the impact of the dioxin contamination of food (a scandal which helped bringing down the previous Christian Democratic Socialist coalition), and to lay out the foundations for a new efficient state, doing away with traditional bureaucracy, introducing governance, and opening up for the benefits of the Information Society. After the May 2003 elections, the Socialists and Liberals agreed to renew their coalition. Again, the focus is on governance, simplification of administration, and actions to protect consumers on the Internet.[14]

Since 2000, Belgian federalism has reached a higher level of maturity. This is illustrated by the fact that governments in the communities and the regions are composed of other parties than the federal government. The Flemish government, for instance, is headed by Christian Democrat Yves Leterme, a situation that is fuelling a spirit of competition between the respective governments. Good government and governance seem to be a shared starting point. Not less then two federal 'secretaries of state' are put on the job from 2003 ontwards: Peter Vanvelthoven is responsible for the informatisation of the state, and Vincent Van Quickenborne is responsible for the simplification of the administration. In the Walloon Region, the Agency responsible for simplification is the E-Administration and Simplification Unit (EASI-WAL). On the Flemish side, there is the Legislative Moderation Unit.

[12] Cass. [*Hof van Cassatie/Cour de Cassation*], 26 September 1978, *Arr.Cass*., 1978-79, 116.
[13] A. Alen & J. Clement, *loc. cit.* n. 10, at 187.
[14] The governmental agreement of July 2003 can be found at http://premier.fgov.be/nl/politics/20030710-accord_gov.pdf. See especially p. 31 (consumer protection regarding the Internet) and 75 (simplification of administration).

New federal instruments for a better informed government and legislator (governance)

The Belgian Data Protection Authority (hereinafter: 'Privacy Commission') was moved from the executive to the legislative branch in 2003.[15] The Commission from now on answers directly to the Belgian Parliament, its members being appointed by this institution. Clearly this 'move' from the executive to the legislative branch seeks to enhance the autonomy and independence of the said institution.

By the same reform, sectoral committees were created within the Privacy Commission in charge of specific data-protection issues. Before 2003, a special committee existed for the social sector and its database [*Banque-Carrefour/ Kruispuntbank*].

In 2001, the Minister of Economic Affairs established the Internet Rights Observatory,[16] with a duty to advise the Minister on the effect of new technologies, to organize consultations amongst the involved economic parties, and to provide information to the public.[17] The Observatory has released reports on the protection of minors on the Internet,[18] e-commerce,[19] e-government,[20] and Voice over IP.[21] A discussion in English of these opinions can be found on the website of the Observatory.

New regional instruments for a better informed government and legislator (governance)

The Flemish Parliamentary Technology Assessment Institute (*Vlaams Instituut voor Wetenschappelijk en Technologisch Aspectenonderzoek,* hereinafter: viWTA), is an independent and autonomous institute created for the purpose of Technology Assessment (TA). viWTA was founded by decree on July 17, 2000 as an autonomous institution within the Flemish Parliament. The role of viWTA is to clarify arguments and positions in the public debate, to interpret subjects in their context, to elucidate the debate, and to see to it that in addition to experts the general public can be heard as well.

The viWTA has staged a conference entitled 'The next technology wave: can policy keep pace with progress? The case of converging technologies', which focused on the benefits and risks of 'Converging Technologies' (CTs), such as biomedical technology and nanotechnology.[22] A 54-page summary report was discussed in the Flemish Parliament.[23]

---

[15] Act of 26 February 2003 modifying the Data Protection Act of 8 December 1992, *B.S.* 26 June 2003. See K.R., 'Institutional changes at the Belgian Privacy Commission, *Stibbe ICT Law Newsletter,* 2003, No. 11, September, at 5. All Belgian acts and degrees can be found at http://www.staatsblad.be.

[16] Royal Decree of 26 November 2001 establishing the Internet Rights Observatory *[Koninklijk Besluit van 26 November 2001 houdende de oprichting van het Internet Observatorium]*, *B.S.* 15 December 2001, 43296. See EPIC and Privacy International, *Privacy and Human Rights 2005. An international survey of privacy laws and developments*, Washington, EPIC, 2006, at 189-190.

[17] The Internet Rights Observatory provides information to the citizen on a website. See http://www.internet-observatory.be/ (last visited 10 October 2006).

[18] Observatoire des Droits de l'Internet, *The Protection of Minors on the Internet, Opinion No. 1*, February 2003, available at http://www.internet-observatory.be/internet_observatory/pdf/advices/advice_en_001.pdf.

[19] Observatoire des Droits de l'Internet, *Pistes pour renforcer la confiance dans le commerce électronique, Opinion No. 3*, submitted to the Federal Minister of Economy, June 1, 2004, available via http://www.droittechnologie.org/, http://www.internetobservatory.be/internet_observatory/pdf/advices/advice_en_003.pdf.

[20] Observatoire des Droits de l'Internet, *Facteurs de succès de l'e-gouvernement, Opinion No. 2*, December 2003, available via http://www.droit-technologie.org/, http://www.internet-observatory.be/internet_observatory/pdf/advices/advice_en_002.pdf.

[21] In its opinion, the Observatory examines the opportunities and challenges related to the development of VoIP services. It concludes that it is important right now to make clear choices about VoIP services and to determine the applicable legislation, while avoiding the creation of too many regulatory obstacles to their development, in order to protect consumers and provide legal certainty. Observatoire des Droits de l'Internet, *Opportunités et défis liés au développement des services Voice over IP*, *Opinion No. 4*, May 2005, available at http://www.internet-observatory.be/internet_observatory/pdf/advices/advice_fr_004.pdf.

[22] *Converging Technologies – Shaping the Future of European Societies, Report of the High Level Expert Group on Foresighting the New Technology Wave*, European Commission, EUR 21357, available at http://europa.eu.int/comm/research/conferences/2004/ntw/index_en.html

[23] viWTA, *Summary report of the Conference and Roundtable of EPTA on Converging Technologies. The next technology wave: can policy keep pace with progress? The case of converging technologies*, Flemish Parliament, Brussels, October 17-18, 2005, 54 p.

In 2005, the viWTA commissioned and published a report on cyber-bullying among youngsters in Flanders.[24] In 2005, viWTA organized a first conference and published a first (European) study regarding the ethical and social aspects of genetic testing services.[25]

As a Flemish parliamentary institution, viWTA is highly interested in a participative approach. Participatory citizen panels have been created by the viWTA for a broad range of issues, including genetically modified food. On January 23, 2006, the viWTA and the King Baudouin Foundation hosted a final panel discussion about the 'Meeting of Minds' program. The discussion marked the last stage of this citizens' assessment of developments in neuroscience. Subsequently, a European report was delivered to the European Parliament.[26] One important recommendation regards brain-imaging techniques used by the government. These could lead to the invasion of privacy, including medical records, potential predispositions for disorders, and perhaps even privacy of thought. The legal right to remain silent, for example, could be made irrelevant by advances in brain science. Hence, it is suggested to prohibit these techniques for law-enforcement use or for public-security reasons.

Governance and E-government

Overseeing recent initiatives, the reader is struck by the fact that the federal government's choice for reducing bureaucracy, introducing governance, and opening up for the benefits of the Information Society (see above) is seldom framed in terms of rights. One senses a straightforward social-liberal rights agenda (more responsible freedom with measures for the social 'underclass'), but this political goal is seldom stressed, and the language is replaced by the language of either money or governance. E-government starting points are the need of citizens for one global solution; their wish to see the government as a whole; their expectation that data that are already known to the government are not asked for again; and their desire to reduce administrative formalities. Privacy is not a starting point but a 'building block' for e-government.[27] Social inclusion is not (even) a building block, but is mentioned as an important factor requiring awareness, support, and a model of e-government that is seen as complementary to physical government.[28]

A good illustration of the money approach is the proposal to distribute freely e-mail addresses and identity-card reading machines (see *below*). A second illustration regards *in vitro* fertilization. From 1 July 2003, based on a Royal Decree,[29] *in vitro* fertilization is only compensated by the social-security system on the condition that the woman is not older than 36 and that only one embryo is implanted (*single embryo transfer*), and not two or three like in the past. On the one hand, the measure has drastically lowered the number of twins, from 25 to 11 percent, while on the other hand, the financial compensation has led to an increase in persons seeking *in vitro* fertilization.[30]

The governance idea behind Belgian e-government is partly the result of a development towards reforming the federal administration that has been underway since the 1980s.[31] This development, modest at first, was fuelled in the late 1990s. In 1998, the outgoing government adopted a law to promote entrepreneurship and competitiveness. This law provided for a number

---

[24] viWTA, *Cyberbullying among youngsters in Flanders, executive overview*, 2005, 13 p., available via http://www.viwta.be/content/nl/doc_Rapporten.cfm.

[25] viWTA, *Ethical and social aspects of genetic testing services: issues and possible actions*, 2005, 71 p. The research was carried out by Danielle Bütschi Häberlin, see http://www.viwta.be/files/FinaleVolledigeDefinitieveEindrapportEurogentest.pdf.

[26] Having started in 2004, to provoke a measured and informed debate before technology truly takes off, the 'Meeting of Minds – A European Citizens' Dialogue on Brain Science' gathered 126 laypeople from nine European countries to formulate continent-level recommendations for policymakers and researchers. See http://www.meetingmindseurope.org. See also Michael Rodgers, 'Meeting of the Minds. 37 recommendations Europeans came up with when they gathered to talk about brain science', *The Scientist* 2006, Vol. 20, No. 10, at 28.

[27] Available via http://www.belgium.be/. See also *Beleidsnota van de Staatssecretaris voor Informatisering van de Staat Peter Vanvelthoven*, November 2003, 22 p., available at http://mineco.fgov.be/information_society/administrations/e-government_BE/note_strateg_inform_Etat_nl.pdf.

[28] *Id.*

[29] Royal Decree of 4 June 2003 modifying the Royal Decree of 25 April 2002 relating to the fixation and the liquidation of the budget of financial means of the hospitals, *B.S.* 16 June 2003.

[30] H. Cammu, 'Topembryo voor proefbuisbaby gezocht', *Eos magazine*, 2006, No. 3, 38-43.

[31] Van Hoorne, 'Better regulation in Belgium (federal level): focus on administrative simplification', 6 p., available at http://www.mcmp.gov.mt/pdfs/VanHoorne.pdf.

of incentives in different areas in order to stimulate business and job creation. Importantly, this law of 1998 created the Administrative Simplification Agency (ASA), a new federal institution under the prime minister, to drastically reduce red tape. The new government that came to power in June 2003 refocused the administrative simplification policy, changing from quantitative targets to a qualitative approach.

In the 2005 *Kafka Report*, the various administrative reforms already completed in favor of citizens, businesses, and other target groups are presented: over 170 laws and regulations have been abolished or simplified.[32] One reform regards the reduction of the amount of paper needed for a marriage certificate or a civil-partnership contract by better using information already known to the authorities. Couples are no longer required to collect the certificates and copies themselves; this is taken care by the government.

Illustrative of the broad scope of the concept of simplification is the bill of 13 February 2005 regarding the simplification of the administration,[33] which abolishes penal laws seldom used (e.g., insulting foreign heads of states), and the proposal in the 2005 *Kafka Report* to abandon – against all police intuitions – the obligation to produce guest registration cards in hotels and to pass these to the police. Again the language is not 'freedom', 'privacy' or 'liberalism', but 'convenience'.[34]

2.3. Changes in the constitutional system

No new fundamental rights have been proposed in connection with ICT or biotechnology. In 2000, a new article 22bis was introduced in the Constitution: 'Every child has the right to respect of his or her moral, physical, mental, and sexual integrity' (see *below,* section 4.3). Presently, discussions are taking place to include a general clause in the Constitution that would allow exceptions to fundamental rights in case of war or other nation-threatening situations. Such a clause would contain the criteria on the basis of which exceptions to most of the fundamental rights could be made.[35] Some experts deem that such a clause would improve legal certainty, as for some fundamental rights, it is not clear under what conditions fundamental rights may be restricted.

The Constitutional Court owes its existence to the development of the Belgian unitary state into a federal state.[36] The official name, Court of Arbitration [*Arbitragehof*], reflects its original mission, which is to supervise the observance of the constitutional division of powers between the federal state, the communities, and the regions.

In the constitutional amendment of 15 July 1988, the competence of the Court was extended to include the supervision of Articles 10, 11, and 24 of the Constitution guaranteeing the principles of equality, non-discrimination, and the rights and liberties in respect of education. By the same constitutional amendment, the power was granted to the special legislator to grant the Court of Arbitration the competence to review compliance with other articles of the Constitution. This facility was used in the special Act of 9 March 2003. The entire Section II, Articles 8 to 32, as well as Articles 170, 172, and 191 of the Constitution, now constitute the frame of reference for constitutional review of statutes by the Court.

A case can be brought before the Court by any authority designated by statute, any person who has a justifiable interest, or, in a preliminary issue, any tribunal. As a general rule, an action must be brought within six months of the publication of the challenged regulation in the Belgian Official Gazette. Alternatively, preliminary issues can be brought before the court. If a question comes up in a particular tribunal about the correspondence of laws, decrees, and ordinances with the rules laying down the division of powers between the State, the communities, and the regions

[32] 'Simplifying government procedures', *Kafka Report II*, 2005, at 17. Available at http://www.kafka.be/doc/1133283810-9191.pdf. See also http://www.staatssecretarisq.be/.
[33] Act of 13 February 2005 regarding the simplification of the administration, *B.S.* 23 February 2005, entry into force 5 March 2005.
[34] 'Simplifying government procedures', *Kafka Report II*, 2005, *loc. cit.* n. 32, at 16.
[35] See, e.g., *Parliamentary Documents*, Chamber [Parl.St., Kamer], 2005-06, 2304/001.
[36] See for a short presentation and for the basic legal texts: http://www.arbitrage.be/.

or with Articles 8 to 32, 170, 172, or 191 of the Constitution, that tribunal must address a preliminary question to the Constitutional Court, as the Court has the exclusive competence of interpreting the Constitution and the competence-dividing rules. When the Court finds a breach of these articles, its decision only has effect between the parties of the specific case.

As observed above, the competence of the Court was extended to the principles of equality, non-discrimination, and the rights and liberties in respect of education in 1988, and to most individual rights in the Constitution in 2003. The constitutional legislator in 1988 clearly did not foresee that through the equality and non-discrimination clause, the Court had in fact become a real constitutional court. It began to review laws in the light of fundamental rights and even unwritten principles, related to equality and the non-discrimination clause. For example, in a judgement of 21 March 2000, the Court found that the presumption of guilt regarding persons that own cars filmed by a traffic camera and who subsequently were held responsible for a traffic crime without having been identified in person unless they prove the contrary, is *not* in violation of article 6 ECHR (the right to be presumed innocent), based on a test of reasonableness.[37] In 2003, the legislator confirmed this evolution by extending the Court's competence to all fundamental rights in the Belgian Constitution.[38] The 2003 reform is therefore less drastic than it seems, but nevertheless fundamental. We will see later on in judgements relating to, for example, the publication of the names of sportsmen on a public website and special investigative powers, that the Constitutional Court applies without hesitation existing rights to new 'digital' issues and that it exercises a strict proportionality test in these cases. Also, when confronted with rights absent from the constitutional order, the Court does not hesitate to borrow from the supranational order.[39] Hence, the Belgian constitutional order is transformed into one very similar of the European human-rights order, but without the necessity for the Constitutional Court to respect a margin of appreciation whenever there is diversity within the member states.

We have already observed that there was support for the idea of a horizontal effect of constitutional rights in legal doctrine, but that this had not been officially recognized in case law. In practice, other legal instruments were available, such as Article 1382 of the Civil Code (civil liability for fault, see above) and the central notion of 'unfair practices' in the Act of 14 July 1991 on Commercial Practices and Consumer Information and Protection, which applies to 'on-line' as much as to 'off-line' unfair trade practices.[40]

A first recognition by the Supreme Court of horizontal effect occurred in a decision of 27 January 2001.[41] The case concerned evidence obtained by cameras which had not been installed in conformity with privacy laws. The Court nevertheless admitted the evidence in a criminal procedure, considering that proving a crime took precedence over the right to privacy of an employee. From a legal point of view, this judgement is crucial, because for the first time, it was accepted in Belgium that Article 8 ECHR also applies to conflicts between private parties.[42] Although precedents exist in case law of the lower courts,[43] this judgement, rendered at the highest level, adds an important new element to the discussion about the possible horizontal effect of the European Convention. Seemingly, the Supreme Court does not only accept the horizontal effect of the first paragraph of Article 8 ECHR ('Everyone has the right to respect for his

[37] Constitutional Court [*Arbitragehof*] No. 27/2000, 21 March 2000, available via http://www.arbitrage.be.
[38] A. Alen & J. Clement, *loc. cit.* n. 10, at 187; P. Popelier, 'The Role of the Belgian Constitutional Court in the Legislative Process', *Statute Law Rev.*, 2005, Vol. 26, 22-40.
[39] In the *traffic camera* case (above), the Court refers to Article 6 para. 2 ECHR (presumption of innocence), a right that is not included in the Belgian Constitution.
[40] Act of 14 July 1991 relating to trade practices and information of the consumer, *B.S.* 29 August 1991. See in detail: E. Terryn, 'Cyber Consumer Protection And Fair Trading – National Report Belgium', in: E. Dirix & Y-H. Leleu (eds.), *The Belgian reports at the congress of Utrecht of the international academy of comparative law*, Brussels, Bruylant, 2006, 421-458.
[41] Cass., 25 January 2001, *Computerrecht* 2002, at 202, with note by J. Dumortier.
[42] For later decisions that also explicitly refer to article 22 of the Constitution and article 8 ECHR in private relations, see Cass., 27 Februari, 2001, *Computerrecht* 2001, p. 199ff, with note by J. Dumortier, at 203; Cass., 2 March 2005, *Computerrecht* 2005, p. 258ff with note by P. Van Eecke & B. Ooms, at 261; Antwerp, 6 January 2003, *Computerrecht* 2003, p. 249ff, with note by E. Kindt.
[43] See also P. De Hert, *Artikel 8 EVRM en het Belgisch recht. De bescherming van privacy, gezin, woonst en communicatie*, [Article 8 ECHR and the Law in Belgium. Protection of Privacy, House, Family, and Correspondence], Ghent, Mys en Breesch Uitgeverij, 1998, at 54.

private and family life, his home and his correspondence'), but also of the second paragraph. This contains the criteria (legality, proportionality, and legitimacy) under which limitations of privacy are deemed possible. The terms of the judgement clearly refer to this paragraph, although the reference is unsatisfactory because it is incomplete. The requirement of legality or transparency (the employer needs a legal basis) is simply not checked, which is a serious flaw in the reasoning of the Court.[44]

As stated in the Koekkoek report of 2000, the development towards a federalist regime has created obstacles for an integrated digital-rights approach. The report identified the case law of the Constitutional Court as accepting that not only the federal state but also regions and communities can make laws in the meaning of the Constitution that impose restrictions in the fields of their competence. We will discuss an example of this case law (see below, section 4.1). Some problems created by overlapping competences remain, however. The report gave the example of telecommunications (a federal competence) and broadcasting institutes or companies (a community competence), rightly noting that with converging technologies, this will create conflicts. Partly, the many legislators try to avoid these conflicts if possible by confining the scope of their projects. A federal 2003 Bill on legal protection of services based on or consisting of conditional access relating to information-society services.[45] Due to the Belgian system, in which legislative powers are divided between different federal entities, the scope of the Bill is mainly limited to information-society services, whereas the directive that the Bill implements also targets television and radio-broadcasting services.[46]

The Flemish governmental agreement laying the foundations for the 2004-2009 period contains a section on information and communication.[47] Engagements to enhance digitization of communication and broadband and to bridge the digital divide are included. Clearly, one feels a certain tension when it is stated that the Flemish government, which has to be competent for the whole framework of media and telecom, will guarantee an open market for these media.
With regard to e-government, the federal government concluded cooperation agreements with the governments of the regions and communities in March 2001, with the explicit desire to involve equally provinces and local governments.[48] All authorities will cooperate within their competences with each other to offer the citizen an integrated service, without having to buy more than one infrastructure or having to use more than one electronic key or signature. Also, interoperability, cooperation, and transparency are key words in the agreements.

[44] P. De Hert & M. Loncke, 'Camera Surveillance and Workplace Privacy in Belgium', in: Sjaak Nouwt, Berend R. de Vries, et al. (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, 2005, 167-209.
[45] Act of 12 May 2003, *B.S.* 26 May 2003, implementing Directive 98/84/EC of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access.
[46] K.R., 'Draft Bill on legal protection of services based on or consisting of conditional access relating to information society services', *Stibbe ICT Law Newsletter*, 2003, April 2003, No. 9, at 4-5.
[47] Vlaamse Regering, *Vertrouwen geven, verantwoordelijkheid nemen. De ontplooiing van Vlamingen en Vlaanderen duurzaam bevorderen. Een zorgzame, lerende samenleving. Goed en doelmatig bestuur 2004 – 2009. Regeerakkoord,* 2004, 85 p., available at http://www3.vlaanderen.be/vlaanderen-in-actie/documenten/vlaamsregeerakkoord2004.pdf.
[48] See, e.g., *Samenwerkingsakkoord van 28 september 2006 tussen de Federale Staat, de Vlaamse, de Franse en de Duitstalige Gemeenschap, het Vlaamse Gewest, het Waalse Gewest, het Brussels Hoofdstedelijk Gewest, de Franse Gemeensmchapscommissie en de Gemeenschappelijke Gemeenschapscommissie betreffende de principes voor een geïntigreerd e-governement en de bouw, het gebruik en beheer van ontwikkelingen en diensten van een geïntegreerd e-government* [Cooperation agreement of 28 September 2006 between the Federal Government, the Flemish, the French and the German-speaking Community, the Flemish Region, the Walloon Region, the Brussels Capital region, the French Community Commission and the common Community Commission regarding the principles for integrated e-government and the construction, the use, and the administration of developments and services of integrated e-government], B.S. (2nd ed.) 19.10.2006, 55747. For the text of the Agreement of March 2001 and a discussion thereof, see 'Samenwerking tussen alle overheden', available via http://www.belgium.be/.

2.4. Privacy-related rights

2.4.1. Privacy and data protection

The Constitution

The right to respect for private life is laid down in Article 22 of the Constitution. The text of Article 22 reads as follows:

> Everyone is entitled to respect of his private life and his family life, except in the cases and under the conditions determined by law.
>
> The law, the decree, or the ruling stipulated in Article 134 guarantee the protection of that right.[49]

The article was inserted in the Constitution in 1994. During the parliamentary discussions, it was stated that the article aims at providing protection to the person, recognizing his identity and the importance of his development and of his family, and that such protection is needed against '*intrusion, including as a result of the continuous development of information technologies,* when measures of search, investigation and control by the government and by private institutions are taken when exercising their functions or activities' [emphasis added].[50] Therefore, one could say that although it does not include any (explicit) reference to privacy protection against the use of new technologies, it has been the intention from the constitutional legislator that Article 22 in its broad formulation shall be apt to cope with intrusions by new technological means. Case law confirms that Article 22 is in general able to deal with risks by the new information technologies, such as the Internet, without Article 22 explicitly mentioning these technologies.

During the discussions in parliament, it was also pointed out that Article 22 shall have the same content and interpretation as Article 8 ECHR, this in order to avoid discussions on the content of both articles.[51] Over the years, case law and legal authors have given a broad application to Article 22 of the Constitution and Article 8 ECHR.[52] The right to respect for private life does not only protect against secret surveillance and monitoring, but also provides protection in case of infringements of the so-called 'personality rights', i.e., the right to physical, psychological and moral integrity of the body (see *infra*, section 4.3), and could also be invoked, for example, in case of breach of reputation and honor, or in case of certain forms of environmental nuisance.[53] For that reason, one could say that the interpretation of the right to respect for private life in Article 22 is to an important degree based on the interpretation of similar rights in international conventions (in particular Article 8 ECHR). However, differences remain between Article 8 and Article 22 of the Constitution, in particular with regard to the criteria for imposing restrictions on the rights and liberties.[54] Compared with other similar provisions in international conventions, Article 22 of the Constitution contains less detailed criteria as to the conditions under which the fundamental right to respect for private life can be restricted.

Constitutional case law

Article 22 states that restrictions can be imposed on the right to respect of private life in the cases and under the conditions stipulated by law. In general, it was accepted that only the federal

---

[49] 'Ieder heeft recht op eerbiediging van zijn privé-leven en zijn gezinsleven, behoudens in de gevallen en onder de voorwaarden door de wet bepaald. De wet, het decreet of de in artikel 134 bedoelde regel waarborgen de bescherming van dat recht.'

[50] *Parliamentary Documents*, Senate [*Parl. St.,* Senaat], 1991-92, 100-4/5, 3.

[51] *Parliamentary Documents*, Chamber [*Parl. St.,* Kamer], 1993- 94, 997/5, 2.

[52] See also A. Alen & K. Muylle, *Compendium van het Belgisch Staatsrecht* [Compendium of Belgian State Law], Mechelen, Kluwer, 2004, No. 777; P. de Hert, op. cit. n. 43.

[53] Constitutional Court [*Arbitragehof*] No. 50/2003, 30 April 2003, *B.S.* 23 May 2003 (2nd ed.); Constitutional Court [*Arbitragehof*] No. 51/2003, 30 April 2003, *B.S.* 12 June 2003: Noise nuisance of airplanes may constitute a breach of the rights of Article 22 of persons who live in the neighbourhood of an airport.

[54] Article 8 para. 2 ECHR reads as follows: '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*' [emphasis added].

legislator was empowered to impose restrictions to fundamental rights by law, and that 'law' was to be understood in the formal sense, i.e., a legislative measure of the federal legislator. Since 2000, there are some cases from the Constitutional Court that give more insight in the debate about the competence of the federal and local legislators for imposing restrictions to the right to privacy. The Constitutional Court stated that the Communities and the Regions are also competent to regulate and restrict the right to respect for privacy if such restrictions fall in the field of their competence.[55]

Since 2000, the Constitutional Court has also reviewed the use of new technologies, such as publication on the Internet, under Article 22. One case involved a new legal requirement by the Flemish legislator to publish the identity and disciplinary sanctions of sportsmen on a public website in the combat against drugs.[56] The Constitutional Court reviewed this requirement of publication under Article 22. The Court found that a limited electronic publication accessible by sport officials and representatives of sport clubs could be deemed necessary for the enforcement of sanctions imposed on sportsmen, and therefore legitimate. In fact, however, the names and sports disciplines would also be accessible by the public. The Constitutional Court stated that since publication on the Internet was not required for the purposes envisaged and since the information could also be abused by others, the consequences of such publication were disproportionate with respect to the purpose of the enforcement of disciplinary sanctions. The Court concluded that for these reasons, publication on the public website was contrary to the right to respect of private life of Article 22 of the Constitution.[57] The Court hereby repeated that the Regions were competent to impose restrictions in their field of competence, but reminded that the federal legislator is competent to determine in which cases and under which conditions this constitutional right of Article 22 can be restricted. In the case at hand, there was no legal basis to restrict the right to privacy of the athletes by publishing their names on a public website. The Flemish legislator had to respect the provisions of the (federal) data-protection legislation in restricting the right to privacy, which he had failed to do. For that reason, the requirement to publish the names was annulled.

Privacy versus security

In the last five years, the debate about privacy and security has intensified. One of the means often suggested to increase security is the use of surveillance cameras in public places. The use of cameras, however, often conflicts with privacy rights. Although it is generally accepted that the general data-protection legislation applies to the use of cameras, the criteria for using these cameras were unclear, partly because of conflicting case law. For these reasons, several bills were introduced in parliament for a specific law on the use of cameras.[58] Further to the proposals, the use of cameras in public places (e.g., streets) or places accessible for the public (e.g., shops) would be subject to a specific authorisation. In December 2006, the Senate adopted Bill 3-1734 on the use of cameras[59] and sent it to the House of Representatives. This proposal applies the principles of the Data Protection Act of 8 December 1992 to protect privacy in relation with the processing of personal data (see below) to the practice of camera surveillance, unless expressly stated otherwise in the proposal. The proposal also adds some specific requirements. It states that the decision to install camera surveillance in places accessible to the public is taken by the

---

[55] See, for example, Constitutional Court [*Arbitragehof*] No. 50/2003, 30 April 2003, *B.S.* 23 May 2003 (2nd ed), considerans B.8.10: 'Deciding otherwise would mean that the competences of the Communities and the Regions would become without subject. The fact that an intrusion in the private life and the family life is the result of a regulation of specific matter which belongs to competence of the regional legislator, does not result in a breach of his competence'; Constitutional Court [*Arbitragehof*] No. 51/2003, 30 April 2003, *B.S.* 12 June 2003.

[56] Article 40 para. 6 al. 2 of the Flemish decree of 27 March 1991 relating to medically accepted sport exercise, inserted by Decree of 19 March 2004.

[57] The nullity of the requirement was decided in Constitutional Court [*Arbitragehof*], No. 16/2005, 19 January 2005, *B.S.* 31 January 2005, 2758.

[58] See, e.g., *Parliamentary Documents*, Chamber [*Parl.St.,* Kamer], 2005-06, 2038/1, *Parliamentary Documents*, Chamber [*Parl.St.,* Kamer], 2005-06, 2187/1, *Parliamentary Documents*, Senate [*Parl.St.*, Senaat], 2005-06, 3-1522/1, *Parliamentary Documents*, Senate [*Parl.St.*, Senaat], 2005-06, 3-1734/1. For the last-mentioned bill, the Privacy Commission has rendered a rather negative opinion (*Parliamentary Documents*, Senate [*Parl.St.,* Senaat], 2005-06, 3-1734/3).

[59] Bill No. 3-1734, available at www.senaat.be. See for a discussion of earlier proposals: 'Bill on regulating the use of surveillance cameras', *Stibbe ICT Law Newsletter*, 2006, No. 23, pp. 5 -7.

controller, but this only after having obtained two positive opinions, one by the local community council and a second one by the local police officer. The second opinion shall indicate that a security and efficiency assessment has been made and that the principles contained in the Data Protection Act of 8 December 1992 are correctly applied (Article 5 of the proposal). The proposal states that camera images shall only be used in real time by the competent authority for allowing the police to intervene immediately in case of crimes and disturbances. The recording of the images is allowed but limited to purposes of evidence-gathering in cases of crime or damages and for identifying the persons concerned. Most provisions contained in the proposed bill are enforceable through criminal-law mechanisms. For that purpose, specific crimes are listed in Article 13 of the proposal.

The use of cameras on the workplace has been subject to a regulatory attempt by the so-called collective labour agreement No. 68.[60] There is presently a legal debate, however, about the status of this regulation, after a decision by the Supreme Court of 2 March 2005 in a criminal case,[61] which stated that video images could be used even though they were obtained by the employer without applying the rules of the collective labour agreement No. 68. The case law of the Supreme Court, however, seems not to be followed by lower courts in employment and dismissal cases.[62]

The debate about the right balance between security measures and the protection of civil liberties and fundamental rights is also going on in the recent case of the Society for Worldwide Interbank Financial Telecommunications (SWIFT). SWIFT gave access to US authorities to its stored financial data in the context of the fight against terrorism.[63] The Belgian Privacy Commission was asked to review the legality of these transfers to US authorities. In its opinion of 27 September 2006, the Privacy Commission explored the conditions for applying the exceptions to the right to privacy as set out in Article 8 paragraph 2 ECHR, besides the compliance of the data transfers with the data-protection legislation.[64] The Privacy Commission stated, inter alia, that exceptional measures imposed by US law provide no legal basis for a hidden, systematic, and massive breach of long duration of European fundamental principles in data protection, but that one should rely on the criteria set forth in Article 8 paragraph 2 ECHR. In case of secret activities, these criteria include transparency, foreseeability of the norm, and sufficient and efficient control. In the opinion, the Commission acknowledged also that there exists a conflict between American and European law in this matter, and that SWIFT made several mistakes in evaluating its (legal) situation.[65] The case illustrates that privacy and data protection (see *below*) are often questioned in the security debate. While the current framework does provide protection, it may, however, not be entirely able to cope with security issues in global systems of international data exchange.

Data-protection legislation

The protection of privacy with regard to the processing of personal data is not explicitly mentioned in the Constitution. The right to respect of private life when personal data are collected, registered, used, and transfered is in general deemed to be included in Article 22 of the

---

[60] Collective Labour Agreement No. 68 of 16 June 1998 relating to the protection of the privacy of employees in relation with camera surveillance on the work floor, *B.S.* [*Belgian State Gazette*], 2 October 1998.

[61] See also *above,* n. 42.

[62] See X, 'Nieuwe rechtspraak over camerabewaking [New case law on camera surveillance]', *Newsflash,* Claeys & Engels (ed.), 12 July 2006, availabe at www.claeysengels.be (last visited 10 October 2006). Reference is made to two lower court decisions (Arbrb. Brussel, 29 March 2006 (not published) and Arbrb. Brussel, 16 March 2006) which rejected the use of video images obtained in contradiction to the collective labour agreement No. 68.

[63] See also European Parliament, *Resolution on the interception of bank transfer data from the SWIFT system by the US secret services*, available at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-539344 (last visited 7 December 2006). For more information about the SWIFT case, see www.privacyinternational.org (last visited 10 October 2006).

[64] *Opinion relating to the transmission of personal data by SWIFT pursuant subpoenas of the US Department of the Treasury (UST) (OFAC)*, Commissie voor de Bescherming van de Persoonlijke Levenssfeer [Privacy Commission], No. 37/2006, 27 September 2006, available at http://www.privacycommission.be/communiqu%E9s/AV37-2006.pdf (last visited 14 December 2006).

[65] See also Article 29 Data Protection Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (*WP 128), 22 November 2006, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf (last visited 7 December 2006).

Constitution and Article 8 ECHR. However, specific legislation does detail the rights of data subjects and the rights and obligations of data controllers when processing personal data. In order to be able to ratify the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Belgium has adopted general data-protection legislation with specific rights and obligations regarding the processing of personal data.[66] The Act is applicable to private and public entities that collect and use personal data and subjects the data processing to a detailed list of principles and obligations very similar to the provisions of Directive 95/46/EC. This general Act is completed with provisions in various other laws that provide for data protection in specific fields, such as consumer credit and the organization of the so-called Social Security Crossroad database [*Kruispuntbank van de Sociale Zekerheid]*. Since 2000, more legal provisions that provide for personal data protection were adopted, for example, relating to the establishment of a central database with information about loans granted to private users (e.g., a legal limitation of use of the data),[67] the rights of patients,[68] and electronic communications.[69] Such legislation is more and more invoked in debates and cases in which privacy rights are at stake, in combination with the processing of personal data.

2.4.2. Inviolability of the home

The Constitution

The right to inviolability of the home is laid down in Article 15 of the Constitution. The text of Article 15 reads as follows:

> The domicile is inviolable; no visit to the individual's residence can take place except in the cases provided for by law and in the form prescribed by law.[70]

The article was already part of the original Constitution. It is supported by criminal-law provisions punishing trespassing (article 439 Criminal Code). The provisions allow for searches within the home that respect formal and other requirements laid down in the law. Articles 87 and 88 of the Code of Criminal Procedure contain the general rule: searches in houses are possible when they are decided by an examining magistrate and this whenever he esteems that they might be useful for carrying out a criminal investigation. The term 'home' in the Constitution is understood in a broad sense; for instance, also a built-in garage and a shed in the garden can be a 'home'. In general, a search of a home is only allowed by order of an examining magistrate, except when the owner consents or when a crime is discovered *in fragrante delicto*.[71]

The constitutional provision has remained very much a 'sleeping' provision due to the tendency of the European Court of Human Rights with respect to Article 8 ECHR to consider most violations of the home under the broader scope of the protection afforded by the right to privacy. This approach was slightly altered in *Niemietz* v. *Germany* (16 December 1992),[72] and in

---

[66] Act of 8 December 1992 on the protection of the privacy in relation with the processing of personal data, as modified by the law of 11 December 1998, *B.S.* 18 March 1993 (hereinafter: Data Protection Act). See also the Royal Decree of 13 February 2001 for the execution of the Act of 8 December 1992 on the protection of the privacy in relation with the processing of personal data, *B.S.* 13 March 2001.

[67] Act of 10 August 2001 relating to the central database of loans to private users [Wet van 10 augustus 2001 betreffende de Centrale voor Kredieten aan Particulieren], *B.S.* 25 September 2001.

[68] Act of 22 August 2002 relating to the rights of patients, *B.S.* 26 September 2002 (see, e.g., in particular the articles 9 para. 2 and 10).

[69] See *below*, section 5.1.

[70] 'De woning is onschendbaar; geen huiszoeking kan plaatshebben dan in de gevallen die de wet bepaalt en in de vorm die zij voorschrijft.'

[71] A. Alen & J. Clement, *loc. cit.* n. 10, at 201.

[72] See http://hudoc.echr.coe.int for the judgement. Cf., 'The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life"'. However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude there from entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature (…)' (§29). 'More generally, to interpret the words "private life" and "home" as including certain professional or business activities or premises would be consonant with the essential object and purpose of Article 8, namely to protect the individual against arbitrary interference by the public authorities (…). Such an interpretation would not unduly hamper the Contracting States, for they would retain their entitlement to "interfere" to the extent permitted by paragraph 2 of Article 8; that entitlement might

Sté Colas Est and others v. *France* (16 April 2002),[73] where the Court 'found' a separate meaning for the right to protection of the house.

In Belgium, 'home' is not taken so broad as to defend against visual intrusion when the door is open and the officer just looks in.[74] Equally, the notion of 'home' does not protect firms.[75] However, one may expect this view to be changed due to the European judgements quoted above. Although neither the Constitution nor the ECHR imposes a duty to guarantee the intervention of an examining magistrate, the Constitutional Court has stressed that omission of this guarantee is only acceptable in exceptional cases and has to be motivated with reference to the nature of the crimes involved.[76]

Articles 87 and 88 of the Code of Criminal Procedure, which allow for searches ordered by the examining magistrate, are rather brief when compared to Article 90ter regarding telephone interception. They do not contain any detailed requirements regarding the form of the warrant. In V*an Rossem* v. *Belgium*, the European Court of Human Rights held unanimously that there had been a violation of Article 8 ECHR (right to respect of one's home),[77] because of the use of insufficiently detailed arrest warrants. In this case, the examining magistrate inquiring into the case had issued five warrants for searches to be carried out at Mr van Rossem's home, his wife's home, and at the offices of the three companies he ran. The court noted that the searches were ordered 'in order to investigate and seize any documents that might assist in the investigation'. No limitation of any sort was imposed, thus conferring wide powers on the investigators. As a consequence, Article 8 of the Convention was violated. The *Van Rossem* judgement has led to a modification of the case law of the Supreme Court, requiring more detailed search warrants from the examining magistrate.[78] This should enable the person objected to a search and enjoying the right in article 15 of the Constitution to control more effectively whether the actual search respects the mandate for the search given by the examining magistrate.

Legislation

We have already commented on proposals to introduce new camera legislation in Belgium. Partly, this regulation will enhance the protection of the people with respect to their homes. Article 5 of the proposed bill prohibits the use of cameras directed at places outside the authority of the controller. Article 8 prohibits all secret imaging of persons without their consent. However, a person entering a place that has a pictogram announcing the use of video cameras, is presumed to have given consent when entering.

In 2006, it became public that certain communities were using satellite pictures, taken by a private company, to identify potential building offences. On 12 July 2006, the Privacy Commission gave an opinion on the matter in response to a request by the Flemish Minister of Environmental and Country Planning.[79] Although the Commission considered the practice to be 'serious' in the light of the right to privacy and although the Commission saw some problems with the provisions regarding proactive investigation in the Code of Criminal Procedure, which only allow proactive investigation under strict conditions and in well-defined circumstances, it did not found any violation of the Data Protection Act. It considered, among other things, that the use of satellite

---

well be more far-reaching where professional or business activities or premises were involved than would otherwise be the case' (§31).

[73] See http://hudoc.echr.coe.int for the judgement. The judgement is available only in French. 'In extending the dynamic interpretation of the Convention, the Court is of the opinion that it is time to recognize, under certain circumstances, that the rights guaranteed under Article 8 of the Convention may be interpreted as including for a company the right to respect for its registered office, agency or business premises' (§41). 'Under these circumstances, to assume that the right of interference may be extended in the context of business premises of a legal person (...), the Court considers that, taking account of the conditions set out above, the operations at issue conducted in the field of competition cannot be considered strictly proportionate to the legitimate goals (...)' [our unofficial translation] (§49).

[74] Cass., 10 January 1995, *Arr. cass*., 1995, 31.

[75] Cass., 21 October 1992, *Arr. cass*., 1991-92, 1233.

[76] Constitutional Court [*Arbitragehof*] No. 140/98, 16 December 1998, available via http://www.arbitrage.be.

[77] *Van Rossem* v. *Belgium (application no. 41872/98)*, see http://hudoc.echr.coe.int for the judgement (available only in French).

[78] Cass., 11 January 2006, *Rechtskundig Weekblad*, 30 September 2006, 174-176, annotated by T. Decaigny ('De Belgische huiszoeking in de Europese pas' ['The Belgian search in conformity with European requirements']).

[79] L.C., 'Privacy Commission issues an opinion on the use of satellite pictures to detect and determine building offences', *Stibbe ICT Law Newsletter*, 2006 No. 25, September 7-8. The opinion can be found at http://www.privacy.fgov.be.

pictures to detect building offences served a legitimate purpose. The Commission did not, however, consider the right to inviolability of the home. Apparently, its position is very much influenced by the current state of technology. In the opinion, one can find the suggestion that the sheer access of all Internet users to sites such as Google Earth stands in the way of a principled prohibitive approach. It can also be assumed that the technical state of the art has played a role as well. Websites such as Google Earth do not produce very precise pictures of persons, and so, there is no question of detailed imaging of houses.

Proactive police methods were introduced in the Code of Criminal Procedure in 2003.[80] In a judgement of 21 December 2004, the Constitutional Court declared several provisions of the Act unconstitutional. The Court stressed the importance of the principle of proportionality in cases where privacy is at stake, which demands that police powers are only applied when there are indications of guilt and when the examining magistrate intervenes. It therefore declared void Article 28septies CCP allowing observation and 'quick looking operations' in houses with technical means without proper checking by a judge. The reasoning of the Court is particularly relevant for this report:[81]

- observation with technical means enabling to look inside houses, should from a privacy perspective be compared with telephone interception and regular searches in houses;
- within the framework of the 2003 Act, observation in houses is 'worse' because there is no possibility for the examining magistrate to take over the investigation from the prosecutor;
- because the measure is as serious as the searching of houses and telephone interception, the same requirements and checks should apply;
- since this is not the case (the examining magistrate cannot take over), the provision is unconstitutional.

Due to this judgement, the law was revised in 2005. The differences in regime between searches of houses and 'quick looking operations' in houses were abandoned.[82]

2.4.3. Inviolability of the body

The Constitution

For the right to inviolability of the body, Articles 22bis and 23 of the Constitution are relevant.

> **Article 22**
>
> Every child has the right to respect of his or her moral, physical, mental, and sexual integrity. (…)[83]
>
> **Article 23**
>
> 1. Everyone has the right to lead a life in conformity with human dignity.
>
> 2. To this end, the laws, decrees, and ruling alluded to in Article 134 guarantee, taking into account corresponding obligations, economic, social, and cultural rights, and determine the conditions for exercising them.
>
> 3. These rights include notably:
>
> 1) the right to employment and to the free choice of a professional activity in the framework of a general employment policy, aimed among others at ensuring a level of employment that is as stable and high as possible, the right to fair terms of employment and to fair remuneration, as well as the right to information, consultation and collective negotiation;
> 2) the right to social security, to health care and to social, medical, and legal aid;
> 3) the right to have decent accommodation;
> 4) the right to enjoy the protection of a healthy environment;
> 5) the right to enjoy cultural and social fulfillment.[84]

[80] Act of 6 January 2003 on the use of special investigation methods, *B.S.* 12 May 2003.
[81] Constitutional Court [*Arbitragehof*] No. 202/2004, 21 December 2004, paras. B.5.7.4-7, available via http://www.arbitrage.be.
[82] Act of 27 December 2005, *B.S.* 30 December 2005.
[83] 'Elk kind heeft recht op eerbiediging van zijn morele, lichamelijke, geestelijke en seksuele integriteit. (…)'
[84] '(1) Ieder heeft het recht een menswaardig leven te leiden. (2) Daartoe waarborgen de wet, het decreet of de in artikel 134 bedoelde regel, rekening houdend met de overeenkomstige plichten, de economische, sociale en culturele rechten, waarvan

Article 22bis has been inserted in the Constitution in 2000 in the aftermath of the Dutroux (child molester) case. There was little discussion about this new provision and no suggestion of expanding its scope to all humans.[85] The right to life is not protected as such in the Belgian Constitution. The right to individual integrity is considered either as a general principle of law,[86] or as an aspect protected by the right to privacy.[87] Many contemporary questions regarding biotechnology and the use of body material are dealt with from these two perspectives.[88] Belgium has neither ratified nor signed the European Convention on Human Rights and Biomedicine.
It is still unclear how Article 23, incorporated in the 1993/1994 revision, will be understood by the courts. Human dignity is introduced in the context of specific social and economic rights. Whether it will acquire a proper role outside this context is still not clear. This was not discussed during the procedure of amending the Constitution. The open formulation of Article 23, combined with the inclusion of specific rights such as health and protection of a healthy environment suggest that such a role is feasible. According to certain authors, the right to human dignity in Article 23 can be seen not only as a generic term for certain social and economic rights, but also as a classic first-generation right, and can, therefore possibly acquire direct effect and imply positive obligations.[89]

Legislation

The body is protected by several provision in the Criminal Code (hereinafter: CC), e.g., manslaughter (Article 393) and murder (Article 394). The Code of Criminal Procedure (hereinafter: CCP) contains detailed provisions regarding 'body searches of the inner part of bodies' (Article 90bis) and regarding the taking of DNA samples (Article 90undecies). In both cases, the examining magistrate plays a central role. Taking fingerprints of suspects is not regulated by law.[90] Surface searches of persons is regulated by Article 28 of the 1992 Police Act; it can be carried out by the police without mandate of an examining magistrate or prosecutor. Searches underneath the clothes fall within the scope of Article 28. This situation, created by the courts, which seemingly contradicts the broad wordings of Article 90bis CCP, is of course very police-friendly. Electronic monitoring of convicts was untill recently made possible not by law, but by Ministerial instructions of 9 August 2002. A new Act on the execution of sentences shifts this kind of measure from the executive authorities to the judiciary.[91]

Belgium does not have a full-fledged regulatory framework dealing with biomedical topics. Often, authors use the theory of personality rights to address specific issues. Over the past decades, many specific acts have been adopted to regulate certain new biomedical developments. Well-known is the Law of 13 June 1986 on the removal and transplantation of organs.[92] This law allows for consent-based transplantation of organs and tissues, but it requires a written consent from the donor. The law limits organ and tissue donation by children and

---

ze de voorwaarden voor de uitoefening bepalen. (3) Die rechten omvatten inzonderheid:
1° het recht op arbeid en op de vrije keuze van beroepsarbeid in het raam van een algemeen werkgelegenheidsbeleid dat onder meer gericht is op het waarborgen van een zo hoog en stabiel mogelijk werkgelegenheidspeil, het recht op billijke arbeidsvoorwaarden en een billijke beloning, alsmede het recht op informatie, overleg en collectief onderhandelen;
2° het recht op sociale zekerheid, bescherming van de gezondheid en sociale, geneeskundige en juridische bijstand;
3° het recht op een behoorlijke huisvesting;
4° het recht op de bescherming van een gezond leefmilieu;
5° het recht op culturele en maatschappelijke ontplooiing.'

[85] A. Vandaele & M. Verheyde, 'Article 22bis van de Grondwet: een grondwettelijke bescherming in de kinderschoenen', *TJK*, 2000, 4-15.

[86] A. Alen & J. Clement, *loc. cit.* n. *10*, at 193.

[87] C. Trouet, *Van lichaam naar lichaamsmateriaal. Recht en het nader gebruik van cellen en weefsels*, Intersentia, Antwerp, 2003, 587 p.

[88] Ibid.

[89] J. Vande Lanotte & Y. Haeck, 'Implementing human rights in Belgium: Sources, Monism – Dualism, Hierarchy, Direct effect, Third-party applicability and implementation mechanisms', in: J. Vande Lanotte, J. Sarkin & Y. Haeck (eds.), *Resolving the tension between crime and human rights. An evaluation of European and South-African issues*, Antwerp, Maklu, 2001, at 35.

[90] Chris Van den Wyngaert, *Strafrecht, strafprocesrecht en internationaal strafrecht*, Antwerp, Maklu, 2006, at 909-910.

[91] Act of 17 May 2006 concerning the external position of the convicted person, *B.S.* 15 June 2005. See ibid., at 485.

[92] Law of 13 June 1986 on the removal and transplantation of organs, *B.S.*14 February 1987, 2129–2132. See 'Belgium', *International Digest of Health Legislation*, Vol. 38, No. 3, p. 523–525.

prohibits the donation of organs and tissues for profit. With regard to organ transplantation of dead persons, the law opts for the 'presumed consent' system (citizens are supposed to become a potential donor unless they have objected during their life). This controversial aspect of the 1986 Law has found acceptance. A recent act, of 14 June 2006, enhances the system by taking away obstacles due to objections made by parents on behalf of their children.[93] Under the new system, the objection is annulled from the moment that children reach the age of eighteen. The Act does not apply to transplantations of testicles and ovaries or the use of gametes. So far, no constitutional issues have been raised in court.

Currently, a proposal is pending to regulate the use of gametes and donor insemination.[94] So far, these issues have remained to a large degree outside the realm of the other acts. The proposal prohibits commercial exploitation of gametes. With regard to donor insemination, a limit is set on the amount of children that can be created (only six women per donor can be inseminated). Women older than 47 are excluded from medical-assisted insemination. The proposal is much debated. Against the will of the opposition, it preserves the current system of donor anonymity (the sperm donor is not identified, and physicians are obliged to remain silent about the identity of the donor because of Article 458 CC (professional secrecy)). Earlier proposals to soften the consequences of anonymity by the creation of a special database (the 'double track' system) have not found a majority in Parliament.[95]

The Euthanasia Act of 28 May 2002 came into force on 23 September 2002.[96] The act is based on the will of the patient, but does not allow to dispose freely of one's life. Only patients older than 18 who are in a hopeless medical situation and under constant suffering can request euthanasia, by a written form. The act has been criticized for being voted without proper debate and for giving doctors and patients too much freedom.[97] The act has been contested before the Constitutional Court by pro-life organizations such as *Jurileven* and *Pro Vita*.[98] Referring (only) to Article 2 ECHR (right to life), the plaintiffs defended the view that the act violated this provision in combination with the rights of Articles 10 and 11 of the Constitution (equality and non-discrimination). People who suffer cannot make a free and informed choice to die and are therefore discriminated in comparison with healthy people. The Court considered all the guarantees in the Act (the age requirement, the written form, etc.) and found no violation.

The Act of 3 April 2003 on research on embryos *in vitro*[99] allows research on embryos *in vitro* under certain conditions: the research has a therapeutic purpose or contributes to a better knowledge of fertility, infertility, organ and tissue transplantation, prevention or treatment of diseases; the research is founded on the most recent scientific findings and conforms to the requirements of correct scientific methodology; the research is conducted in a licensed laboratory that is linked to an academic program for assisted reproduction or human genetics and is performed in appropriate technical and material conditions; the research is conducted under the supervision of a specialist or a qualified person; the research is performed on embryos during the first 14 days of development, the period of freezing not included, and no other research method is equally efficient. The creation of embryos *in vitro* for research purposes is forbidden, except if the goal of the research cannot be achieved by research on supernumerary embryos and insofar as the conditions of this law are respected (Art. 4 para. 1).

Researchers should bring their research projects before the local ethics committee of the academic institute involved and before the Federal Commission for medical and scientific research on embryos *in vitro* (Article 7). They need to obtain the written consent of persons involved; consent can only be given after the persons involved have received all necessary information regarding the following: the provisions of the law; the technology to obtain the gametes; the purpose, method, and time period of the research or treatment; the advice of the

---

[93] Law of 14 June 2006 amending the Law of 13 June 1986 on the removal and transplantation of organs, *B.S.* 28 August 2006.
[94] Proposal for an act concerning medical-assisted procreation and the use of saviour siblings and gametes, *Parliamentary Documents*, Senate [*Parl. St.,* Senaat], 2005-2006, No. 3-1440, available via www.senate.be.
[95] G. Pennings, 'The "double track" policy for donor anonymity', *Human Reproduction* 1997 12 (12), pp. 2839-2844.
[96] Act of 28 May 2002 with regard to euthanasia, *B.S.* 22 June 2002.
[97] M. Adams, 'De stok achter de deur. Over sancties, preventieve rechtshandhaving en een responsieve rechtscultuur', *R.W.*, 22 June 2002, Vol. 65, 1589-1598.
[98] Constitutional Court [*Arbitragehof*] No. 4/2004, 14 January 2004, available via http://www.arbitrage.be.
[99] *B.S.* 25 May 2003. For an English version, see http://www.eshre.com/emc.asp?pageId=751.

local ethics committee, and, if applicable, of the Federal Commission. The researcher informs the persons involved that they have the right to refuse to donate gametes or embryos for research or treatment and that they can withdraw their consent until the start of the research (Article 8). The Act establishes a Federal Commission for medical and scientific research on embryos *in vitro* (Article 9) that (among other things) evaluates the application of this law and all research projects submitted to her (Article 10).

Certain authors hold that the law is inspired by the idea that 'everything that is not forbidden by this law is allowed'.[100] The law does not prohibit germ-line gene therapy and therapeutic cloning. *A contrario*, these authors assume that these applications are allowed.

In a judgement of 19 December 1991, the Court has held that there is no constitutional duty of international treaty obliging Belgium to recognise an absolute right to life to embryos. The Abortion Act of 1 April 1990 did therefore not create an unjustified discrimination between born and unborn children. Neither was there a violation of these rights and of the privacy rights of the father who could not oppose a decision to have an abortion.[101] Perhaps this state of affairs explains the absence of a procedure before the Court with regard to the Act of 3 April 2003 on research on embryos.

The Act of 7 May 2004 concerning experimentation on human subjects is likewise a consent-based instrument, in this case, to regulate experiments that aim to develop biological and medical knowledge.[102] Chapter II of the Act contains definitions of the key notions in the Act and of its scope. Subsequent chapters deal with the requirements that have to be fulfilled in experiments and with the duties of the respective actors (the participant, the researcher, the institute, the minister, the ethical committees). Written consent should be given by all persons participating in experimentation (Article 6). In addition, the Act contains particular provisions for people under age (Article 7), particular provisions for people unable to give their consent (Article 8), and particular provisions for people whose consent cannot be given due to an emergency (Article 9).

The Act was contested, but not because of its implications for the body. It was contested successfully by the Flemish government, who argued that the Federal Act infringed on its competences. Article 2 paragraph 11 of the Act defines 'experimentation' as 'any trial, study, or investigation undertaken in humans with a view to developing biological or medical knowledge'. The Flemish government argued that by regulating not only every 'trial' but also every 'study' or 'investigation', the federal act violated its competence to legislate on scientific matters. In a judgement of 16 November 2005, the Court found that the federal legislator had violated the separation of powers between the respective legislators by including not only trials on humans, but also studies and investigations.[103]

2.5. Communication-related rights

2.5.1. Secrecy of communications

The Constitution

In the Belgian Constitution, there is no general article protecting the secrecy of (electronic) communications as such. Therefore, it needs to be examined whether the secrecy and confidentiality of communications is left unregulated by the Belgian constitutional legislator or whether it falls under the protection of other articles of the Constitution.

The most relevant article is Article 29 of the Constitution. This article reads as follows:

---

[100] G. Pennings, 'New Belgian law on research on human embryos: trust in progress through medical Science', *J Assisted Reprod Genetics*, 2003, Vol. 20 (8), pp. 343-346. G. Pennings & A. Van Steirteghem, 'De Belgische wet op onderzoek op embryo's in vitro', *Tijdschrift voor Fertiliteitsonderzoek*, 2004, Vol. 18 (1B), pp. 12-15.

[101] Constitutional Court [*Arbitragehof*] No. 39/1991, 19 December 2001, available via http://www.arbitrage.be.

[102] Act of 7 May 2004 concerning experimentation on human subjects, *B.S.* 18 May 2004. The Act implements European Directive 2001/20/ EC on the approximation of the laws, regulations and administrative provisions of Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use.

[103] Constitutional Court [*Arbitragehof*] No. 164/2005, 16 November 2005, available via http://www.arbitrage.be/. See George Pickering, 'Belgian Constitutional Court revokes part of clinical trials law', *Bird & Bird Life sciences update*, January 2006, pp. 1-2, available via http://www.twobirds.com.

> The secrecy of letters is inviolable.
>
> The law shall determine which officers are responsible for the violation of the secrecy of the letters entrusted to the postal services.[104]

This article dates from 1831 (old Article 22) and refers to 'letters'. While the wording of this article could lead to the question regarding its applicability to new forms of correspondence and communications, the principle of the secrecy of communications has – as already stated in the Koekkoek report of 2000[105] – been extended and applied in other legislation, such as in the Electronic Communications Act.[106] Although the intention to review Article 29 of the Constitution has been voiced several times, no progress has been made so far.

The right to respect for private correspondence and communications of any kind may also be protected under Article 22 of the Belgian Constitution (see *supra*, section 4.1). New forms of communications, irrespective of the medium used, may therefore also fall under the protection of Article 22 of the Constitution.[107] In this case, not only the communication itself, but also the information regarding the parties that participate in it and the details of the communication (traffic and location data[108] respectively) are protected by the Constitution.

As stated above, Article 22 will be interpreted in principle in conformity with Article 8 ECHR. The European Court of Human Rights has interpreted Art. 8 in a broad way, reasoning that '[t]here appears (…) to be no reason of principle why [the] understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.'[109] Furthermore, in *Kopp* v. *Switzerland*, the Court has ruled that 'telephone calls made from or to business premises (…) may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 §1 [ECHR].'[110]

Legislation

As already stated, the freedom and secrecy of electronic communications have been dealt with extensively in other legislation. By a 1994 Act penalizing wiretapping, penalties are provided for the crimes of interception of communication by a public official or civil servant (Article 259*bis* CC) and for breaches of the secrecy of private communications and telecommunications (Article 314*bis* CC*)* during the transfer of a private communication between other parties, in cases not foreseen by law.[111] The Articles 90ter through 90decies CCP describe the cases and procedure when interception, cognizance, and recording of private communications and telecommunications are allowed for the investigation of specific criminal offences. The law provides that this shall be under the supervision of the examining magistrate.

Other legislation with rules and exceptions on the secrecy of communications concerns the Electronic Communications Act, which implemented the European directives for the new electronic-communications regulatory framework. In Article 2 of the Act, the terms 'electronic communications networks', 'providers of electronic communications networks', and 'electronic communications services' are defined. However, unlike the European directives, no definition of the term 'communication' is included, which may lead to confusion regarding what falls under the provisions of the Act.

Article 124 Electronic Communications Act protects the secrecy of the existence of a communication amongst third persons, including the identification of the persons involved, and

---

[104] 'Het briefgeheim is onschendbaar. De wet bepaalt welke agenten verantwoordelijk zijn voor de schending van het geheim der aan de post toevertrouwde brieven.'
[105] A. Koekkoek , P. Zoontjens, et al., *op. cit. n. 7,* at 143.
[106] See, for example, Article 122 et seq. of the Act of 13 June 2005 on electronic communications [Wet van 13 juni 2005 betreffende de elektronische communicatie], *B.S.* (2nd ed.), 20 June 2005 (hereinafter 'Electronic Communications Act').
[107] K. Rimanque, *De Grondwet toegelicht, gewikt en gewogen* [The Constitution commented and reviewed], Antwerp, Insertia, 2005, at 92.
[108] See for the definitions, Article 2.6 and 2.7 Electronic Communications Act.
[109] *Niemietz* v. *Germany*, Judgement of 16 December 1992, paras. 28–33.
[110] *Kopp* v. *Switzerland*, Judgement of 25 March 1998, para. 50.
[111] Act of 30 June 1994 for the protection of the private life against listening in, taking knowledge, and opening of private communciation and telecommunication, *B.S.* 24 January 1995.

prohibits the intentional revealing of information related to a communication taking place via electronic means, without the consent of the parties concerned.[112] Article 125 provides for exceptions to this principle of secrecy of communication and to the Articles 259*bis* and 314*bis* CC, for example, if the law allows or imposes taking knowledge of the existence of the communication, for the good functioning of the network and network service, for emergency services, and for preventing spam.[113] Article 126 Electronic Communications Act stipulates that the provider of electronic communications services or networks (including resellers) shall retain the 'traffic data' and 'identification data' of end-users for a period between 12 and 36 months. For enforcing this obligation, a royal decree is currently in preparation. The decree will need to define the exact retention period and under what conditions the providers will register and retain the data at issue. This will be allowed for the investigation and prosecution of criminal acts, for the tracking of malicious calls to emergency services, and to enable the research of the Ombudsman for Telecommunications [*Ombudsdienst voor Telecommunicatie*] in revealing the identity of people making improper use of electronic communications services or networks.[114]

In December 2001, a new legislative provision was enacted that bans anonymity for subscribers and users of telecommunications network services and equipment.[115] It prohibited the supply and use of telecommunications services or equipment that render caller identification impossible, or that otherwise make it difficult to track, monitor, wiretap, or record communications. This provision is now part of Article 127 Electronic Communications Act. That article further allows the King to determine the technical and administrative measures to be imposed on operators or end users, in order to be able to identify the calling line in cases of emergency calls as well as for the investigation of specific crimes. An exception to this rule could be established for encryption systems that can be used to guarantee the confidentiality of communications and the security of payment. Article 128 allows taking knowledge and recording of electronic communications and traffic data with the sole purpose of the control of calling centers under certain conditions. Article 128 further allows the recording of electronic communications and the related traffic data carried out in the course of lawful business practice or other professional communication, when all parties are informed in advance of the recording, the precise purposes thereof, and the time period for which the recording will be stored. Article 129 prohibits using electronic communication networks for the storage of information for gaining access to information stored in the terminal equipment of the user or the subscriber, such as cookies and spyware. Such use is only allowed when the subscriber or the user concerned are informed in a clear and comprehensive way, in accordance with the Data Protection Act (see *supra*, section 4.1), and when he is offered the right to refuse such processing. Furthermore, technically storing information or accessing information stored on the terminal equipment of the user or the subscriber is allowed when its sole purpose is to carry out or to facilitate the transmission of a communication or to provide an information-society service that was explicitly requested by the user or the subscriber. This provision has triggered a debate in Belgium: the question is whether the consent of the user shall be given *before* the installation of the information on his terminal equipment, as the Act does not mention anything about the time when consent shall be given.

The Data Protection Act addresses the issue of data security, requiring data controllers to take 'appropriate technical and organizational measures'[116] governing the processing to be carried out. To the extent that this principle covers the security requirements and robustness of the network itself, it overlaps with the security and confidentiality requirements laid down in Articles 114 and 122 et seq. Electronic Communications Act. Taken as a whole, this principle imposes a statutory obligation on data controllers to ensure that personal data are processed in a secure environment. This means that data controllers must consider the state of technological development and the cost of the implementation of any security measures. Bearing in mind these

[112] Article 124 Electronic Communication Act is similar to Article109ter D to which the Koekkoek report refers (p. 150) and which it replaced.
[113] Article 125 para. 1 Electronic Communication Act is similar to Article109ter E to which the Koekkoek report refers (p. 150) and which it replaced.
[114] E. Kosta & P. Valcke, 'Retaining the data retention directive', 22 *Computer Law & Security Report* 2006, pp. 370 et seq., at 377.
[115] Art. 150, 2° Programmawet van 30 december 2001 [Article 150, 2° of the Program Law of 30 December 2001], *B.S.* 31 December 2001.
[116] Article 16 para. 1 Data Protection Act.

factors, the security measures adopted by the data controllers must ensure a level of security that is appropriate to both the nature of data to be protected and the likely harm that would result from a breach of this principle.[117]

The control by employers of on-line communication data of employees is regulated in a so-called Collective Labour Agreement No. 81 of 26 April 2002, concluded in the National Labour Council.[118] This agreement sets rules on the control of electronic on-line communication data at the workplace, in an attempt to clarify the constitutional and legal rights and principles relating to privacy on the one hand, and the secrecy of communications on the other. In particular, the Collective Labour Agreement determines how the principles of finality, proportionality, and transparancy of the Data Protection Act need to be applied to the control of employee on-line communications. The agreement states that the employer shall only control on-line communications data of his employees for the prevention of illicit facts, facts contrary to good manners, or facts that may harm the dignity of another person, for the protection of the confidential information and interests of the company, for ensuring the safety and proper technical functioning of the network, or for controlling the compliance with the company's ICT use regulations.[119] In the latter case, the employer is not entitled to immediately identify the employee who does not respect the ICT policy, but shall first launch an information campaign stating that breaches have been spotted and that upon repitition thereof, the employee(s) concerned will be identified and sanctioned. The employee, however, is entitled to a hearing by the employer before sanctions are taken.

2.5.2. Freedom of expression

The Constitution

The Belgian constitutional 'frame of reference'[120] concerning the right to freedom of expression and freedom of the press is shaped by Articles 19, 25, and 150 of the Constitution.[121] Article 19 refers to the freedom of expression, Article 25 introduces the freedom of the press, and Article 150 stipulates that 'press crimes' [*drukpersmisdrijven*][122] should be brought before a jury (at the 'Hof van Assisen').[123] No fundamental developments relating to these articles have occurred since the Koekkoek report of 2000.

> **Article 19**
>
> Freedom of worship, public practice of the latter, as well as freedom to express one's opinions on all matters, are guaranteed, except for the criminalisation of offenses committed when using these freedoms.
>
> **Article 25**

[117] P. Carey, *E-Privacy and Online Data Protection*, Butterworths, 2002, at 58.
[118] The Collective Labour Agreement No. 81 on the protection of privacy of the employees in relation with the control of electronic on-line communication data can be found at http://www.privacycommission.be/normatieve_teksten.htm (last visited 14 December 2006).
[119] See also X,, 'National Labour Council adopts Collective Labour Agreement on the control of electronic on-line communication data of employees', *Stibbe ICT Law Newsletter* 2002, No. 5, p. 3.
[120] J. Velaers, 'De actuele toepassing van de grondwettelijke waarborgen inzake de vrijheid van de media' [The current application of the constitutional guarantees regarding freedom of the media], in: Interuniversitair Centrum Mensenrechten, *Jaarboek Mensenrechten 1995-1996* [Yearbook Human Rights 1995-1996], Antwerpen, Maklu, 1996, at 85.
[121] Cf. Koekkoek et al., *op. cit.* n. 7, at 142-143. A detailed description of these articles is available in D. Voorhoof, *Handboek Mediarecht* [Handbook Media Law], Brussel, Larcier, 2003, at 26-30 and 53-79; E. Lievens, P. Valcke, and D. Stevens, 'Vrijheid van meningsuiting' [Freedom of expression], in: R. De Corte, ed., *Praktijkboek Recht & Internet* [Book of practice law & the Internet], Brugge, Vanden Broele, 2005, 9; P. Valcke, 'Democratie en diversiteit op de informatiesnelweg: beschouwingen over de vrijheid van meningsuiting op het Internet' [Democracy and diversity on the information highway: considerations on freedom of expression on the Internet], in: Interuniversitair Centrum Mensenrechten, *De rechten van de mens op Internet* [Human rights on the Internet], Antwerpen, Maklu, 2000, at 93; C. Uyttendaele, *Openbare informatie – Het juridisch statuut in een convergerende mediaomgeving* [Public information – The legal statute in a converging media environment], Antwerpen, Maklu, 2002, at 244 et seq.; S. Hoebeke and B. Mouffe, *Le droit de la presse,* Louvain-la-Neuve, Bruylant Academia, 2005, at 57 et seq.
[122] However, press crimes inspired by racism or xenophobia do not have to be brought before a jury.
[123] The 'Hof van Assisen' is a court of law composed by both professional judges and a jury of citizens, which judges the most serious and delicate offences.

> The press is free; censorship can never be established; no security from authors, publishers, or printers can be demanded. When the author is known and resident in Belgium, neither the publisher, nor the printer, nor the distributor can be prosecuted.
>
> **Article 150**
>
> The jury is established for all criminal matters, in addition to political and press crimes, except for press crimes inspired by racism or xenophobia.[124]

The three articles relating to freedom of expression and freedom of the press are still formulated in exactly the same way as in 1831,[125] despite the enormous evolution that has occurred in the media landscape. It is, however, generally accepted that – due to the technology-neutral wording of Article 19 –[126] the constitutionally protected freedom of expression is applicable to any medium: the written press, radio, television broadcasting, movies, the Internet, and any future media.[127] Contrary to Article 19, Articles 25 and 150 are not formulated in the same technology-neutral manner, as they use the word 'press' or 'printing press'. The Belgian courts seem reluctant to extend the specific freedom of the press to new information and communication technologies.[128] The Belgian Supreme Court, for instance, is of the opinion that Article 25 is not applicable to audiovisual media.[129] This does not alter the fact that a more extensive interpretation of the concept 'press' has been advocated.[130] The problem is that an extension of this concept in Article 25 would also lead to an extension of the competence of the '*Hof van Assisen*' (*supra*). Since the Second World War, however, only one 'press crime' has been brought before this court.[131] Hence, *de facto*, an extension of the concept 'press crime' would also lead to an extension of criminal immunity.[132] Although Article 150 has been declared 'open for constitutional review' a number of times, as was also announced in the Koekkoek report of 2000,[133] this has still not led to an actual constitutional change.[134]

Case law

Whether 'press crimes' can be committed over the Internet is still an open question in Belgium. Whereas a lower court has explicitly considered the Internet as a type of 'press' ('attendu que les messages diffusés par Internet peuvent constituer des délits de presse'),[135] a year later, the Court of Appeal did not confirm this explicitly.[136] In another, lower-court case, however, it was accepted

---

[124] Art. 19: 'De vrijheid van eredienst, de vrije openbare uitoefening ervan, alsmede de vrijheid om op elk gebied zijn mening te uiten, zijn gewaarborgd, behoudens bestraffing van de misdrijven die ter gelegenheid van het gebruikmaken van die vrijheden worden gepleegd.' Art. 25: 'De drukpers is vrij; de censuur kan nooit worden ingevoerd; geen borgstelling kan worden geëist van de schrijvers, uitgevers of drukkers. Wanneer de schrijver bekend is en zijn woonplaats in België heeft, kan de uitgever, de drukker of verspreider niet worden vervolgd.' Art. 150: 'De jury wordt ingesteld voor alle criminele zaken, alsmede voor politieke misdrijven en drukpersmisdrijven, behoudens voor drukpersmisdrijven die door racisme of xenofobie ingegeven zijn.'

[125] J. Velaers, *loc. cit.,* n. 120, at 83.

[126] C. Uyttendaele, 'Bescherming van de communicatievrijheid in digitale omgevingen: verminderde bruikbaarheid van nationaal (grondwettelijk) recht?' [Protection of the freedom of communication in digital environments: decreased utility of national (constitutional) law?] , in: Interuniversitair Centrum Mensenrechten, *Jaarboek Mensenrechten 2000-2001 van het Interuniversitair Centrum Mensenrechten* [Yearbook Human Rights], Antwerp, Maklu, 2002, at 33-34.

[127] J. Velaers, *loc. cit.* n. 120, at 85; C. Uyttendaele, *op. cit.* n. 121, at 253.

[128] C. Uyttendaele, *op. cit.* n. 121, at 252.

[129] 'Art. 18 Constitution [since 1994: Art. 25, authors' note] is not applicable to broadcasts via television or cable television, since these are not forms of expression by means of printed writing' (authors' translation). Cf., Cass. 9 December 1981, *Arr. Cass*. 1981, pp. 493-496.

[130] J. Velaers*, loc. cit.* n. 120, at 70 and 194-196.

[131] D. Voorhoof, *op. cit.* n. 121, at 76.

[132] C. Uyttendaele, *loc. cit.* n. 126, at 36.

[133] A. Koekkoek*, op. cit*., n. 7, at 143.

[134] J. Velaers, *loc. cit.* n. 120, at 202-203; C. Uyttendaele, *loc. cit.* n. 126, at 41.

[135] Corr. Brussel (55e k.) 22 December 1999 (with comment of Dirk Voorhoof), *Auteurs & Media* 2000, Vol. 1-2, at 134-138. The reasoning of the Court is as follows: 'Attendu que si le concept de délit de presse devait être limité par l'approche de son sens littéral (presse écrite par opposition aux nouveaux moyens, toujours plus sophistiqués, d'expression de la pensée), une telle interprétation constituerait une "méconnaissance" de l'esprit du constituant qui a voulu protéger la libre diffusion des idées et non pas l'instrument de celle-ci, la presse en tant que telle dont, de surcroît, l'évolution future sous des formes nouvelles telles que la télévision lui était bien évidemment inconnue. Attendu que pareil raisonnement doit être tenu en ce qui concerne le nouveau mode d'expression de la pensée que constitue le réseau Internet.'

[136] However, it should be noted that in the case at hand it did not really matter whether the crime could be qualified as a

without much doubt that a press crime could be committed by way of the Internet.[137] At the moment, there is altogether not enough jurisprudence related to freedom of expression and new media to draw valuable conclusions over the definitive Belgian approach to this digital constitutional right.

Hate speech on the Internet

From 2000 onwards, a number of court cases have dealt with racism disseminated over the Internet. In Belgium, in 1981, the Anti-racism Act [*Anti-racisme Wet*] was introduced.[138] It is generally accepted that Article 1 of this Act,[139] in combination with Article 444 CC,[140] applies to images and texts that circulate on the Internet.[141] Repeatedly, lower courts have convicted people who distributed racist material via the Internet.[142]

Furthermore, in order to align Belgian legislation with the Convention on Cybercrime[143] and the Additional Protocol to this convention,[144] a bill was proposed in July 2004.[145] This bill aimed at extending the Act of 23 March 1995 on punishing the denial, minimisation, justification, or approval of the genocide perpetrated by the German National-Socialist Regime during the Second World War[146] to 'genocide' in general, as suggested by Article 6 of the Additional Protocol. This proposal caused a number of heated debates in the House of Representatives and the Senate, particularly over the exact definition of the concept of 'genocide' and the proposal's implications for the freedom of expression.[147] In the end, it was decided that a separate bill would be introduced, following a thorough study of this subject by the Interministerial Commission on Human Rights. At the moment, such a new bill has not yet been introduced.

Finally, in the struggle against online hate speech, in 2006 an online 'hotline' was established by different actors, including the Belgian federal government, to facilitate the reporting of online cyberhate: www.cyberhate.be.

Confidentiality of sources

In June 2006, the Constitutional Court issued a judgement with significant implications for an important aspect of the right to freedom of expression, namely, the confidentiality of journalistic sources. Since the introduction in April 2005 of the Act on the protection of journalistic sources,[148] the right not to disclose certain sources had been attributed to 'journalists, hence everyone who is

---

'press crime', as the case centered around racist remarks. As mentioned above (footnote 123), since 1999 the 'Hof van Assisen' is no longer competent with respect to racist or xenophobe press crimes, hence the 'correctionele rechtbank' was competent anyway.

[137] Rb. Brussel 2 March 2000 (with comment of Marc Isgour), 1 *Auteurs & Media* 2001, pp. 151-157.

[138] Act of 30 July 1981 on the punishment of certain acts motivated by racism or xenophobia, *B.S.* 8 August 1981. An English version of the Act is available at http://www.diversiteit.be/CNTR/EN/legislation/Racism/leg_fed_racism.htm.

[139] Article 1 criminalises racist or discriminatory behaviour in certain circumstances.

[140] Article 444 CC describes conditions that certain kinds of behaviour must fulfill in order to be criminalised.

[141] D. De Prins, S. Sottiaux, and J. Vrielink, *Handboek discriminatierecht* [Handbook discrimination law], Mechelen, Kluwer, 2005, at 320.

[142] Corr. Antwerpen (4e k.) 9 September 2003, *Auteurs & Media* 2004, Vol. 1, pp. 83-85; Corr. Brussel 15 January 2002, available at www.antiracisme.be; Corr. Brussel (11e k.) 27 June 2000 (with comment by D. Voorhoof), *Auteurs & Media* 2001, Vol. 1, pp. 142-147. See also Corr. Brussel 22 December 1999 (with comment by D. Voorhoof), *Auteurs & Media* 2000, Vol. 1-2, pp. 134-138.

[143] Council of Europe, Convention on Cybercrime, ETS No. 185, 23 November 2001, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[144] Council of Europe, Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, 28 January 2003, available at http://conventions.coe.int/Treaty/EN/Treaties/Html/189.htm.

[145] Proposal to amend the Act of 28 November 2000 regarding computer crime, the Act of 20 June 1994 regarding copyright and neighbouring rights and the Act of 23 March 1995 on punishing the denial, minimisation, justification or approval of the genocide perpetrated by the German National Socialist Regime during the Second World War, *Parliamentary Documents*, Chamber [*Parl. St.,* Kamer], 2003-2004, No. 1284.

[146] Belgian courts have already convicted people who disseminated negationist information via the Internet; see also Corr. Brussel 15 January 2002, available at www.antiracisme.be, and D. Voorhoof, 'Eén jaar effectieve straf voor holocaustontkenner' [One-year sentence for denial of holocaust], 109 *De Juristenkrant* 2005, pp. 2-3.

[147] See, e.g., 'Report on behalf of the Commission "Justice" by Mrs. Defraigne and Talhaoui', *Parliamentary Documents*, Chamber [*Parl.St., Kamer*] 2004-2005, No. 1135/3, avialable via http://www.senate.be.

[148] Act of 7 April 2005 on the protection of journalistic sources, *B.S.* 27 April 2005.

working either self-employed or as an employee, as well as any legal entity, and who regularly contributes directly to assembling, editing, producing or disseminating information aimed at the public via a medium'. The Constitutional Court tested the scope of application *ratione personae* of this act against the fundamental principles of freedom of expression and freedom of the press and found that Article 2, 1°, of the act infringed these principles because it denies the right to protection of sources to certain people. Thus, from now on, 'everyone who directly contributes, edits, produces or disseminates information aimed at the public via a medium' has the right to keep his or her sources confidential. Hence, for instance, bloggers who regularly publish new facts or opinions on their web pages could now be considered to fall within the scope of application of the act.

Right to reply

In Belgium, for the time being, no technology-neutral legislative framework with respect to the right to reply has been established. So far, a number of attempts at the federal level[149] to broaden the scope of application of the Act of 23 June 1961 on the right to reply[150] to all periodic media have failed. However, the Flemish Community has, meanwhile, on the basis of its competence with respect to radio and television broadcasting,[151] established its own regulatory framework concerning the right to reply on radio and television.[152] Noteworthy is the fact that this framework – due to the broad interpretation of the Constitutional Court[153] – is applicable to programmes distributed via the Internet or on demand as well.

Children: freedom of expression v. protection against harmful material

The protection of minors against harmful new media content has been on the policy agenda globally for the past decade. In Belgium, one legislative initiative has been taken regarding this issue, which, however, proved unsuccessful. The Bill concerning the protection of minors against harmful content in the information society[154] had two key objectives. On the one hand, intermediaries would be obliged to offer free filtering solutions to the end-user (Art. 3). On the other hand, a trusted third party would be established, in charge of assessing the harmful character of information as well as attributing specific 'child-friendly' labels (Art. 4). Whereas the first idea could be welcomed, the latter proposal concerning the practical functioning of the trusted third party was formulated in a vague way, leaving room for significant criticism.[155] Hence,

---

[149] *Parliamentary Documents*, Chamber [*Parl.St.,* Kamer] 1999-2000, No. 325/1 and *Parliamentary Documents*, Chamber [*Parl.St.,* Kamer] 1999-2000, No. 815/1 (also *Parliamentary Documents*, Chamber [*Parl.St.,* Kamer] 1999-2000, nr. 816/1). For more details, see D. Voorhoof, 'Het recht van antwoord in België: een inspirerend voorbeeld voor Nederland? Deel II' [The right to reply in Belgium: an inspiring example for the Netherlands? Part II], 5 *Mediaforum* 2001, pp. 152-160.

[150] Act of 23 June 1961 on the right to reply, *B.S.* 8 July 1961.

[151] For more details on the relation between the federal and Flemish initiatives in the light of the Belgian division of competences, cf., P. Valcke, *Digitale Diversiteit – Convergentie van Media-, Telecommunicatie- en Mededingingsrecht* [Digital diversity – Convergence of Media, Telecommunications and Competition Law], Brussel, Larcier, 2004, at 315-317.

[152] Decree of the Flemish Parliament of 18 July 2003 on the adaptation of certain provisions of the Decrees on radio and television broadcasting, coordinated on 25 January 1995 regarding the introduction of the right to information via radio and television and the creation of a right to reply with respect to radio and television, *B.S.* 3 September 2003. This Decree has in the meantime been incorporated by the Decrees on radio and television broadcasting, coordinated on 4 March 2005, *B.S.* 8 April 2005 (Articles 177 et seq.).

[153] 'Radio-omroep is een zaak van het uitzenden van radio- of televisieprogramma's, bij wege van al dan niet gecodeerde signalen; een radio-omroepprogramma is, vanuit het oogpunt van degene die het uitzendt, bestemd voor het publiek in het algemeen of voor een deel ervan, en heeft geen vertrouwelijk karakter, zelfs wanneer op individueel verzoek wordt uitgezonden en ongeacht de techniek die voor de uitzending ervan wordt gebruikt, met inbegrip van de zogenaamde point-to-point-techniek die voorheen niet voor radio-omroep werd aangewend. Een dienst die geïndividualiseerde en door een vorm van vertrouwelijkheid gekenmerkte informatie levert, valt daarentegen niet onder de radio-omroep.' Constitutional Court [*Arbitragehof*] No. 156/2002, 6 November 2002, available via http://www.arbitrage.be. The judgement is also published on *Mediaforum* 2003, Vol. 3, pp. 112-116, with comment by P. Valcke and C. Uyttendaele, and was confirmed by Constitutional Court [*Arbitragehof*] No. 132/2004 14 July 2004 (B.10.1 and B.10.2) and Constitutional Court [*Arbitragehof*] No.155/2004 22 September 2004 (B.4.1 and B.4.2), *Auteurs & Media* 2005, Vol. 2, pp. 159-166, with comment by D. Stevens, and 21 *Revue du Droit des Technologies de l'Information*, 2005, pp. 51-73, with comment by R. Queck and P. Valcke.

[154] Proposal for an Act regarding the protection of minors against harmful content in the information society, *Parliamentary Documents*, Senate [*Parl.St.,* Senaat] 2003-2004, 3-484, available at http://www.senaat.be.

[155] For a more detailed appraisal, see E. Lievens and J. Dumortier, 'Bescherming van minderjarigen online: stand van zaken en blik op de toekomst' [Protection of minors online: state of the art and a look at the future], 2 *Computerrecht* 2005, pp. 59-

the fact that the proposal sank into oblivion in the course of 2004 should perhaps not be regretted.

Another project that can be mentioned in this context is 'SaferChat', which was set up by the Minister for Computerisation of the State, Peter Vanvelthoven, in cooperation with the Belgian Internet Service Providers Association.[156] This public-private partnership established a system that requires the use of a child's electronic identity card to gain access to a 'safe' chatroom.[157] All children over the age of twelve receive a free card reader in an attempt to promote this feature.[158] In order to verify the age of a person requesting access to a particular 'safe' chatroom, the National Registry identification number embedded in the electronic identity card is used.[159] This scheme, however, is also prone to criticism. It raises significant privacy concerns,[160] and will probably fail to be successful because it is limited to particular chatrooms.[161]

Other developments

To our knowledge, in Belgium, there are currently no active debates at the policy level regarding freedom of expression related to search engines,[162] filtering, or the chilling effect that can result from these developments.

2.6. Other and new constitutional rights

The massive use of new technologies has had an influence on the exercise of certain rights, resulting in an adaptation of the legislation, usually following solutions established by jurisprudence. Several modifications should be mentioned: the notion of equal treatment (2.6.1), no crime without law (2.6.2), the right of access to public information (2.6.3), the right to communicate with the Administration by electronic means (2.6.4), and e-voting (2.6.5).

2.6.1. Equal treatment

Articles 10 and 11 of the Constitution guarantee equal treatment and the benefit of the fundamental rights and freedoms to all Belgians without discrimination. The relevant sections read as follows:

> **Article 10**
>
> 2. Belgians are equal before the law (…);
>
> **Article 11**

64.

[156] For more information, in Dutch and French, see http://www.saferchat.be/.

[157] 'Safe' in this instance means that only children will be present in this chatroom, and hence no adults with possible bad intentions.

[158] Children under the age of twelve do not possess an electronic identity card. In the future, this lacuna would be overcome by providing children under the age of twelve with a particular electronic certificate.

[159] Privacy Commission, *Consultation concerning the application of the Federal Public Agency for Information and Communication Technology (Fedict) to be authorised to use the National Registry identification number to enable the safe use of internet services*, No. 20/2005, 25 May 2005, available at http://www.privacy.fgov.be/machtigingen/Ber020_2005_RR.pdf (in Dutch).

[160] It could be argued that in this scheme, the child's right to privacy is restricted disproportionately by using its National Registry identification number. In the regime proposed by Fedict, children would be identifiable every time they log in on a certain chatroom, due to the fact that when the electronic identity card is used, not only the National Registry number (which reveals the exact date of birth and the sex), but also the name of the child is transmitted. This contradicts the fact that actually, only one attribute of their identity, i.e., that they are under a certain age, would be needed to grant access to the 'safe' chatroom.

[161] Clickx, 'Chatten: veilig of vunzig?' [Chatting: safe or dirty?], 24 January 2006, available at http://clickxmagazine.zdnet.be/magazines.cfm?id=52968. This article claims that research has proven that almost no children use the chatrooms.

[162] A recent judgement, however, relates to Google News and their alleged infringement of the copyright of newspapers linked to the news portal; see http://www.chillingeffects.org/international/notice.cgi?action=image_7796. For more information, see L. Kaye, 'When is a search engine not a search engine? Answer: when it's a publisher', available at http://www.scl.org/editorial.asp?i=1382.

> The enjoyment of the rights and freedoms of the Belgians have to be assured without discrimination.[163]

These constitutional rights were invoked when the decision was made to reform the publication of the Belgian State Gazette into an electronic publication. In the Belgian State Gazette, all new laws and regulations, as well as other notifications, are made public to the citizens. The federal legislator had decided to replace the distribution of the printed version of the Belgian State Gazette to the public by an electronic copy on the Internet site of the Belgian State Gazette. The Constitutional Court annulled the relevant articles in the Program Act I of 24 December 2002, because 'a considerable number of persons would no longer have access to the official texts, particularly because of the lack of accompanying measures which give them the possibility to consult these texts, while before, they had the possibility to take knowledge of the content of the Belgian State Gazette without specific tools and without the need of any other qualification than the ability to read'.[164] In the meantime, new legislative measures have been taken in order to guarantee due access by the citizens to the electronic version of the Belgian State Gazette.

2.6.2. No crime without law

Article 12, paragraph 2, of the Constitution states that nobody shall be prosecuted without prior legislative rules decided by a democratic body. The provision reads as follows:

> Nobody shall be prosecuted unless in the cases determined by law and in the manner prescribed by law.[165]

This constitutional principle requires that new legislation is adopted in order to cope with new forms of criminal behaviour in the information age. This constitutional right is relevant in the context of digital rights because it requires that the legislator defines clearly when the (ab)use of information technology becomes a crime. In 2000, a new law on computer crime was adopted.[166] The Act introduced several new crimes in the Criminal Code, such as fraud in informatics (Article 210bis), deception in informatics (Article 504quater), unlawful access to information systems and data (Article 550bis), and informatics sabotage (Article 550ter).[167] In many of these articles, reference is also made to the use of 'any other technological means' to commit the crime, in an attempt to make the description technology-neutral. The new Act also introduced several new articles relating to search and seizure in informatics in the Code of Criminal Procedure, and it modified some other articles relevant to the secrecy of communications.[168] In July 2004, another bill was proposed to adapt the provisions of the Criminal Code to the Convention on Cybercrime and the Additional Protocol.[169] As a result, some minor modifications to the provisions relating to computer crimes have been discussed and approved, in order to remove uncertainty in which cases one would be prosecuted.[170] As stated before, the only element lacking parliamentary consensus is the concept of 'genocide' in the bill on criminalization of acts of a racist and xenophobic nature committed through computer systems.[171]

2.6.3. Right of access to public information

Article 32 of the Constitution was amended in 1993 to include a right of access to government documents. Article 32 reads as follows:

---

[163] Art. 10, para. 2: 'De Belgen zijn gelijk voor de wet; (…)'. Art. 11: 'Het genot van de rechten en vrijheden aan de Belgen toegekend moet zonder discriminatie verzekerd worden. (…)'

[164] Constitutional Court [*Arbitragehof*] No. 106/2004, 16 June 2004, *B.S.* 2 July 2004, 53697, B.21. In the meantime, new legislation allows the e-publication of the Belgian Official Gazette; see the Act of 20 July 2005 with several provisions, *B.S.* 29 July 2005.

[165] 'Niemand kan worden vervolgd dan in de gevallen die de wet bepaalt en in de vorm die zij voorschrijft.'

[166] Act of 28 November 2000 relating to computer crime, *B.S.* 3 February 2001.

[167] A few cases have been brought before the courts based on the new articles. See, e.g., Rb. Hasselt, 21 January 2004, *Computerrecht* 2004, p. 130.

[168] See above, section 2.5.1, in particular in relation with the procedure for wiretapping under the supervision of a judge.

[169] See also above, n. 145.

[170] Act of 15 May 2000 modifying Articles 259bis, 314bis, 504quater, 550bis en 550ter of the Criminal Code, *B.S.* (2nd ed.), 12 September 2006, 46332.

[171] See above, section 2.5.2.

> Everyone has the right to consult any administrative document and to obtain a copy, except in the cases and under the conditions stipulated by law, decree, or ruling referred to in Article 134.[172]

The legislators on the federal and regional level must ensure these rights within their respective powers and competences. All governments can define exemptions that must be abided by other governments, if the matter pertains to a competence of the former government.
On the federal level, the Act on the transparency of the administration was enacted in 1994.[173] The Act regulates the double role of the government: actively ensuring that government information is disseminated among the public, and the right for individuals to request information and access to government documents. The government has the obligation to respond within thirty days to requests. Should the request be denied, the reasons must be provided, along with an explanation of the process of appeal.

Government documents are defined in a broad sense, and the Act does not refer to a specific method by which the information should be stored. The requests made to the government have to be in writing. Requests made by electronic mail or fax are problematic when the request pertains to personal information. In principle, the right to access of information is exercised free of charge, but the government can ask a fee for paper copies.

Generally, there are three exemptions in which the government can deny a request for access. First, certain information relating to public security, international relations, defense, criminal investigations, or confidential information can be withheld unless the public interest warrants its release. Second, the right to personal privacy must prevail, as well as legal restraints regarding secrecy. Third, there is a discretionary category for requests that are abusive, vague, or misleading.

Meanwhile, EC Directive 2003/98/EC on the reuse of public-sector information has put forward rules applicable to the reuse of public-sector information resources, creating the possibility for commercial exploitation. Although the deadline was 1 July 2005, it has not yet been transposed into Belgian law.[174] A bill is pending in Parliament that would allow public-sector bodies to authorize or refuse the re-use of documents.[175] A procedure of appeal will be created. It excludes any documents over which third parties have intellectual-property rights. Governments have the right to charge for the delivery of data or documents, but this price must be based on real costs or can, in some cases, include a reasonable return on investment. If documents contain personal data, the government has the responsibility to make them anonymous with reasonable means, in accordance with the opinion of the Privacy Commission.[176]

Earlier, the European Directive of 7 June 1990 regarding free access to information regarding environmental matters had imposed certain obligations on the member states. As a result, in 2000, amendments were approved regarding documents relating to the environment. These documents cannot be withheld under the exemptions mentioned above, unless the Act stipulates otherwise in cases where the second category of exemptions would be valid. Furthermore, the Aarhus Convention on Access to Information on Environmental Matters was signed by Belgium in 1998 and ratified in 2001. The EC Directive 2003/4/EC on public access to environmental information replaced the previous directive and also proscribed a right to commercial exploitation. It was transposed in Belgian law in 2006 by the different government levels.[177]

On the regional level, legislation exists similar to the federal Act of 1994 regarding the right of access to public information.[178] Since the competences regarding the municipalities and

---

[172] 'Ieder heeft het recht elk bestuursdocument te raadplegen en er een afschrift van te krijgen, behoudens in de gevallen en onder de voorwaarden bepaald door de wet, het decreet of de regel bedoeld in artikel 134.'
[173] Act of 11 April 1994 regarding the transparency of the administration, *B.S.* 30 June 1994.
[174] K. Janssen, 'Hergebruik van overheidsinformatie – binnenkort ook bij u in de winkel?' [Re-use of public-sector information – soon in your shop too?], 2 *Privacy en Informatie* 2006, pp. 59-63.
[175] Proposal for an Act to transpose Directive 2003/98/EC of the European Parliament and the Council of 17 November 2003 regarding the reuse of public-sector information, *Parliamentary documents*, Chamber [*Parl. St.* Kamer*],* 2005-2006*,* nr. 2634.
[176] Privacy Commission, *Opinion on the draft bill in order to transpose directive 2003/98/EC of the European Parliament and the Council of 17 November 2003 regarding the reuse of public-sector information*, No. 04/2006, 8 February 2006.
[177] Act of 5 August 2006 regarding access by the public to environmental information, *B.S.* 28 August 2006.
[178] For the Flemish Region, see Decree of 26 March 2004 regarding the transparency of administration, *B.S.* 18 August 2004; for the Brussels Region, see Ordinance of 30 March 1995 regarding the transparency of administration, *B.S.* 23 June 1995; for the Walloon Region, see Decree of 30 March 1995 relating to the publicity of administration, *B.S.* 28 June 1995; for the French Community, see Decree of 22 December 1994 relating to the publicity of administration, *B.S.* 31 December 1994; for the German-speaking Community, see Decree of 16 October 1995 about the publicity of administration, *B.S.* 29 December

provinces were transferred from the federal level to the regions in 2001, the Flemish Decree now applies to local government. For the other regions, federal legislation is still in place.[179] Generally speaking, the regional legislation differs only in the practicalities of the requests and in the procedure of appeal.

2.6.4. The right to communicate with the Administration by electronic means

In 2005, the Secretary of State for administrative simplification offered for free 5000 machines to read the chip on electronic identity cards, with the aim of promoting e-services.[180] The Belgian government has also announced plans to give every inhabitant of Belgium a free e-mail address.[181] Every citizen will be entitled to ask for a free e-mail alias that can be used to communicate with the different governmental authorities. The Secretary of State for Government computerisation, Mr Vanvelthoven, wishes to promote government communications with this plan, while at the same time cutting costs and saving the environment. He stressed that the protection of privacy is most important, and that citizens wishing to be contacted by the government should provide an existing e-mail address to which the government then attaches an encrypted alias, thus preventing abuse of the e-mail address by third parties.[182]

The federal Council of Ministers has approved the memorandum on the use of open standards for creating and exchanging office documents.[183] The creation and exchange of office documents such as text documents and spreadsheets is currently based on different office suites like Microsoft Office, Corel WordPerfect Office, and OpenOffice. Until recently, users of one of these suites experienced difficulties in exchanging documents with users of other software. Over the past few years, however, the government has attempted a standardization effort, leading to a new standard using XML and ODF (Open Document Format). The federal Council of Ministers proposes establishing ODF as the standard for exchanging office documents such as texts, spreadsheets, and presentations within the civil service, as soon as the format is definitively approved by the International Organisation for Standardization.

2.6.5. E-voting

Voting is mandatory for people aged 18 years and older.[184] The laws regarding voting, enacted in 1919 and amended to include women in 1949, are strictly enforced. In 1991, experiments began with using electronic voting machines at polling locations. The Election Law was subsequently adapted in 1998 to allow 'automated' voting. The development towards e-voting has not raised much concern over rights, in contrast to the United States and, to a lesser degree, the Netherlands. The development is apparently not considered relevant with respect to human rights.

2.7. Conclusion

Many things have changed since the Koekkoek report of 2000. In this chapter, the following developments have been identified:

1995.

[179] Act of 12 November 1997 regarding the transparency of the administration in the communes and the provinces, *B.S.* 19 December 1997, 34253.

[180] 'Win een gratis e-id kaartlezer. Zonder kaartlezer heeft e-ID weinig nut', Brussels, 15 May 2006, http://www.staatssecretarisq.be/.

[181] 'Free e-mail address for every Belgian', http://www.edri.org/edrigram/number2.6/e-belgium. See also 'Internet for all', Federal Civil Service Information and Communication Technology (Fedict), about the 'Internet for all' campaign for raising awareness and to promote the pc and the Internet as the norm for communication, available via http://www.belgium.be/ (search for 'Internet for all').

[182] Ibid.

[183] 'Open standards: Belgium's federal Council of Ministers approves ODF (Open Document Format)', 6 July 2006, http://presscenter.org/archive/other/2648eda677208241081d4d8e02c22975/?lang=en. Further information on open standards can be found at www.belgif.be.

[184] This section draws from EPIC, loc. cit. n. 16, at 198.

- the establishment of a true constitutional court and the rediscovery of existing constitutional rights in a legal system;
- the recognition in case law of the horizontal effect of constitutional privacy rights;
- the federal system entering a more mature phase;
- a long period of a liberal-led coalition focusing on technological progress, development of the information society, and liberalization of ethical constraints (abortion, euthanasia); and
- the confrontation with technology, which has not been one in terms of digital constitutional rights, but rather one in terms of governance, money, and democracy.

Almost no new fundamental rights have been proposed or laid down in the Constitution in connection with ICT or new technologies, and there does not seem to be a broadly shared feeling that this should be done. The 2003 reform of the Constitutional Court is fundamental in this respect. In judgements such as those relating to the publication of the names of sportsmen on a public website and relating to special investigative powers, the Constitutional Court applies without hesitation existing rights to new 'digital' issues and exercises a strict proportionality test in these cases.

Also, when confronted with rights lacking in the constitutional order, the Court does not hesitate to borrow from the supranational order. Hence, we conclude that the Belgian constitutional order is transformed into one that is very similar to the European human-rights order, but without the necessity for the Constitutional Court to respect a margin of appreciation whenever there is diversity within the member states.

Chapter 3. Constitutional Rights and New Technologies in Canada

Jason M. Young*

3.1. Introduction

This chapter is intended to give a high-level overview of the Canadian constitutional framework and how it can and has evolved under tension from new information and communications technologies since 2000. As the primary means of constitutional interpretation and evolution is by the courts, the focus is on how Canada's courts have interpreted and given shape to privacy and freedom of expression rights found in the Canadian *Charter of Rights and Freedoms*. Various quasi- or non-constitutional facets of these rights are discussed as well.

3.2. History of Digital Constitutional Rights

3.2.1. Before 2000

The Canadian Constitution includes several documents dating to the *Constitution Act, 1867* and including the *Constitution Act, 1982*, also known as the *Canadian Charter of Rights and Freedoms.*[1] While the Constitution provides several methods of amendment, for political and historical reasons legislative amendment to constitutional documents is almost never done. Instead, the role of interpreting constitutional rights in modern contexts is left to the courts. Every court 'of competent jurisdiction' in Canada has the power to assess the constitutionality of federal and provincial laws and to 'read in' or 'read down' legal language to render a law constitution or strike down a law that is unconstitutional. The Supreme Court also has unique reference jurisdiction and can consider the constitutionality of laws or proposed laws at a legislatures' request.

There is no constitutional right to privacy *per se*, but Canadian courts have recognized a broad penumbra of individual privacy rights *vis à vis* the state as part of the Section 8 right to be secure against unreasonable search or seizure.[2] Additionally, Canadians enjoy comprehensive statutory privacy rights in the public and private-sector at both the federal and provincial levels.

The Supreme Court of Canada, the nation's highest, has found that Section 8 of the Charter protects 'people, not places'[3] against 'unjustified state intrusions upon their privacy.'[4] The degree of privacy protected depends on the reasonable expectations of the individual in the circumstances.[5] This test has both an objective and a subjective quality.

The Supreme Court has interpreted Section 8 to protect, at least an element, of the right to information self-determination in the case of *R.* v. *Plant* where Sopinka J. stated:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that Section 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.[6]

---

* Jason Young, LL.B., LL.M., is an associate at Deeth Williams Wall LLP in Toronto, where he practices information technology and intellectual property law, with a particular focus on privacy matters. He is grateful to articling student Andrei Edwards for his assistance. He can be reached at jyoung@dww.com.

[1] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11 [hereinafter: Charter].

[2] See *Hunter* v. *Southam*, [1984] 2 S.C.R. 145 .

[3] *Katz* v. *United States*, 389 U.S. 347 (1967), Stewart J., cited in ibid. at para. 23.

[4] *Supra* note 2 at para. 27, Dickson J.

[5] See *R.* v. *Wise*, [1992] 1 SCR 527; *R.* v. *M.* (*M.R.*), [1998] 3 SCR 393.

[6] *R.* v. *Plant*, [1993] S.C.J. No. 97, [1993] 3 S.C.R. 281 at para. 20.

Some Canadian courts have also suggested that an individual's right to privacy could be found in the broad constitutional right to 'life, liberty and security of the person' under Section 7 of the Charter, though the jurisprudence on this point is sparse.[7]

Section 2(b) of the Charter provides the freedom of thought, belief, opinion and expression to every Canadian. This also includes freedom of the press and other forms of communication. Freedom of expression is not an absolute right, but is subject to 'such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.'[8] In practice the Supreme Court has demonstrated considerable tolerance for laws that limit freedom of expression in the name of protecting minority interests, such as those prohibiting hate speech[9] and pornography.[10] Similarly, protection of reputation has sometimes prevailed over expression.[11] With respect to commercial speech, the Supreme Court has insisted upon a relatively high level of proof that legal restraints are required to achieve state objectives.[12]

3.2.2. Since 2000

Freedom of information is discussed in detail later in the chapter.

Copyright

The federal government attempted in 2005 to amend[13] the Copyright Act to ratify the WIPO Treaties. Though the amending bill did not pass, the bill included measures to strengthen Digital Rights Management (DRM), including:

- Making it an infringement to make available a copyrighted work on the Internet, where it can be downloaded on demand by members of the public;
- Making it illegal to circumvent encryption or digital rights management on copyrighted works; and
- Creating a statutory 'notice and notice' scheme whereby once Internet service providers (ISPs) are notified by copyright holders that one of their customers is infringing copyright, the ISPs are required to notify those customers they are infringing copyright, and keep information on those customers.[14]

Though it did not pass, Bill C-60 is likely to be reintroduced in the next two years and is, therefore, worth mentioning. Section 27 of the Bill contained an amendment to the Copyright Act which would prohibit removing or inactivating any 'technological measure protecting any material form of the work, the performer's performance, or the sound recording.'[15] This offence would apply to copying the work for *any* purpose, including for purposes of 'fair dealing'[16] or private copying, which is allowed under Section 80(1) of the Copyright Act.[17]

---

[7] See *Re BC Motor Vehicle Act*, [1985] 2 S.C.R. 486 at paras. 28-31; *R.* v. *Stillman*, [1997] 1 S.C.R. 607; *Thomson Newspapers Ltd.* v. *Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, 1990 S.C.J. No. 23, [1990] 1 S.C.R. 425 [*Thomson*].

[8] *Irwin Toy Ltd.* v. *Quebec (A.G.)*, [1989] 1 S.C.R. 927 describes the interpretative analysis framework to be followed in freedom of expression cases. The first stage broadly interprets 'expression', except for acts of violence. The second stage determines whether there has been a violation and, if so, whether it is a content-based restraint or one that merely has the effect of limiting expression. If the latter, the party claiming the protection of the *Charter* must be able to show that the activity in question promotes one of the three principles underlying freedom of expression: political debate, the marketplace of ideas, or autonomy and self-fulfillment. The final stage of the analysis places the burden on the state to justify the limit it seeks to impose as being reasonable in a free and democratic society.

[9] See *R. v. Keegstra*, [1990] 3 S.C.R. 697.

[10] See *R. v. Butler*, [1992] 1 S.C.R. 452.

[11] See e.g. *Hill* v. *Church of Scientology*, [1995] 2 S.C.R. 1130.

[12] See e.g. *Ford* v. *Quebec (A.G.)*, [1988] 2 S.C.R. 712.

[13] Bill C-60, *An Act to Amend the Copyright Act*, 1st Sess. 38th Parl., 2004-2005 [Bill C-60].

[14] Sam N.K. Banks, and Andrew Kitching, LEGIS Info, Library of Parliament, 'Legislative Summary, Bill C-60: An Act to Amend the Copyright Act' (20 September 2005), available at http://www.parl.gc.ca/LEGISINFO/index.asp?List=ls&Query=4527&Session=13&Language=e.

[15] *Supra* note 13 at s. 27.

[16] *Copyright Act*, R.S. 1985, c. C-42, at s. 29.

[17] Ibid.

Security versus privacy rights

The events of September 11, 2001 brought terrorism to the forefront of the legislative agenda. To enhance the ability of law enforcement to combat terrorist organizations and their supporters, the federal government passed Bill C-36, which became known as the Anti-Terrorism Act.[18] Bill C-36 included many controversial provisions, including:

- Increasing police electronic surveillance powers;
- Limiting public disclosure of information and expanding exemptions under access-to-information legislation;
- Making it easier to 'preventatively' detain individuals alleged to have knowledge of terrorism and to force them to appear before a judge to offer information under the pretense of 'investigative hearings';
- Substantially enhancing the interception capabilities and investigative powers of security services; and
- Giving the Attorney General of Canada the power to issue 'gag orders' that prohibit the disclosure of information for the purpose of protecting international relations, national defense, or security.[19]

Critics were concerned with the Bill's limited oversight applications, lack of sunset clauses, and the fact that aspects of the legislation could trump federal privacy legislation.[20] To address some of these concerns, Bill C-36 was modified before it was passed. These amendments to the draft legislation included:

- The addition of a sunset clause so that preventative arrest and investigative hearing powers would expire after five years unless the government extended them;
- Provincial ministers responsible for policing would be required to report annually to Parliament on the use of preventative arrest and investigative hearing powers;
- Provisions dealing with Attorney General certificates would be amended so that the certificate could no longer be issued at any time, but only after an order or decision for disclosure has been made in a proceeding;
- Certificates were subject to review by a Federal Court of Appeal judge;
- A new interpretive clause was added that clarified that any political, religious, or ideological beliefs would not be considered a terrorist activity unless they specifically met the definition of 'terrorist activity'.[21]

The federal government also enacted the Public Safety Act, 2002,[22] containing several measures intended to combat terrorism, which impact an individual's right to privacy, such as:

- A requirement that air carriers and reservation system operators provide detailed passenger information to law enforcement agencies without the consent of the passenger; and
- Amendments to existing federal private-sector privacy legislation to allow organizations to collect personal information without consent for the purposes of disclosing it to government, law enforcement, and national security agencies.[23]

As part of its response to the events of September 1, 2001, Canada now operates an Advance Passenger Information/Passenger Name Record (API/PNR) database, through the Canada

---

[18] 2001, c. 41.
[19] Bill C-36, *Anti-Terrorism Act*, 1st Sess., 37th Parl., 2001.
[20] See Ronald J. Daniels, Patrick Macklem, and Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto: University of Toronto Press Inc., 2001).
[21] Department of Justice Canada, 'Amendments to Bill C-36' (20 November 2001), available at http://canada.justice.gc.ca/en/news/nr/2001/doc_27902.html. In the case of *R.* v. *Khawaja*, [2006] O.J. No. 4245 the definition of 'terrorist activity' that the Anti-terrorism Act added to the Criminal Code, R.S. 1985, c. C-46 at s. 83.01(1)(b)(i) (A) was declared constitutionally invalid because it included activities performed for religious, political, or ideological causes, purposes, or objectives. The Court held that this definition of 'terrorist activity' infringed the Charter rights to freedom of religion, expression, and association respectively.
[22] 2004, c. 15.
[23] Jennifer Stoddart, Privacy Commissioner of Canada, 'Bill C-7, the Public Safety Act, 2002' (Address to the Senate Standing Committee on Transport and Communications, 18 March 2004), available at Office of the Privacy Commissioner of Canada http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp. See also Privacy Commissioner of Canada, 'Annual Report to Parliament, 2003-2004' (2004), available at Office of the Privacy Commissioner of Canada http://www.privcom.gc.ca/information/ar/200304/200304_e.asp#foreword.

Border Services Agency (CBSA). Personal information about all airline passengers arriving in Canada is collected and stored in this database, and is used in special Canada-US border-crossing programs to allow pre-approved low-risk travelers and commercial shipments to move back and forth between the two countries.

CBSA phased in the requirement to provide PNR data relating to persons onboard flights bound for Canada between March 2003 and September 2004, and from February 2005 introduced a system of monetary penalties for non-compliance. As of July 2005, airlines will face potential sanctions for non-compliance. However, the penalties were suspended for European airlines during the negotiation of the EU-Canada API/PNR agreement on the use of personal data provided by airlines to the border authorities of Canada.

This agreement, which entered into force on March 22, 2006,[24] provides that airlines flying from an EU Member state to Canada will have to transfer selected passenger data to the Canadian authorities to help identify passengers who could be a security, and in particular, a terrorist threat.[25]

Canada also signed the European Convention on Cybercrime,[26] and amended the federal Criminal Code[27] to include provisions for new production and preservation orders allow law enforcement authorities to compel persons (i.e., an Internet service provider) to produce personal information in their custody or control about an individual the police had a 'reasonable ground to suspect' had committed a crime.[28]

In the face of these changes, many Canadians have pondered if the government's pursuit of terrorist threats has eroded the constitutional rights that underlie Canadian democracy. In *Suresh* v. *Canada (Minister of Citizenship and Immigration)*,[29] the Supreme Court, in *obiter*, confronted the challenge facing democratic societies today:

> On the one hand stands the manifest evil of terrorism and the random and arbitrary taking of innocent lives, rippling out in an ever-widening spiral of loss and fear. Governments, expressing the will of the governed, need the legal tools to effectively meet this challenge.
>
> On the other hand stands the need to ensure that those legal tools do not undermine values that are fundamental to our democratic society – liberty, the rule of law, and the principles of fundamental justice - values that lie at the heart of the Canadian constitutional order and the international instruments that Canada has signed. In the end, it would be a Pyrrhic victory if terrorism were defeated at the cost of sacrificing our commitment to those values. Parliament's challenge is to draft laws that effectively combat terrorism and conform to the requirements of our Constitution and our international commitments.[30]

In the face of increasing surveillance powers for law enforcement and national security agencies, many have emphasized the need for increased judicial and legislative transparency. As the balance between liberty and security becomes ever more challenging to maintain, this issue will continue to be at the center of Canadian debates about constitutional rights in the digital age.

3.3. Changes in the Constitutional System

Canada is a federal state, meaning that legislative powers are distributed between the federal government and the provincial governments: each 'equal and coordinate' in their own sphere of

[24] EC, *Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record Data*, [2006] O.J. L. 86/49 at 19, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_086/l_08620060324en00190019.pdf.
[25] EC, *Council Decision 2006/230 of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of API/PNR data*, [2006] O.J. L. 82/49 at 14, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_082/l_08220060321en00140014.pdf; EC, *Agreement between the European Community and the Government of Canada on the processing of API/PNR data*, [2006] O.J. L. 82/49 at 15, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_082/l_08220060321en00150019.pdf.
[26] Council of Europe, Convention on Cybercrime, CETS No.: 185 (23 November 2001), available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
[27] R.S., 1985, c. C-46.
[28] Ibid. at ss. 487.012, 487.013.
[29] [2002] 1 S.C.R. 3, 2002 SCC 1.
[30] Ibid. at paras. 3-4.

jurisdiction under the Constitution. This arrangement entails the supremacy of a written constitution.[31] It also means that the provisions governing the distribution of powers must be couched in general terms, which can never possibly be free from doubt or ambiguity. Not surprisingly, Canadian courts play an important role in settling disputes.

Judicial interpretation of Canada's constitution has been shaped by a 'living tree' doctrine first articulated in *Re Section 24 of the B.N.A. Act*.[32] In this landmark 1930 judgment, Lord Sankey L.C. of the Judicial Committee of the Privy Council, then Canada's highest court, stated that the constitution had to be given 'a large and liberal interpretation'[33] so that it could be adapted to fit changing social conditions. Canadian courts continue to refer to the 'living tree' doctrine when interpreting constitutional rights in modern contexts.

Though Canada's Constitution contains five different amending formula,[34] these require a high level of agreement between the provinces and federal government which, for historical and political reasons, has proved impractical. Consequently, legislative amendments to the Constitution are exceedingly rare.

3.4. Privacy-related Rights

3.4.1. Privacy and data protection

In *Hunter* v. *Southam Inc*.[35] the Supreme Court held that a reasonable expectation of privacy lies at the core of the right to be secure against unreasonable search or seizure guaranteed by Section 8 of the Charter. The scope of this guarantee is 'a broad and general right to be secure from unreasonable search where the person who is the object of the search has a reasonable expectation of privacy.'[36]

This qualification of reasonableness shows that an assessment must be made which balances the individual's reasonable expectation of privacy against the state's security interests:

> The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by Section 8, whether it is expressed negatively as freedom from 'unreasonable' search and seizure, or positively as an entitlement to a 'reasonable' expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by the government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.[37]

The Supreme Court has identified several criteria which must be met if a search is considered to be reasonable. In a criminal law context, the Court has stipulated three conditions:

1. a search warrant or other authorization must be obtained prior to the search;
2. the warrant must be issued by a judicial officer who is not actively involved in the ongoing investigation (i.e. she must be independent); and
3. the warrant must be issued only on reasonable and probable grounds to believe that an offence has been committed and evidence for that offence will be found in the location to be searched.[38]

However, in the case of a warrantless search, *Hunter* v. *Southam* established that there will be a presumption of unreasonableness and the onus is on the Crown to 'rebut this presumption'[39] In

---

[31] The Judicial Committee of the Privy Council adopted a rationale similar to that in the US case of *Marbury* v. *Madison* to justify to assume the right to judicially review legislation, although the rationale was based more on imperialism than on constitutionalism, as the BNA Act was an imperial statute, see Peter H. Russell, *The Judiciary in Canada* (Toronto, ON: McGraw-Hill Ryerson, 1987).
[32] [1930] 1 D.L.R. 98.
[33] Ibid.
[34] Part V of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11, s. 38(1).
[35] *Supra* note 2.
[36] *R.* v. *Wise*, [1992] 1 S.C.R. 527 *per* Cory J.
[37] *Supra* note 2 at para. 25, Dickson J.
[38] *Supra* note 2; See also Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham, ON, Lexis Nexis Canada Inc., 2005) at p. 114.
[39] *Supra* note 2 at para. 30, *per* Dickson J.

the later Supreme Court case of *R.* v. *Collins*,[40] Lamer J. expounded on these three criteria by finding that 'a search will be reasonable if it is authorized by law, if the law itself is reasonable and if the manner in which the search was carried out is reasonable.'[41]

The criteria to establish a reasonable search in *Hunter* were within the context of a criminal investigation. Prior authorization for a search may not be feasible or even warranted in all situations. In *Thomson Newspapers Ltd.* v. *Canada (Director of investigation and research, restrictive trade practices commission)*[42] Wilson J. explained that the nature and extent of the constitutional requirements for establishing the reasonableness of a search requires analyzing the *context* of the search:

> [T]hese [Hunter] criteria are not hard and fast rules which must be adhered to in all cases under all forms of legislation. What may be reasonable in the regulatory or civil context may not be reasonable in a criminal or quasi-criminal context. What is important is not so much that the strict criteria be mechanically applied in every case but that the legislation responds in a meaningful way to the concerns identified (…) in *Hunter*.[43]

Therefore, not all searches will require the full application of the *Hunter* criteria. When the state is not enforcing a criminal or quasi-criminal statute, the absence of a prior judicial authorization for a search will not render that search invalid.[44] However, the legal instrument that enables the search must set out a framework that will be constitutionally sufficient to uphold the individual's right not to be deprived of his Section 8 right to be secure against an unreasonable search or seizure.[45]

The appropriation of information from a computer by state agents may constitute a search or seizure under Section 8 of the Charter, because this right is broad enough to 'embrace all existing means by which the agencies of the state can electronically intrude on the privacy of the individual, and any means which technology places at the disposal of law enforcement authorities in the future.'[46] Section 8 is supported, in this context, by the Section 7 Charter right to 'security of the person', because both of these provisions focus on protecting individuals' legitimate expectations of privacy.[47]

The act of state agents accessing personal information held by the government in its own files or computer databases could also attract Charter scrutiny. Section 7 has a residual capacity to protect privacy rights, which the courts have interpreted to include an element of privacy that is either incidental to personal security,[48] or an aspect of personal liberty.[49] Therefore, any information that is retained by government officials must be subject to certain safeguards. As the Supreme Court found in *R.* v. *Duarte*:[50]

> the regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.
>
> The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance.

The Supreme Court of Canada has developed criteria that must be considered when examining the 'totality of the circumstances' surrounding whether or not a reasonable expectation of privacy exists regarding acquired and stored information.[51] These criteria include:

---

[40] [1987] S.C.J. No. 15, [1987] 1 S.C.R. 265.
[41] Ibid. at para. 23.
[42] [1990] 1 S.C.R. 425.
[43] Ibid.
[44] Cohen op. cit. n. 38, at p. 116.
[45] Ibid.
[46] *R.* v. *Wong*, [1990] 3 S.C.R. 36, *per* La Forest J.
[47] *Supra* note 2; *R.* v. *Mills*, [1999] S.C.J. No. 68, [1999] 3 S.C.R. 668.
[48] *R.* v. *Stillman*, [1997] S.C.J. No. 34, [1997] 1 S.C.R. 607, cited in Cohen op. cit. n. 38, at p. 417.
[49] *R.* v. *O'Connor*, [1995] S.C.J. No. 98, [1995] 4 S.C.R. 411; *B. (R.)* v. *Children's Aid Society of Metropolitan Toronto*, [1994] S.C.J. No. 24, [1995] 1 S.C.R. 315; *R.* v. *Beare*, [1988] 2 S.C.R. 387; *R.* v. *Higgins*, [1987] S.C.J. No. 92, [1988] 2 S.C.R. 387; See also *Ruby* v. *Canada (Solicitor General)*, [2002] S.C.J. No. 73, [2002] 4 S.C.R. 3, cited in Cohen op. cit. n. 38, at p. 417.
[50] [1990] S.C.J. No. 2, [1990] 1 S.C.R. 30.
[51] Ibid. at p. 418.

1. the nature of the information itself;
2. the relationship between the party releasing the information and the party claiming its confidentiality;
3. the place where the information was obtained;
4. the manner in which it was obtained;
5. existence of a subjective expectation of privacy;
6. the objective reasonableness of the expectation; and
7. the purpose for which the information is obtained.[52]

If we apply these criteria to computer information, it is the nature of the information that proves to be the most determinative factor in establishing a reasonable expectation of privacy.[53] For example, Canadian courts have found that business records have a reduced expectation of privacy than records containing personal information, because business records tend to contain information required to be collected for a regulatory purpose or alternatively contain little information of a personal nature.[54] Information that does not reveal significant details about the lifestyle and personal choices of the individual carries little or no expectation of privacy, because it falls outside of the so-called 'biographical core' of personal information that courts have found is protected by the constitution.[55]

An individual's name by itself may not be regarded as personal or private information, even if it is part of a commercial databank containing subscriber information.[56] But the combination of a name and other information can elicit a higher expectation of privacy. Neutral datum, when combined, can reveal the type of information that lies at the protected biographical core described in *Plant*.

In *R.* v. *Eddy*,[57] the Supreme Court found that the state must seek prior judicial authorization before gathering seemingly innocuous, but cumulatively personal, privately held pieces of information.[58] In that case, a police search of a vehicle led to the discovery of a bankbook with an account number, branch location, and account transactions. The police called the bank to find out the name of the bankbook owner. In finding that a simple name attracted a greater expetation of privacy in this context, the Newfoundland Supreme Court Trial Division noted the inherent sensitivity of personal financial information.

> [T]here is a substantially greater expectation of privacy relating to the records of an individual's personal financial position, and the pattern of the individual's operating on his or her bank account, then with respect to electricity consumption records [referring to *R.* v. *Plant*].[59] I note that the Crown argues that the police in this case already had access to the bank book itself and the account number, and that therefore the only 'new' information they were abstracting in this connection was the name of the owner. However, in my view that does not lessen the privacy interest protected. It is one thing to have an unidentified bank book containing records of deposits and withdrawals and revealing financial information, when it is not linked to a name. The linkage of a name to that information creates at once the intimate relationship between that information and the particular individual, which is the essence of the privacy interest. I do not accept the Crown's suggestion that the mere obtaining of the name of the owner of an account about which information is already available is not deserving of protection under Section 8.[60]

This finding does not preclude the government from using techniques such as data-matching to link disparate pieces of information in their custody or control to further investigations and develop intelligence gathering.[61] In *Smith v. Canada*[62] the court considered the practice of Canada

---

[52] See *R.* v. *Plant*, [1993] S.C.J. No. 97, [1993] 3 S.C.R. 281 at 293; *R.* v. *Edwards*, [1996] S.C.J. No. 11, [1996] 1 S.C.R. 128 at para. 45; *Schreiber v. Canada (Attorney General)*, [1998] S.C.J. No. 42, [1998] 1 S.C.R. 841, cited in Cohen op. cit. n. 38 at p. 418.
[53] Cohen op. cit. n. 38 at p. 418.
[54] *Thomson, supra* note 7 at 517-518, cited in ibid.
[55] *Supra* note 6 at para. 20.
[56] See e.g., *R.* v. *Solomon*, [1996] A.Q. No. 2131, 110 C.C.C. (3d) 354 (C.A.); *R.* v. *Brown*, [2000] O.J. No. 1177, 2000 W.C.B.J. LEXIS 10405, 46 W.C.B. (2d) 53 (S.C.J.); *R.* v. *Hutchings*, [1996] BCJ. No. 3060, 111 C.C.C. (3d) 215 (C.A.); *R.* v. *Edwards*, [1999] O.J. No. 3819, 44 W.C.B. (2d) 45 (S.C.J.), cited in Cohen op. cit. n. 38 at p. 419.
[57] [1994] N.J. No. 142, 119 Nfld. & P.E.I.R. 91 (S.C.T.D.).
[58] Cohen, op. cit. n. 38, at p. 420.
[59] See note 53.
[60] *Supra* note 57 at para. 175, Puddester, J.
[61] Cohen, op. cit. n. 38, at p. 420-421.

Customs sharing information on customs declaration forms with Human Resources Development Canada (HRDC), the federal agency responsible with administering employment insurance benefits. HRDC sought to obtain information about employment insurance recipients who were absent from Canada because it was concerned that employment insurance recipients were continuing to receive insurance payments during their absences from Canada, thereby violating the Employment Insurance Act.[63] The customs declaration form includes information such as a person's name, date of birth, address, postal code, date of departure from Canada, mode of arrival into Canada, country of departure, etc.[64] Ms. Smith, an employment insurance recipient claimed that this data-matching practice violated her Section 8 Charter right to be free from unreasonable search and seizure. Considering the nature of the information on the customs declaration form, the relationship between Ms. Smith and other returning Canadian residents and Canada Customs, the place and manner in which the relevant information was disclosed, and the seriousness of the alleged offence,[65] the Umpire found in favour of the government of Canada, stating:

> Canadian residents returning to Canada by air (…) cannot be said to have held a reasonable expectation of privacy in relation to information found on their [customs declaration form] information disclosed to the [Canada Employment Insurance] Commission, which outweighs the government's interest in enforcing the laws disentitling unemployment insurance claimants from receiving benefits while outside Canada. The disclosure of E-311 information in this case is not in violation of section 8 of the Charter.[66]

Umpire Rothstein J.'s decision was upheld by the Federal Court of Appeal, and the Supreme Court of Canada.

3.4.2. Inviolability of the home

Section 8 of the Charter also protects the privacy of a person's home against intrusions by the state. As in other contexts, these rights are subject to a court finding that a reasonable expectation of privacy exists.

Two Supreme Court cases, *R.* v. *Plant*, and *R.* v. *Tessling*[67] found that some information gleaned from the home cannot be considered to attract a reasonable expectation of privacy. In *R.* v. *Plant*,[68] police suspected that the defendant's home was being used to illegally grow marijuana and requested computerized records from the local electricity utility in order to assess electricity consumption. On this information, police officers conducted a warrantless perimeter search of the home and subsequently sought a warrant to search the home itself. The Supreme Court upheld the constitutionality of the initial request for information from the utility, on the grounds that the information produced did not 'reveal intimate details of the lifestyle and personal choices of the individual' and so was not subject to a reasonable expectation of privacy. The Court's approach in *Plant* gives valuable insight to when and how a court might find a reasonable expectation of privacy in information produced by new information and communications technologies:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that Section 8 of the *Charter* should seek to protect a *biographical core* of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar, while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence.

Despite finding that the records in *Plant* did not attract a reasonable expectation of privacy, the Supreme Court clearly anticipated that more sophisticated or invasive technologies could attract

---

[62] [2001] S.C.J. No. 85, [2001] 3 S.C.R. 902, affirming [2000] F.C.J. No. 174, 252 N.R. 172 (C.A.), affirming CUB-44824
[63] S.C. 1996, c. 23, s. 37(b).
[64] Cohen, op. cit. n. 38, at p. 421.
[65] Ibid.
[66] CUB-44824 at para. 136, Rothstein J., cited in Cohen, op. cit. n. 38 at p. 422.
[67] [2004] 3 SCR 432, 2004 SCC 67.
[68] [1993] S.C.J. No. 97, [1993] 3 S.C.R. 281.

critical scrutiny under the Charter. The Court also found that while commercial records often did not attract Charter protection, a commercial relationship did not preclude a reasonable expectation of privacy.

> The nature of the relationship between the appellant and the [electrical utility] cannot be characterized as a relationship of confidence. The [utility] prepared the records as part of an ongoing commercial relationship and there is no evidence that it was contractually bound to keep them confidential. This is not to suggest that records prepared in a commercial context can never be subject to the privacy protection afforded by Section 8 of the *Charter*. If commercial records contain material which meets the 'personal and confidential' standard set out above, the commercial nature of the relationship between the parties will not necessarily foreclose a Section 8 claim.[69]

In *R.* v. *Tessling*, the Supreme Court found that the use of aerial infrared cameras by the police to scan a home for abnormal patterns of heat emissions (a sign that the house might be used for an illegal marijuana growing operation) was not an unreasonable search of the home, because forward looking infrared (FLIR) technology cannot, in its present state of development, permit any inferences about the precise activity giving rise to the heat. The accused had a privacy interest in the activities taking place in his home, but the FLIR records contained only information already exposed to the public and did not expose any intimate details of the accused's lifestyle or his core biographical data. In the totality of circumstances, the accused did not have an objective reasonable expectation of privacy in the heat distribution.

However, as in *Plant*, the Court cautioned that technology was a moving target and the determination of whether the use of a new technology did infringe Charter rights must be a fact-based one.

> [T]echnology must be evaluated according to its current capability, and its evolution in future dealt with step by step. Concerns should be addressed as they truly arise. FLIR technology at this stage of its development is both non-intrusive in its operations and mundane in the data it is capable of producing. The taking of a FLIR image therefore did not violate the respondent's reasonable expectation of privacy within the scope of s. 8 of the *Charter*.[70]

3.4.3. Inviolability of the body

Canadian courts have consistently protected an individual's physical integrity from unreasonable search and seizure,[71] which is not surprising given the subjective expectation of privacy that we each have in our bodies. In several landmark decisions, the Supreme Court has made it clear that the constitutional protection extended to one's physical integrity is unparalleled.[72] In *R. v. Dyment*, the Supreme Court held that the warrantless seizure of a blood sample from a physician treating a suspect amounted to a violation of the high expectation of privacy that one has in their person.

In 1998, the federal government passed the DNA Identification Act[73] which established a national DNA databank operated by the Royal Canadian Mounted Police (RCMP). Under the DNA Identification Act, the DNA databank consists of an index of DNA profiles collected at certain types of crime scenes, and an index of DNA profiles of offenders convicted of violent or sexually-based crimes.[74]

When it comes to taking DNA samples of suspects, the Criminal Code[75] contains provisions which allow provincial court judges to issue warrants that permit police officers to obtain DNA samples by:

a) plucking of individual hairs from the person, including the root sheath;

---

[69] Ibid. at paras. 20, 21, *per* Sopinka J.
[70] *Supra* note 67 at para. 55.
[71] See *R.* v. *Soldat*, [1995] N.W.T.R. 349 (S.C.); *R.* v. *Legere* (1988), 43 C.C.C. (3d) 502 (N.B.C.A.) and *R.* v. *S. (C.)* (1997), 13 C.R. (5th) 375 (Ont. Prov. Div.).
[72] *R.* v. *Pohoretsky*, [1987] 1 S.C.R. 945, a violation of the sanctity of a person's body is much more serious than that of his office or even his home; *R. v. Colarusso*, [1994] 1 S.C.R. 20, '[t]hat physical integrity, including bodily fluids, ranks high among the matters receiving constitutional protection, there is no doubt.'
[73] 1998, c. 37.
[74] Ibid. at s. 5; The types of crimes and crime scenes which meet the requirement for DNA collection and storage in the national DNA databank are listed in s. 487.04 of the Criminal Code, R.S. 1985, c. C-46, and s. 196.11 of the National Defence Act, R.S., c. N-4.
[75] R.S. 1985, c. C-46.

b) taking of buccal swabs by swabbing the lips, tongue and inside cheeks of the mouth to collect epithelial cells; or
c) taking of blood by pricking the skin surface with a sterile lancet.[76]

A judge can issue a DNA warrant if they have reasonable grounds to believe:
a) that a designated offence [listed in s. 487.04 of the Criminal Code] has been committed, and;
b) that a bodily substance has been found or obtained
    a. at the place where the offence was committed,
    b. on or within the body of the victim of the offence,
    c. on anything worn or carried by the victim at the time when the offence was committed, or
    d. on or within the body of any person or thing or at any place associated with the commission of the offence,
c) that a person was a party to the offence, and
d) that forensic DNA analysis of a bodily substance from the person will provide evidence about whether the bodily substance referred to in paragraph (b) was from that person.[77]

The judge must also be satisfied that it is in the best interests of justice to issue such a warrant.[78] Collected DNA samples may only be used in the investigation of the alleged offence. The DNA sample and its corresponding record are destroyed if the DNA sample excludes the suspect from the investigation, the suspect is acquitted of the offence, or one year expires after the person is discharged from a preliminary hearing, the information is withdrawn or dismissed, or a stay of charges is granted.[79]

The constitutionality of the DNA warrant scheme was challenged in the Supreme Court case of *R.* v. *S.A.B.*[80] In upholding the constitutionality of these warrants, the Court acknowledged that the taking of bodily samples can significantly intrude on an individual's privacy and human dignity, but found that the legislative protections were constitutionally sufficient:[81]

> [U]nder a properly issued DNA warrant, the degree of offence to the physical integrity of the person is relatively modest. (…) [Therefore, in] my view, the *statutory framework* alleviates any concern that the collection of DNA samples pursuant to a search warrant under ss. 487.04 to 487.09 of the *Criminal Code* constitutes an intolerable affront to the physical integrity of the person.[82]

As for the potential of DNA warrants to unreasonably intrude upon personal information, the Court noted that while bodily samples can reveal intimate personal details about an individual, forensic DNA analysis examines only the non-coding regions of DNA, thereby not revealing an individual's medical, physical, or mental characteristics.[83] Since the forensic analysis involves only comparing the DNA sample obtained from an individual to that DNA found at a crime scene, Arbour J. found that obtaining a sample of an individual's DNA for the limited purpose set out in DNA warrants is reasonable under Section 8 of the Charter.[84]

3.5. Communication-related Rights

3.5.1. Secrecy of communications

General

The Criminal Code[85] requires that a police officer seek judicial authorization before she intercepts a private communication,[86] except in certain extraordinary cases.[87] Under normal circumstances,

[76] Ibid. at s. 487.06(1).
[77] Ibid. at s. 487.05(1).
[78] Ibid.
[79] Ibid. at s. 487.09(1).
[80] [2003] S.C.J. No. 61, 2003 SCC 60.
[81] Ibid. at para. 40.
[82] Ibid. at paras. 44, 47, Arbour J.
[83] Ibid. at para. 49.
[84] Ibid. at paras. 48, 49, 61.
[85] R.S. 1985, c. C-46.

judicial authorization may only be granted for the interception of a private communication if the authorizing judge is satisfied that

> [o]ther investigative procedures have been tried and have failed, [other investigative procedures] are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.[88]

In *R.* v. *Araujo*,[89] which dealt with whether a judge's authorization to intercept was constitutionally valid, the Supreme Court further underlined the conditions precedent:

> [The] interception of private communications is a serious matter, to be considered only for the investigation of serious offences, in the presence of probable grounds, and with a serious testing of the need for electronic interception in the context of the particular investigation and its objects (…). There must be, practically speaking, no other reasonable alternative method of investigation, in the circumstances of the particular criminal inquiry.[90]

While the law on wiretapping telephones is well-established, the law on the interception of e-mails is yet inchoate. There is uncertainty among law enforcement officials as to the type of investigative order required to obtain e-mails. Frequently, the order used depends solely on the stage of e-mail transmission.[91] For example, law enforcement often uses intercept orders for in-transit e-mails, and search warrants for e-mails stored in e-mail inboxes. The Federal Department of Justice is currently exploring amendments to the Criminal Code to harmonize the privacy interests in e-mail so that the test for interception of email would be uniform regardless of the mode of transmission.

In *R.* v. *Weir*[92] an Alberta trial court found that e-mails are subject to a reasonable expectation of privacy and are thereby subject to Charter protection against unreasonable search and seizure.[93] However, the Court found that e-mail is subject to a lower expectation of privacy than first class (letter) mail, because unencrypted e-mails are vulnerable to being read by unintended intermediaries.[94]

The Court in *R.* v. *Weir* drew an analogy between e-mails and first class letters to illustrate which aspects of an e-mail carry a reduced expectation of privacy. P. Smith J. described this analogy as follows:

> The envelope on first class mail shields the contents of the message. The information on the cover carries a lower expectation of privacy than does the message inside.
>
> In the e-mail environment, the headers (hidden and exposed) can be likened to the information on the envelope. The message is directed by its headers. Much repair work to e-mail can be done through headers. Like the outside of the envelope, the headers have a lower expectation of privacy.
>
> The difference between the two types of cover is that in first class mail the cover is respected. In e-mail, the cover is (or was in June of 1996) routinely violated in order to repair the technology. There are two or three levels of violation depending on the type of repair done and excluding a repair done by deleting the message or by enlarging the e-mail box. The size of the attachments may be viewed. The list of attachment names may be viewed. The message itself may be opened which can include looking at the message and the attachments or either. These facts about the technology help me to conclude the e-mail message is unlike first class mail in the level of privacy that it can attract.

---

[86] Ibid. at s. 186.
[87] Ibid. at s. 184.1(1) which allows interception without judicial authorization if a party to the communication consents to the interception, the officer believes on reasonable grounds that the there is a risk of bodily harm to the consenting party and the interception is for the purpose of preventing that harm.
[88] Ibid. at s. 186(1)(b); S. 186(1.1) provides an exception to this provision, whereby a judge may issue warrants to intercept private communications involving criminal organizations or terrorism offences without this condition being satisfied.
[89] [2000] 2 S.C.R. 992, 2000 SCC 65.
[90] Ibid. at para. 29, LeBel J.
[91] Department of Justice Canada, 'Emails: Considerations for Criminal Law Policy' (March 2005), available at http://www.cippic.ca/en/projects-cases/lawful-access.
[92] [1998] A.J. No. 155, 1998 ABQB 56, aff'd [2001] A.J. No. 869, 2001 ABCA 181.
[93] Ibid. at para. 77.
[94] Ibid.

> Another difference between e-mail and first class mail is that in order to make an e-mail message truly private, one can encrypt it.[95]

Lawful Access Initiative

In 2001, Canada signed the European Convention on Cybercrime.[96] The objectives of the Convention are as follows:

1. to harmonize the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime;
2. to provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system; and
3. to create an efficient and effective regime of international cooperation.

In August 2002, the federal government launched a review to assess what legislative amendments would be required in order to ratify the treaty.[97] Among other things, the review[98] called for telecommunications service providers (TSPs) to have the capability to intercept communications on their networks, and allow warrantless access by police to 'subscriber data' (e.g., name, IP address, telephone number, e-mail address) on request.[99]

Arguably, the most contentious aspect of the Convention is that which would require signatories to adopt 'production orders' to compel individuals or service providers to produce, respectively, 'specified computer data' or 'subscriber information' in their possession or under their control.[100] Consequently, the review proposed enacting general production orders which would require information holders to deliver or make available requested information within a certain period of time, and specific production orders for traffic data and Internet subscriber and/or service provider data respectively.[101] The specific 'traffic data' production orders would be issued under a lower threshold than that now required for a search warrant or authorization to intercept because, as the federal government argued:

> the standard for Internet traffic data should be more in line with that required for telephone records and dial number recorders in light of the lower expectation of privacy in a tele-phone number or Internet address, as opposed to the content of a communication.[102]

The review also proposed that specific production orders for Internet subscriber and/or service provider data be issued under a lower threshold than that required for a search warrant or authorization to intercept because this information has historically been made available by service providers without a prior judicial authorization.[103]

The federal government further argued that a reduced threshold for production orders would be appropriate because production orders are less intrusive than search warrants.[104]

These proposals are not yet law. If passed, it could be years before such considerations come before the courts. However, the foundations on which the government has argued that new legal standards for surveillance are appropriate remains constitutionally suspect for a number of reasons.

First, it overemphasizes the purely physical aspect of a search and seizure at the expense of the impact on the individual to whom the search was targeted and the seized information pertained. In *R. v. Edwards*,[105] the Supreme Court held that an interpretation of the degree of intrusiveness is not a matter of where the information in question is located, but to what extent

---

[95] Ibid. at paras. 72-75.
[96] Council of Europe, Convention on Cybercrime, CETS No.: 185 (23 November 2001), available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
[97] Cohen, op. cit. n. 38 at p. 522.
[98] Department of Justice, Industry Canada, Solicitor General Canada, 'Lawful Access – Consultation Document' (25 August 2002), available at http://www.justice.gc.ca/en/cons/la_al/law_access.pdf.
[99] Ibid.
[100] *Supra* note 96 at art. 18.
[101] *Supra* note 98 at p. 10.
[102] Ibid. at p. 11-12.
[103] Ibid. at p. 12.
[104] Ibid. at p. 11.
[105] [1996] 1 S.C.R. 128.

disclosure of that information would impact the reasonable expectation of the individual's privacy.[106] It is a well-established principle – and one which is reflected in the court's analysis in *R. v. Plant* despite the passage above – that Section 8 of the Charter protects 'people, not places or things'.[107] In *R. v. O'Connor*,[108] Cory J. said:

> [W]hen a private document or record is revealed and the reasonable expectation of privacy therein is thereby displaced, the invasion is not with respect to the particular document or record in question. Rather, it is an invasion of the dignity and self-worth of the individual, who enjoys the right to privacy as an essential aspect of his or her liberty in a free and democratic society.[109]

Second, the argument assumes that the third party search would be more reasonable *because* it is less intrusive. Clearly, there will be situations in which a third party search is not less intrusive and perhaps unreasonable by that aspect. The American case of *United States* v. *Bach*[110] provides a fitting example of this situation. According to intervenor Yahoo!, ISP technicians do not selectively choose or review the contents of the named account, they simply hand over the entire contents in response to a subpoena.[111] This can hardly be seen as less intrusive, given that if the search had been conducted by law enforcement, the execution would be restricted to the terms of the warrant. Unfortunately, the court declined to find on this point.

Third, the government argument ignores the capacity of new technologies and new public-private relationships to draw public inferences of private activities such that the location of the search becomes irrelevant in factoring the severity of the intrusion, something the Supreme Court in *Tessling* clearly warned against.

Fourth, the assertion that a search of a third party data custodian would be 'less invasive' of the data subject's privacy than one of the subject him or herself, also ignores the question of the availability of remedial measures intrinsic to any determination of invasiveness. That is, if a third party stands in place of the subject as the object of unreasonable surveillance, do they have equal standing in law to advance such a claim against the government? Third party intermediaries would not have standing under Section 24 of the Charter for infringements of subscribers' privacy, which reads:

> *Anyone whose rights or freedoms*, as guaranteed by this Charter, *have been infringed or denied* may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.[112]

The contours of a Charter remedy do much to govern the shape of the protected right, a factor the Supreme Court recognized in *R.* v. *Rahey* when it stated that:

> The question of breach must, therefore, be assessed in terms of the interests protected by the section and such remedy as the court can provide to secure them.[113]

An individual would have no knowledge of a search of personal information held by a third party and therefore no ability to challenge the reasonableness of a search. Current search and seizure law requires notification of the subject of a search or interception after the fact,[114] it would seem at least a partial solution to require that any production order standard incorporate the same requirement.

In claiming that a third party search would be 'less invasive,' the government seeks to foist responsibility for seeking remedies for Section 8 breaches on third parties with no standing under Section 24(1) to enforce them. In *R. v. Thompson*,[115] The Court was careful to point out that the

---

[106] Ibid.; See also *Del Zotto* v. *Canada (Minister of Nat'l Revenue)*, [1997] 147 D.L.R. (4th) 457.
[107] See *R.* v. *Colarusso*, [1994] 1 S.C.R. 20, 60 (*per* La Forest J.); See also *R.* v. *Plant*, [1993] S.C.J. No. 97, [1993] 3 S.C.R. 281 at 291; *Hunter* v. *Southam*, [1984] 2 S.C.R. 145, at 158, citing *Katz* v. *United States*, 389 U.S. 347 (1967); and *R.* v. *Dyment*, [1988] 2 S.C.R. 417, 428-29.
[108] [1995] 4 S.C.R. 411.
[109] Ibid. at para. 119, Cory J.
[110] 310 F.3d 1063, 1067 (8th Cir. 2002).
[111] Ibid. at 1065.
[112] *Charter*, *supra* note 1, s. 24(1). Emphasis added.
[113] [1987] 1 S.C.R. 588, at para. 111 [*Rahey*].
[114] *Supra* note 75 at s. 189 (5) (notice of intention to produce evidence), s. 196 (notification required after interception), s. 487.01(5.1) (notice required after covert entry).
[115] [1990] 2 S.C.R. 1111, at 1143-1144.

invasion of third-party privacy rights is not determinative of the reasonableness of the search. That is to say, an abrogation of third party privacy rights in the execution of a warrant would rarely factor into a Section 8 challenge. A plain reading of Section 24(1) would not grant standing to third parties in such cases.

The Court in *Rahey* interpreted Section 24(1) as providing application for remedy only to a person whose rights under the Charter have been infringed.[116] This would necessarily exclude third party standing, even were telecommunications and Internet service providers so inclined to act as guardians of their subscribers' privacy rights.[117]

Section 24(1) is not an exclusive remedy for breach of the Charter.[118] Nor is it necessary for an applicant to argue anything more than a breach of his or her Section 8 rights to invoke a remedy under Section 24(1) or Section 52(1). Any court seized of the dispute has the power and the duty to determine the validity of the statute.[119] However, it seems clear that a Section 52(1) remedy is narrower than the range granted under Section 24(1). Thus, severance of the Section 24(1) remedy or range of remedies for lack of standing is significant, particularly in the context of proposed routinized surveillance of subscribers by intermediaries acting as 'agents of the state'.[120]

Telecommunications and Internet service providers will be the first line of defence against unreasonable electronic surveillance, particularly under any scheme of diluted judicial oversight. Providers are by default the guardians of informational privacy on the Internet. By offering online services, providers gain access to personal and private information of their many users. Individuals are therefore dependent on those who provide them with online services to keep their private communications secure and confidential.[121]

Presented with narrow constitutional redress, intermediaries will be less inclined to resist unreasonable investigatory demands by law enforcement, even in circumstances when they feel that such demands are unreasonable.

The Lawful Access initiative is still in its development stages, yet the brief discussion here illustrates that its proposals raise substantial challenges to current interpretations of Section 8 of the Charter and will provoke further discussion for the foreseeable future.

3.5.2. Freedom of Expression

Section 2(b) of the Charter provides the freedom of thought, belief, opinion and expression to every Canadian. This also includes freedom of the press and other forms of communication. Freedom of expression is not an absolute right, but is subject to 'such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.'[122] The

---

[116] [1987] 1 S.C.R. 588, at para. 61.

[117] Canadian Internet service providers have taken some steps to protect the privacy of their subscribers, but it is not unequivocal. See Canadian Association of Internet Providers, 'Code of Conduct' (2000), available at http://www.cata.ca/_pvwc8ae40/communities/caip/codeofconduct/codeconduct.html (Article 4 stating 'Private information will be disclosed to law enforcement authorities only as required by law') (last visited 24 November 2006); Canadian Association of Internet Providers, 'Privacy Code' (2000), available at http://www.cata.ca/communities/caip/codeofconduct/privacycode.html (Article 5 stating that member ISPs 'will use or disclose personal information only for the purposes it was collected, unless a user gives consent or as required by law') (last visited 23 November 2006). However, the explanatory note somewhat ambiguously expands on the point with the statement that members 'may disclose personal information without consent when required to do so by law, *e.g.,*, subpoenas, search warrants, other court and government orders, or demands from other parties who have a legal right to personal information, or to protect the security and integrity of its network or system.' See also Jay Thompson, 'Liability for On-Line Activity: The Buck Stops Where?' (unpublished paper presented to the IT-CAN Conference, 3 October 2002) (President of the Canadian Association of Internet Providers explaining that in the event of a third-party complaint about content, a member would 'then typically advise the complainant to contact the police to pursue the complaint').

[118] *R.* v. *Big M Drug Mart*, [1985] 1 S.C.R. 295, at para. 37.

[119] Peter Hogg, *Constitutional Law of Canada*, *4th Edition* (Scarborough, ON: Carswell, 1999).

[120] *Ibid.* at 773; s*ee, e.g., Rahey*, *supra* note 113 (comparing the interpretations of Wilson and La Forest JJ. on the theory that the contours of a remedy give shape to the right).

[121] Ian R. Kerr, 'The Legal Relationship Between Online Service Providers and Users' (2001) 35 *Canadian Business Law Journal* 419 at 443.

[122] *Irwin Toy Ltd.* v. *Quebec (A.G.)*, [1989] 1 S.C.R. 927 describes the interpretative analysis framework to be followed in freedom of expression cases. The first stage broadly interprets 'expression', except for acts of violence. The second stage determines whether there has been a violation and, if so, whether it is a content-based restraint or one that merely has the effect of limiting expression. If the latter, the party claiming the protection of the *Charter* must be able to show that the

Supreme Court has demonstrated considerable tolerance for laws that limit freedom of expression in the name of protecting minority interests, such as those prohibiting hate speech[123] and pornography.[124] Similarly, protection of reputation has sometimes prevailed over expression.[125] With respect to commercial speech, the Supreme Court has insisted upon a relatively high level of proof that legal restraints are required to achieve state objectives.[126] The following Section considers the primary facets of freedom of expression in Canada.

Anti-terrorism and cybercrime

In 2004, federal police executed search warrants at the home and offices of Juliet O'Neill, a reporter for the *Ottawa Citizen* newspaper. O'Neill had been critical of Canadian authorities' handling of the Maher Arar affair. Arar was a Syrian-born Canadian citizen about whom Canadian law enforcement shared faulty intelligence with U.S. authorities, leading to his arrest and deportation to Syria, where he was tortured. O'Neill was accused of retrieving and retaining 'secret official' government information under the Security of Information Act (SOIA).[127] Police searched O'Neill's home and seized documents and computer information, but never laid any charges.[128]

O'Neill brought a lawsuit against the federal government claiming that the police searches and seizures were invalid because the applied sections of SOIA[129] infringed her right to freedom of expression under Section 2(b) of the Charter, and her right to life, liberty, and security of the person under Section 7 of the Charter. The Ontario Superior Court found in favour of Ms. O'Neill and held that the impugned sections of SOIA were a *prima facie* violation of Ms. O'Neill's right to freedom of expression[130] and her right to life, liberty, and security of the person, because they were overbroad and unconstitutionally vague.[131]

The Charter right to freedom of expression, religion and association played a key role in the case of *R.* v. *Khawaja*,[132] wherein the Ontario Superior Court found that the definition of 'terrorist activity' in the Criminal Code[133] was invalid, because it stipulated that a 'terrorist activity' involved an activity that was committed, 'in whole or in part for a political, religious or ideological purpose, objective or cause.'[134]

> Canadians who might share the political, religious or ideological stripe of the foreign groups under scrutiny [of terrorism] could not help but fall under some sort of shadow. It is exactly that sort of phenomenon that has given rise to concerns for racial or ethnic profiling and prejudice in the aftermath of the notorious terrorist actions in a number of countries around the world in recent years.[135]

In response to the events of September 11, 2001, the federal government enacted the omnibus Anti-terrorism Act.[136] This act facilitates enhanced use of electronic surveillance against terrorist groups, allows law enforcement to invoke judicially-supervised investigative hearings to compel disclosure of information related to terrorism; and, allows for the suppression of information in the national interest during judicial proceedings.[137]

---

activity in question promotes one of the three principles underlying freedom of expression: political debate, the marketplace of ideas, or autonomy and self-fulfillment. The final stage of the analysis places the burden on the state to justify the limit it seeks to impose as being reasonable in a free and democratic society.

[123] See *R. v. Keegstra*, [1990] 3 S.C.R. 697.
[124] See *R. v. Butler*, [1992] 1 S.C.R. 452.
[125] See e.g. *Hill* v. *Church of Scientology*, [1995] 2 S.C.R. 1130.
[126] See e.g. *Ford* v. *Quebec (A.G.)*, [1988] 2 S.C.R. 712.
[127] R.S.C. 1985, c. O-5, *as am.*
[128] *O'Neill* v. *Canada (Attorney General)*, [2006] O.J. No. 4189.
[129] *Supra* note 127 at ss. 4(1)(a), 4(3), 4(4)(b).
[130] *Supra* note 128 at para. 84.
[131] *Supra* note 128.
[132] [2006] O.J. No. 4245.
[133] R.S. 1985, c. C-46 at s. 83.01(1)(b)(i) (A).
[134] Ibid.
[135] *Supra* note 132 at para. 52, D.J.A. Rutherford J.
[136] 2001, c. 41.
[137] Ibid.; See also Privacy International and the GreenNet Educational Trust, *Silenced* (Setline Data Ltd., 2003) at p. 123, available at http://www.privacyinternational.org/survey/censorship/Silenced.pdf.

In 2002, the federal government amended the Criminal Code to provide an explicit 'notice and takedown' order for the removal of child pornography or other data which makes it possible to access child pornography.[138]

Human rights

In 2002, the Canadian Human Rights Tribunal ordered the Canadian operator of a California-based Web site to cease publication on the grounds that the content was in violation of the Human Rights Act[139] and would likely expose Jews to hatred or contempt.[140] An analogous order was made against British Columbia operators of a Web site whose content associated or equated homosexuality with pedophilia, bestiality and the sexual predation of children.[141]

In May 2003, the same Tribunal issued a cease-and-desist order against a British Columbia operator of a Web site deemed anti-Semitic.[142] In another case involving a Canadian operating an anti-Semitic web site, the Tribunal persuaded the Federal Court to issue an interlocutory injunction, barring the operator from posting hate messages on the Internet.[143] When the operator violated this court order, he was imprisoned for contempt of court.[144] However, the Federal Court of Appeal granted the operator release from prison while he appealed his contempt of court conviction.[145] The Tribunal eventually issued a cease-and-desist order barring the operator from retaliating against the person who launched the action, and requiring that he pay the complainant for 'pain and suffering', special compensation, and punitive damages.[146] The Tribunal has also taken creative steps to enforce its cease-and-desist orders by addressing aspects of extra-territoriality[147] and Internet archiving.[148]

Political speech

The Canada Elections Act prohibits anonymous political advertising.[149] In May 1997, the federal elections watchdog gave notice to an Ottawa operator of a political Web site that he was in violation of the law for failing to identify the sponsor of the site. The operator eventually removed the information from the site, but it was immediately mirrored on other servers around the world.[150]

The Elections Act also bans political advertising in the 20 hour period preceding the closing of polls, but exempts any message transmitted to the public on the Internet before the blackout period and not changed during that period.[151] In 2001, an Alberta court found the blackout provision violated the Charter right to freedom of expression, but was nevertheless deemed a reasonable measure in a free and democratic society under Section 1 of the Charter.[152] On appeal, the finding was overturned because the law did not distinguish between issue advocacy and partisan advocacy. The court found that this failure represented a disproportionate and total ban on expression and precluded citizens from engaging in meaningful expression.[153]

---

[138] Bill C-15A, *Criminal Law Amendment Act, 2001*, 1st Sess., 37th Parl., 2002, cl. 7 (assented to 4 June 2002) (amending s. 164 of the *Criminal Code*: 'If a judge is satisfied by information on oath that there are reasonable grounds for believing that there is (…) child pornography or data which makes child pornography available (…)').
[139] R.S.C. 1977, c. H-6, s. 13(1).
[140] *Citron et al.* v. *Zündel*, (January 2002), T460/1596 (C.H.R.D.).
[141] *Schnell* v. *Machiavelli and Associates Emprize Inc.*, (August 2002), T594/5200 (C.H.R.D.).
[142] *Warman* v. *Kyburz*, (May 2003), T726_3102 (C.H.R.D.).
[143] *Canada (Human Rights Commission)* v. *Winnicki*, [2005] F.C.J. No. 1838, 2005 FC 1493.
[144] *Warman* v. *Winnicki*, [2006] F.C.J. No. 1092, 2006 FC 873.
[145] *Canada (Human Rights Commission)* v. *Winnicki*, [2006] F.C.J. No. 1439, 2006 FCA 314.
[146] *Warman* v. *Winnicki*, [2006] C.H.R.D. No. 18, 2006 CHRT 20.
[147] *See* A. Humphreys, 'U.S. Internet giant pulls Zundel's Web site: Canadian rights panel warned firm of hate literature' *National Post* (13 May 2003).
[148] *Supra* note 142 at para. 86 (ordering the Canadian Human Rights Commission, a separate investigative and mediation body, to write to the operators of Archive.org requesting the removal of an archived mirror of the respondent's web site).
[149] S.C. 2000, c. 9 at s. 213 (prohibition of anonymous political advertising) [Elections Act].
[150] A. Uncles, 'Elections Canada silences a Green Party webmaster' *The Ottawa Citizen* (31 May 1997).
[151] *Supra* note 149, at ss. 323, 324.
[152] *Harper* v. *Canada (Attorney General)*, [2001] A.J. No. 808 (Q.B.).
[153] *Harper* v. *Canada (Attorney General)*, [2002] A.J. No. 1542 at para. 154 (C.A.).

The Canada Elections Act prohibits premature communication of polling results prior to the close of all polling stations.[154] In September 2000, a retired teacher was charged with violating this provision when he posted to a Scottish Web site, the results of a Nova Scotia by-election before the polls closed in a simultaneous by-election held in British Columbia. Although authorities eventually dropped the charges, the incident spurred another individual to post polling results gleaned from Atlantic Canada to a Web site during the 2001 Canadian general election: again, before the polls had closed in British Columbia.[155] In April 2003, this individual was fined a nominal sum.[156] The court found that the prohibition violated constitutional guarantees of freedom of expression, but that it was a reasonable limitation under Section 1 of the Charter.

On appeal, the BC Supreme Court overturned the defendant's conviction, because he was posting election results, not projections.[157] The Court found that the only potential harm that could arise from the defendant exercising his Charter right to freedom of expression in this case was that Western voters would know Atlantic Canada's election results, when Atlantic-Canada voters had no corresponding knowledge of Western Canadian results.[158] The Court found that this informational imbalance was not sufficient to restrict the defendant from exercising his right to freedom of expression.[159] However, in May 2006, the BC Court of Appeal reversed the lower court judgment and upheld the ban on reporting election results as promoting fairness and helping to ensure that all voters receive equal treatment on election day.[160] The Supreme Court upheld this decision.[161]

Court proceedings

Canadian law prohibits the reporting of some aspects of court proceedings. For example, Parliament has legislated restrictions on the publication of the identity of a complainant in sexual offences,[162] restricted the publication of evidence at a preliminary inquiry,[163] and evidence given at a 'show cause' hearing.[164] In addition to these statutory restrictions, a court has the power to restrict publication of any part of a proceeding it deems necessary to protect an accused's right to a fair trial.[165] These restrictions have frequently run head first into the Internet-enabled axiom that information wants to be free.

In 1993, an Ontario couple was charged with the abduction, rape and murder of two teenage girls. The wife was tried first and, to protect her co-accused husband' rights to a fair trial, the court issued a time-limited publication ban on most aspects of the trial.[166] However, the case dealt with particularly gruesome facts and attracted a terrific amount public interest at a time when the Internet was becoming a mainstream information and communication medium.

Although Canadian media outlets were subject to the ban and foreign media had been excluded from the courtroom altogether, details of the trial were regularly leaked to foreign media outlets and Web sites. Court-ordered publication bans and the Internet have continued to collide in years since. In 2001, details from the preliminary hearing on the Air India Flight 182 bombing were posted to an Internet Web site notwithstanding a publication ban imposed by the court.[167] In April 2003, shortly after the start of the preliminary hearings into Canada's largest ever serial murder case, defence counsel alleged violations by both Canadian and U.S. media of the court-ordered publication ban. In response, the judge threatened to bar all foreign media from covering

---

[154] *Supra* note 149, at s. 322.1.
[155] 'Case dismissed against Internet vote-results rebel' *The Halifax Herald* (14 November 2002).
[156] *R.* v. *Bryan*, [2003] BCJ. No. 318 at para. 13 (Prov. Ct. (Crim. Div.)).
[157] *R.* v. *Bryan*, [2003] BCJ. No. 2479, 2003 BCSC 1499.
[158] Ibid.
[159] Ibid.
[160] *R.* v. *Bryan*, [2005] BCJ. No. 1130, 2005 BCCA 285.
[161] CBC News, 'Top Court rejects appeal to suspend election gag law' (13 January 2006), available at http://www.cbc.ca/news/story/2006/01/13/election060113.html.
[162] Criminal Code, R.S. 1985, c. C-46, s. 486(3).
[163] Ibid. at s. 539.
[164] Ibid. at s. 517.
[165] *R.* v. *Barrow* (1989), 48 C.C.C. (3d) 308 at 315 (N.S.C.A.).
[166] *R.* v. *Bernardo* [Publication ban - Proceedings against co-accused [1993] O.J. No. 2047 (Gen. Div.).
[167] R. Mattas, 'Forbidden Air-India details posted on Internet Web site reveals information on suspects' bail hearing, despite ban on publication' *The Globe and Mail* (13 Feb 2001).

the trial and specifically noted that publishing prohibited information on Internet sites would constitute a violation.[168]

In July 2003, the author of two controversial books on the previously mentioned 1993 Ontario murder trial was arrested, had his computer seized and his Web site shut down for violating a court order to suppress materials relating to the trial. The author had posted photographs, videotapes, and interviews from the case to the Internet. The executive director of Canadian Journalists for Free Expression said his group viewed the arrest with suspicion.[169]

In the anti-terrorism context, s. 83.28 of the Criminal Code allows for *in camera* investigative hearings if there are reasonable grounds to believe that a terrorist offence has been or will be committed. In the matter *Application under Section 83.28 of the Criminal Code (Re)*,[170] the Supreme Court upheld the constitutional sufficiency of this procedure. In the companion case *Vancouver Sun (Re)*,[171] the Court omitted the necessity of investigative hearings for national security. It found that these hearings should be subject to openness and not be presumptively displaced in favour of an *in camera* process.[172] Courts are therefore, obligated to reveal as much information about a case as can be without jeopardizing an investigation.[173] Only when necessary, should resort be made to publication bans.[174]

Blocking and filtering

There are no known instances of federal or provincial governments attempting to block or filter Web sites outside of an employment context. Nor are there public initiatives at either the federal or provincial level to force public libraries to adopt filtering software; the decision is left up to individual libraries. An informal sampling conducted by the CBC Marketplace television program indicates that even of the libraries that do choose to filter patron-accessible content, most also provide unfiltered Internet terminals away from children's areas of the library.[175] The Canadian Library Association has described filtering as a 'slippery slope' and has taken a strong stand against it.[176]

In 2002, the Canadian Union of Public Employees launched six grievance hearings in an effort to force the Ottawa Public Library to prevent patrons from using Internet terminals to access sexually explicit materials, presumably by installing filtering software.[177] The Ottawa Public library eventually enacted a policy that provides filtered Internet access for all library patrons under 17 years of age, but unfiltered Internet access for adults.[178]

Protest and parody

In January 2001, a British Columbia court found that a union's use of an employer's domain name and meta-tags did not constitute an attempt to 'pass off' under the *Trade-marks Act*.[179] The Court found that 'when a Web site is used for expression in a labour relations dispute, as opposed to commercial competition, there is (…) a reasonable balance that must be struck between the

---

[168] D. Girard, 'BC pig farmer to be tried in the deaths of 15 women' *The Toronto Star* (24 July 2003).
[169] D. Nolan, 'Karla author's home raided, computers taken' *The Hamilton Spectator* (19 July 2003).
[170] [2004] S.C.J. No. 40, [2004] 2 S.C.R. 248, cited in Cohen, op. cit. n. 38 at p. 292.
[171] [2004] S.C.J. No. 41, [2004] 2 S.C.R. 332 at 355, cited in Cohen, op. cit. n. 38 at p. 292.
[172] *Vancouver Sun (Re)*, [2004] S.C.J. No. 41, [2004] 2 S.C.R. 332 at 339, cited in Cohen, op. cit. n. 38 at p. 293.
[173] Cohen, op. cit. n. 38 at p. 295.
[174] Ibid.
[175] R. Wright and C. Jones, 'Internet Filters: Internet Filtering at selected Canadian libraries' *CBC Marketplace* (22 October 2002), available at CBC http://www.cbc.ca/consumers/market/files/health/kids_online/policies.html date accessed: 21 November 2006.
[176] J. Campbell, 'Filtered Internet starts library down "a slippery slope"' *The Ottawa Citizen* (28 January 2003) B1 (quoting the executive director of the CLA as stating that unfettered access to information as fundamental to an open and democratic society); See also R. Kantner, 'Legal Issues Resulting from Internet Use in Public Libraries' (2000) 46(1) *Feliciter* 14.
[177] K. Gray, 'City library becoming a "porn palace": CUPE: Children can glimpse explicit material on library computers' *The Ottawa Citizen* (25 January 2003) D1.
[178] Ottawa Public Library, 'Booking a Library Computer: Frequently Asked Questions' (accessed 21 November 2006), online http://www.biblioottawalibrary.ca/explore/virtual/obs_faq_e.html.
[179] R.S. 1985, c. T-13.

legitimate protection of a party's intellectual property and (…) [freedom] of expression.'[180] However, the court found that the union's use of the colour scheme, page layout, logo and other aspects of the graphic design to parody the employer's site amounted to copyright infringement because it contained no criticism nor did it mention the source and author of the site, as required by the *Copyright Act*.[181]

In 2003, a British Columbia court ordered a plaintiff in a defamation suit to 'be more specific' in a claim based on, among other things, postings made to a Web site.[182] The court found that a claim of defamation requires a greater degree of specificity than is required in most other causes of action.[183]

In July 2003, Air Canada sent a letter to the operator of a Web site critical of Air Canada CEO Robert Milton. The protest site had copied the company's logo, banner and featured a photograph of an Air Canada plane.[184] An Air Canada representative stressed that the company did not object to the criticism of its officers and directors, but only to the unauthorized use of its registered trademarks.

Anonymity

In at least two cases, Ontario courts have ordered Internet Service Providers (ISPs) to disclose the names of subscribers who have allegedly made fraudulent postings in chat rooms.[185] Although the order is not granted automatically, the threshold for granting access is low.

In at least two other cases, Canadian courts have granted motions to compel ISPs to disclose the identity of the senders of anonymous emails to the Canadian Blood Services (CBS) agency. In both instances the correspondents had claimed that they were sexually-active gay men who had donated blood and would continue to do so in contravention of a CBS policy.[186]

In 1999, a BC court granted injunctions against two Web sites on which users had posted anonymous and allegedly defamatory messages. In granting the *ex parte* motion, the judge noted that the concern for the protection of free speech was lessened because the speakers chose 'to throw around accusations of the most serious kind behind the cowardly screen of an alias.'[187]

In *BMG Canada Inc.* v. *John Doe*[188] the Federal Court of Appeal established the legal test that plaintiffs must meet in order to compel ISPs to disclose their customers' identities in matters brought before the federal courts, such as intellectual property disputes. The test requires a *bona fide* claim of copyright infringement, admissible and timely evidence linking the IP address in question to the alleged infringement, clear evidence that the information cannot be obtained from another source, and only collecting enough information as required for the lawsuit to take place.[189]

In anticipation of ratifying the Council of Europe's *Convention on Cyber-crime*, the federal government has proposed introducing legislation to force ISPs to collect and keep accurate identifying information on their subscribers, to preserve dynamic routing information with a simple administrative order and to make their networks wiretap capable.[190] There is, as yet, no requirement or proposal to require automatic data retention of all subscribers, as in many European states.

Unlike in some states, such as Australia, the Netherlands, and Germany, there is presently no requirement for service providers in Canada to collect or maintain accurate subscriber information. The Canadian Association of Chiefs of Police has lobbied for the establishment of a

---

[180] *British Columbia Automobile Assn.* v. *Office and Professional Employees' International Union, Local 378*, [2001] BCJ. No. 151 at para. 130 (Sup. Ct.) [*BCAA*].
[181] Ibid. at para. 205.
[182] *Craig* v. *Langley Citizens' Coalition*, [2003] BCJ. No. 141 (Sup. Ct.).
[183] Ibid. at para. 17.
[184] 'Air Canada claims web infringement' *The Globe and Mail* (11 July 2003) B2.
[185] *Phillips Services Corp.* v. *John Doe*, (1998) Court file no. 4582/98 (Ont. Ct. (Gen. Div.)), *Irwin Toy* v. *Doe*, [2000] O.J. No. 3318.
[186] 'E-mails claim gay man defied blood policy' *The Globe & Mail*, (29 July 2002); 'Gay Blood Donor' *Canadian Press* (28 July 2002); 'Blood services stymied in search for second gay donor through e-mails' *Canadian Press* (29 July 2002).
[187] *Henry* v. *Stockhouse Media Corp.*, [1999] BCJ. No. 3202 (Sup. Ct.) at paras. 8-13.
[188] 2005 FCA 193.
[189] Ibid. at paras. 41-45.
[190] *Supra* note 98.

national database of Internet and wireless subscribers and the requirement that service providers be held liable for collecting and maintaining accurate information on their subscribers.[191] This proposal has been met with hostility by privacy advocates and industry representatives alike.[192]

In July 2003, a British Columbia court ordered a Vancouver-based ISP to provide the identities of 30 of its subscribers to America Online, which had identified the account-holders as prolific 'spammers'.[193] Controlling spam remains on the legislative radar. In 1999, the federal government released a discussion paper on spam which concluded that the existing policy and legal framework were sufficient to address the situation.[194] Following a dramatic rise in spam, the government revisited the issue in a new discussion paper in January 2003, which raised the prospect of anti-spam legislation.[195] In 2004 the Federal government created an anti-spam task force which released a report recommending more rigourous law enforcement, public education, policy development and legislation to combat spam.[196]

In November 2005, the Federal government introduced Bill C-74, the *Modernization of Investigative Techniques* Act (MITA).[197] Under MITA, law enforcement and national security officials could intercept communications,[198] or compel telecommunications service providers (TSPs) to provide them with subscriber information[199] without a warrant. MITA died on the order paper when a general election was called less than a month later, however the newly elected Conservative government may revive this bill in 2007.

Intermediary liability

There is no 'common carrier' exemption or 'safe harbour' available to Canadian Internet intermediaries, as there is under the U.S. *Digital Millennium Copyright Act of 1998*.[200] ISP liability for copyright infringement must be determined on the basis of the *Copyright Act*, which exempts from liability a person whose only act in respect of the communication of a work to the public consists of providing *the means of telecommunication necessary* for another person to communicate the work.[201] In 1999, the federal Copyright Board found that ISPs were entitled to rely on this exemption.[202] On appeal to the Federal Court of Appeal, this was affirmed, but the court found that an Internet intermediary who *caches* material does not merely provide the means necessary for another to communicate a musical work.[203] Rather, a cache operator performs an editorial function and is thus not merely a passive transmitter of data.

On appeal, the Supreme Court held that an ISP's knowledge that someone might be using content-neutral technology to violate copyright is not necessarily sufficient to constitute authorization to infringe. Rather, authorization requires a demonstration that the defendant gave approval to, sanctioned, permitted, favoured, or encouraged the infringing conduct. [204] Notice of

---

[191] *Ibid.* at 18.
[192] Nevis Consulting Group, ed., *Summary of Submissions to the Lawful Access Consultation*, (Ottawa, ON: Department of Justice Canada, 2003), available at Lex Informatica <http://www.lexinformatica.org/cybercrime/pub/la_summary.pdf date accessed: 21 November 2006.
[193] B. Mudry, 'Peer 1 accepts BC spam subpoena in AOL probe' *Canada Stockwatch* (10 July 2003).
[194] Industry Canada, *Internet and Bulk Unsolicited Electronic Mail (SPAM)*, (Ottawa: Industry Canada, 1999).
[195] Industry Canada, *E-mail marketing: Consumer choices and business opportunities*, (Ottawa: Industry Canada, 2003).
[196] Industry Canada, 'Task Force on Spam' (7 April 2006) available at http://strategis.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00248e.html.
[197] Bill C-74, *An Act regulating telecommunications facilities to facilitate the lawful interception of information transmitted by means of those facilities and respecting the provision of telecommunications subscriber information*, 1st Sess., 38th Parl., 2004-2005 [MITA].
[198] Ibid. at s. 6(1).
[199] Ibid. at s. 17(1).
[200] Pub. L. No. 105-304, § 512 (1998).
[201] R.S.C. 1985, c. C-42, s. 2.4(1)(b) [Copyright Act].
[202] *SOCAN Statement of Royalties, Public Performance of Musical Works 1996, 1997, 1998 (Tariff 22, Internet) (Re),* (1999) 1 C.P.R. (4th) 417 (Copyright Board), (In general, the parties who may rely on this exemption include an ISP of the person who makes the work available, persons whose servers are used as a cache or mirror, the recipient's ISP, and those parties who operate routers used in the transmission. However, the exemption may not apply to a person who has a relationship with the person who makes the musical work available so as tobe acting in concert with that person, or if the person's role is not confined to that of an 'intermediary').
[203] *Society of Composers, Authors, and Music Publishers of Canada v. Canadian Association of Internet Providers*, 2002 FCA 166 at para. 161, var'd [2004] S.C.J. No. 44, 2004 SCC 45 (S.C.C.).
[204] *Society of Composers, Authors and Music Publishers of Canada* v. *Canadian Assn. of Internet Providers*, [2004] S.C.J.

infringing content, and a failure to respond by 'taking it down', may in some circumstances lead to a finding of 'authorization.'[205] Therefore, authorization could be inferred in some cases, but that would depend on the facts.[206]

The notion of intermediary liability has grown increasingly important in the defamation context, where these laws place a 'reverse onus' on the speaker to prove that the speech is not defamatory. There are several lawsuits ongoing, though as yet no court decisions, on the issue of intermediary liability for speech. In the U.S., intermediaries have broad immunity from liability for third party speech. There is no equivalent immunity in Canadian law.

Copyright

For a number of reasons, the tension between copyright and freedom of expression is less and criticism more muted than in the United States.[207] Unlike in the U.S., rights collectives have not been successful in litigating against peer-to-peer users or Internet intermediaries.[208] This is, in part, due to the 'private copying levy' (found also in many Continental copyright regimes), which creates an exception to infringement for copying music for private use in exchange for a levy on all 'blank audio recording' media typically used to make such copies. The provision does not exempt musical works communicated by telecommunication to the public (and thereby does not at all address uploading),[209] but the levy has nevertheless tempered Canadian copyright owners' criticism of music file-sharing.

Trademarks and domain names

In January 2001, a British Columbia court found that a union's use of an employer's domain name did not constitute passing-off under the *Trademarks Act* because although the domain name contained a registered mark, it was not identical and the context was not misleading. The court also found it significant that the site did not compete commercially with the mark holder.[210]

The Canadian, Québec and Alberta governments have all succeeded in requests for transfers of domain names registered by private parties. In all cases, the private parties had registered names for the purpose of selling or renting them and the names were found to be 'confusingly similar' to actual government Web sites or agencies.[211]

In addition, there have been numerous domain dispute resolutions between private parties under the Canadian Internet Registration Authority's Domain Name Dispute Resolution Process (CDRP).[212] However, at least one critic has noted that the CDRP is not always applied predictably.[213]

Of more concern for freedom of expression than inconsistency in the CDRP, is the growing tendency of U.S. courts to apply the long-arm provision of the *Anticybersquatting Consumer Protection Act*[214] to domain name disputes between Canadian nationals merely on the basis that

---

No. 44, 2004 SCC 45 at paras. 127, 128.

[205] Ibid.

[206] Ibid.

[207] See e.g. J. Cohen, 'Information Rights and Intellectual Freedom' in A. Vedder, ed., *Ethics and the Internet* (Antwerp: Intersentia, 2001) at 22 ('with these [safe harbour] provisions, copyright law now gives content owners new powers to silence creators of unauthorized expression, including fair use expression').

[208] *Supra* note 202.

[209] *Supra* note 201at s. 80(2)(c).

[210] *BCAA*, *supra* note 180 at paras. 123-126.

[211] See e.g. *Government of Canada* v. *David Bedford a.k.a. DomainBaron.com* (2001), WIPO Case D2001-0470, (UDRP), *Gouvernement du Québec* c. *Peter McCann* (2002), WIPO Case D2002-1010, (UDRP), *Government of Canada* v. *David Bedford a.k.a. Abundance Computer Consulting* (2003), CIRA Case 00011 (CIRA), *Government of Alberta* v. *Advantico* Internet Solutions, Inc. (2003), 00012 (CIRA).

[212] See e.g. *Red Robin International* v. *Greg Tieu* (2002), CIRA Case 00001 (CIRA), *Canadian Broadcasting Corporation* v.*William Quon* (2002), CIRA Case 00006 (CIRA), *Great Pacific Industries, Inc.* v. *Ghalib Dhalia* (2003), CIRA Case 00009 (CIRA).

[213] M. Geist, 'Fairness demands review of domain-name policy' *The Toronto Star* (11 August 2003); See e.g. *Air Products Canada* v. *Index Quebec, Inc.* (2002), CIRA Case 00007 (CIRA) (domain name 'airproducts.ca' not deemed confusingly similar to name of complainant company; registration of thousands of domain names not demonstrating 'bad faith' on part of defendant).

[214] 15 U.S.C. § 1125(d). (A challenge inherent in resolving domain name disputes is that the parties will frequently reside in different jurisdictions. While the trademark holder may be able to obtain a local court order to have the domain name

the domain name was registered in the United States.[215] For example, in *Technodome*, a U.S. district court asserted *in rem* jurisdiction over a domain name in a dispute between two Canadian trademark holders, adopting the rationale that:

> [the p]laintiff may not be able to assert the same rights in Canada, which lacks a body of law equivalent to the [*Anti-cybersquatting Protection Act*] and whose enforcement of its trademark laws cannot extend into the United States. Defendants suggest that Canadian intellectual property law, drawing upon recent English case law, might view the registration of a trademark-infringing domain name as an actionable trademark violation (…). However, Defendants' prediction of what the Canadian courts will do when presented with this issue is necessarily speculative and provides little support for the argument that Canada is a satisfactory alternative forum for this lawsuit.[216]

The U.S. is not the only offender of comity, but U.S. hegemony makes its exercise of legislative jurisdiction more poignant than in any other country. Often this is particularly true for Canada.

3.6. Conclusion

In a nation that spans a continent, Canada's federal structure – providing as it does more democratic governments – is one of its greatest strengths. It is also the source of much consternation when it comes to addressing the inevitable tensions between new technologies and constitutional rights in areas like privacy, defamation, consumer protection, and taxation among others.

New information and communications technologies have done much to make geographical boundaries irrelevant, but the constitutional division of powers means that the federal government is hampered from acting in areas where new technologies may most strain constitutional and other legal rights and harmonization of laws makes sense.

This situation is unlikely to change. Though Canada's Constitution contains five different amending formulae,[217] each requires a high level of agreement between the provinces and federal government, which for historical and political reasons has proved impractical. Consequently, legislative amendments to the Constitution are exceedingly rare and the evolution of Canadian constitutional rights is left almost exclusively to the courts.

When it comes to the consideration of new technologies, there are certain advantages to the plodding pace of a court-based approach to constitutional interpretation.

Laws are expensive to administer, both in terms of economic and social costs.[218] The most expensive kind of legal administration is enforcement. Well-designed laws act as normative signals which encourage compliance with minimal cost. Conversely, poorly-designed or ill-timed laws often exacerbate the problem to which they are addressed; else stifle the entry of more efficient yet unrealized solutions, market, technological or regulatory.

Because administration is costly, policymakers must consider the role of technology to change the value equation. Law is never developed in a vacuum. It interfaces with the political, cultural and social fabric of its environment; and, increasingly it must also take account of technology. Nor is technology developed in a vacuum. It carries inherent values and valences, some of which are intentionally designed and others which derive from the unexpected ways in which individuals perceive or adapt technology to their unique purposes.

Further, technology will always change faster than law and clumsy legislation is never more likely than when the underlying technostrata is yet mature.[219] It seems common sense to demand

---

transferred or cancelled, enforcing the order against an *ex juris* registrant is often expensive. The ACPA addresses this by granting trademark holders the right to file an *in rem* action against the domain name itself, rather than an *in personam* suit against the registrant).

[215] *A.E. Heathmount* v. *Technodome.com*, 106 F.Supp. 2d 860 (E.D. Va. 2000); See also M. Geist, 'U.S extends its hegemony over the Net' *The Toronto Star* (9 June 2003).

[216] *Heathmount A.E. Corp.* v. *Technodome,* [2000] U.S. Dist. LEXIS 20316 at 21 (U.S. Dist. Ct. Eastern Div.), LEXIS (MEGA).

[217] Part V of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c.11, s. 38(1).

[218] Eric Posner, 'Law and Social Norms: The Case of Tax Compliance,' (2001) 86 Va. L. Rev. 1781 at 1791-1792 'Judges, lawyers, courthouses, and the rest of the apparatus of the legal system are expensive. If people conformed to desirable social norms, then these costs could be avoided [and] the system of norm-driven or nonlegal [sic] coordination may be as expensive as the legal system.'

[219] Frank Easterbrook, 'Cyberspace and the Law of the Horse,' (1996) *U. Chi. Legal F.* 207 at 215 [Easterbrook].

caution in the regulation of complex things, but all too frequently passions and hyperbole rule agendas. Governments want to be seen to be doing something, even if they have no idea of the implications of their actions.[220] Justice Easterbrook, Chief Justice of the U.S. Court of Appeals for the Seventh Circuit, answers the rhetorical: what should we do?

> By and large, nothing. If you don't know what is best, let people make their own arrangements. Next after nothing is: keep doing what you have been doing. Most behavior in cyberspace is easy to classify under current property principles.[221]

Legislative humility does not advocate either ignorance or inertia, but preconditions regulatory action on two events. First, policymakers need to make policy choices based on an objective observation of facts. Action without objective facts will likely be just as harmful as inaction (precaution) without principle.[222] The difficulty is that technology is often opaque, unpredictable and complex. Even relatively simple technologies can have underlying complex values. These characteristics can confuse policymakers' attempts to understand how the technostrata might interact with norms or laws, or how the values it represents might change over time.

Inputs to complex systems cannot be summed to give trends and create conditions ripe for ineffective regulation. Poorly-designed laws can signal unwanted norms, increase administrative and enforcement costs and obscuring the context in which they were drafted, forcing courts to adopt contextually-inappropriate interpretations.

Even an adequate collection of objective facts can only ever be a snapshot if the technostrata is in flux. New technologies create disequilibrium,[223] which is rarely ever a good time to make judgments on value. Thus, policymakers should not adopt regulatory solutions before the technostrata has matured. There are a number of different ways to measure maturity, including market dominance, evidence of monopoly, standards-setting, or – at a lower threshold – of profit-making.[224] Absence of any of these indicia should be an indication that regulation is probably premature and will be ineffective.

A long, broad approach to regulation[225] will allow the values of the technostrata to solidify, give the market the first opportunity to respond to potential failures, and lend policymakers perspective on the how technostrata values and valences will interact with laws and social norms. The Canadian approach – by the legislatures and courts – to areas such as copyright and cybercrime has been characterized by such a perspective, though perhaps not by design.

Legislative humility also means also that policymakers should avoid overly-prescriptive solutions when they do choose to act.[226] Nor should policymakers attempt to legislate 'perfect' solutions, because this will inevitably lead to laws tied too closely to a particular set of facts, technology or else to nothing at all, thus prejudicing particular valences over others, including as yet unknown ones.[227] Overprescription divests administrators of the ability to respond appropriately to normative or technological changes.

> Detailed, technology-specific provisions reflecting the passing concerns of a moment have proven difficult to adapt to new technologies. The IP system does best when it responds to new technologies with broad, enabling amendments. This leaves considerable room for maneuvering in the courts, and

---

[220] *See e.g.* Bill C-11, *An Act to amend the Copyright Act*, 1st Sess., 37th Parl., 2002 (prohibiting retransmitters who use the Internet to hold compulsory licences).
[221] Easterbrook, *supra* note 219 at 207.
[222] Gregory Conko and Henry Miller, 'Precaution Without Principle,' (2001) 19:4 *Nature Biotechnology* 302.
[223] Robert Merges, 'One Hundred Years of Solicitude: Intellectual Property Law, 1900-2000', (2000) 88 *Calif. L. Rev.* 2187 at 2190.
[224] *See generally* Robert Litan, 'Law and Policy in the Age of the Internet,' (2001) 50 *Duke L.J.* 1045[Litan], regulation of dominant or monopoly players is a theme borrowed from the telecommunications world; *compare See e.g.* Siva Vaidhyanathan, *Copyrights and Copywrongs* (New York, NY: NYU Press, 2001) at 181 who argues that if the market is working, as evidenced by profit-making, then policymakers should be skeptical of introducing corrections.
[225] *See e.g.* Jennifer Light, 'New Technologies and Regulation: Why the Future Needs Historians' (2001) *L. Rev. Mich. St. U. Det. C.L.* 241 at 242 [Light].
[226] Litan, *supra* note 224 at 1085: 'When they do act, though, they must do so pragmatically and with a humility that allows for constant mid-course corrections.'
[227] *See e.g.* John Holland, 'What Is To Come And How To Predict It' in John Brockman, ed., *The Next Fifty Years: Science in the First Half of the Twenty-First Century*, (Toronto: Vintage Books, 2002).

buys more time for the inevitable consolidation of quasi-common-law changes in major statutory revisions.[228]

Canadian legislatures and courts have, particularly, in areas such as privacy and data protection acted, explicitly (and in many instances implicitly) from principles found or informed by the broad Charter protections described herein.

Policy-makers should also be aware that there are significant opportunity costs to legal preemption of technology. Such preemption can preclude beneficial future innovation, immeasurable precisely because it is undefined.[229]

References

Sam N.K. Banks and Andrew Kitching, Library of Parliament, 'Legislative Summary, Bill C-60: An Act to Amend the Copyright Act' (2005), available at http://www.parl.gc.ca/LEGISINFO/index.asp?List=ls&Query=4527&Session=13&Language=e.

J. Cohen, 'Information Rights and Intellectual Freedom' in A. Vedder, ed., *Ethics and the Internet* (Antwerp, Belgium, Intersentia, 2001) p. 21.

Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham, ON, Lexis Nexis Canada Inc., 2005).

Gregory Conko and Henry Miller, 'Precaution Without Principle', 19(4) *Nature Biotechnology* (2001) p. 302.

Ronald J. Daniels, Patrick Macklem, and Kent Roach, eds., *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill* (Toronto, ON, University of Toronto Press Inc., 2001).

Department of Justice Canada, 'Amendments to Bill C-36' (2001), available at http://canada.justice.gc.ca/en/news/nr/2001/doc_27902.html.

Department of Justice Canada, 'Emails: Considerations for Criminal Law Policy' (March 2005), available at http://www.cippic.ca/en/projects-cases/lawful-access.

Department of Justice, Industry Canada, and Solicitor General Canada, 'Lawful Access – Consultation Document', (25 August 2002), available at http://www.justice.gc.ca/en/cons/la_al/law_access.pdf.

Frank Easterbrook, 'Cyberspace and the Law of the Horse', *U. Chi. Legal F.* (1996) p. 207.

Paul Goldstein, *Copyright's Highway: The Law and Lore of Copyright From Gutenberg to the Celestial Jukebox*, (New York, NY, Hill & Wang, 1996).

Peter Hogg, *Constitutional Law of Canada*, *4th Edition* (Scarborough, ON, Carswell, 1999).

John Holland, 'What Is To Come And How To Predict It' in John Brockman, ed., *The Next Fifty Years: Science in the First Half of the Twenty-First Century*, (Toronto, ON, Vintage Books, 2002).

Industry Canada, *E-mail marketing: Consumer choices and business opportunities*, (Ottawa, ON, Industry Canada, 2003).

Industry Canada, *Internet and Bulk Unsolicited Electronic Mail (SPAM)*, (Ottawa, ON, Industry Canada, 1999).

R. Kantner, 'Legal Issues Resulting from Internet Use in Public Libraries', 46(1) *Feliciter* (2000) p.14.

Ian R. Kerr, 'The Legal Relationship Between Online Service Providers and Users', 35 *Canadian Business Law Journal* (2001) p. 419.

Robert Litan, 'Law and Policy in the Age of the Internet', 50 *Duke L.J.* (2001) p. 1045.

Jennifer Light, 'New Technologies and Regulation: Why the Future Needs Historians', *L. Rev. Mich. St. U. Det. C.L.* (2001) p. 241.

Robert Merges, 'One Hundred Years of Solicitude: Intellectual Property Law, 1900-2000', 88 *Calif. L. Rev.* (2000) p. 2187.

[228] Merges, *supra* note 223 at 2191.

[229] *See generally* Light, *supra* note 225; *compare* Paul Goldstein, *Copyright's Highway: The Law and Lore of Copyright From Gutenberg to the Celestial Jukebox*, (New York: Hill & Wang, 1996) at 202, advocating quick action in the face of disruptive technologies.

Nevis Consulting Group, ed., *Summary of Submissions to the Lawful Access Consultation*, (Ottawa, ON, Department of Justice Canada, 2003), available at http://www.lexinformatica.org/cybercrime/pub/la_summary.pdf.
Eric Posner, 'Law and Social Norms: The Case of Tax Compliance', 86 *Va. L. Rev.* (2001) p. 1781.
Privacy International and the GreenNet Educational Trust, *Silenced* (Setline Data Ltd., 2003) p.123, available at http://www.privacyinternational.org/survey/censorship/Silenced.pdf.
Jennifer Stoddart, Privacy Commissioner of Canada, 'Annual Report to Parliament, 2003-2004' (2004), available at http://www.privcom.gc.ca/information/ar/200304/200304_e.asp#foreword.
Jennifer Stoddart, Privacy Commissioner of Canada, 'Bill C-7, the Public Safety Act, 2002' (Address to the Senate Standing Committee on Transport and Communications, 18 March 2004), available at http://www.privcom.gc.ca/speech/2004/sp-d_040318_e.asp.
Jay Thompson, 'Liability for On-Line Activity: The Buck Stops Where?' (unpublished paper presented to the IT-CAN Conference, 3 October 2002).
Siva Vaidhyanathan, *Copyrights and Copywrongs* (New York, NY, NYU Press, 2001).
R. Wright and C. Jones, 'Internet Filters: Internet Filtering at selected Canadian libraries', *CBC Marketplace* (22 October 2002), available at http://www.cbc.ca/consumers/market/files/health/kids_online/policies.html.

Chapter 4. Constitutional Rights and New Technologies in France

Fanny Coudert,[1] Anne Debet,[2] Paul de Hert[3]

4.1. Introduction

This chapter aims at giving a general overview of the influences of new technologies on the development of constitutional rights in the French Constitutional Law since the year 2000. The emergence of new technologies has always given rise to new legal concerns that have to be absorbed and solved by the legal system. The emergence of computer-based technologies and particularly the wide-spread use of the Internet are producing an important reform of society and our way of living, and thus our legal system should adapt. This is particularly the case in the field of constitutional rights, which are challenged by the new possibilities created by these technologies. The processing and profiling of vast quantities of data, for example, implies new trespasses on privacy. The possibilities of gathering information have been multiplied through technical means such as video surveillance, Internet tracking, etc., often without the acknowledgment of the subject. Freedom of speech is promoted by the free and easy use of the Internet. However it becomes more difficult to control possible abuse and the publication of harmful content. Questions of liability of the actors of the Internet arise.

As the French Constitution does not provide a catalogue of constitutional rights, and because the sources of constitutional rights are a composite of former constitutional texts that included a general formulation of the rights, the adaptation of French Law to the new circumstances have been relatively easy and have not implied constitutional modifications. Moreover, concerns raised by new technologies are not usually solved at the constitutional level, but at a lower level, by administrative or judicial authorities, when it comes to the application of the rules. The Constitutional Council appears limited in its control over new legislation as it can only realise an *a priori* and abstract control of the laws.

This chapter does not only discuss constitutional jurisprudence regarding new technologies but also the modalities of exercise of constitutional rights in the context of new technologies, as defined by lower jurisdictions and administrative bodies, in particular since the year 2000. It will focus on privacy-related and communication-related rights.

From 1998 onwards, the French government has developed a series of Action Plans to face societal changes generated by new technologies and to adapt the existing framework, as well as to enable citizens to take advantage of the changing economy and society. Before giving an overview of the public initiatives in this field and the constitutional modifications, a brief description of the French constitutional system related to the protection of fundamental rights should be provided.

Unlike most Western constitutions, The French Constitution of 1958 does not include a catalogue of fundamental rights. Their recognition in French constitutional law has been the result of the jurisprudence of the Constitutional Council [*Cour Constitutionnelle*].[4] The Constitution does

[1] Fanny Coudert is a legal researcher at ICRI, KU Leuven, Belgium. She has a Law degree in French and Spanish Law from the University Panthéon-Sorbonne of Paris and from the University Complutense of Madrid and a Master Degree in ICT Law from this same University.

[2] Anne Debet has a PhD in Law (*The influence of the European Human Rights Convention on Civil Law*, Dalloz, 2002), *agrégée* in Private Law. She was associate professor at the University Panthéon-Assas (Paris II) from 2001 to 2003. Since 2003, she is professor at the University of Angers (France) and co-director of a Master on Comparative Law of legal acts [*Master recherche étude comparée des actes juridiques*] at the University of Angers. She is editor of a quarterly column on European Contract Law in *Revue des contrats*. She is a member of the French Data Protection Authority, the *Commission nationale de l'informatique et des libertés*, since January 2004.

[3] Paul de Hert is Associate Professor in Law & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands, and Professor at Law, Science, Technology & Society (LSTS), Free University of Brussels, Belgium.

[4] A. Koekkoek, P. Zoontjens, et al., *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek*

not confer to the Council an explicit power to operate a control of the constitutional validity relative to fundamental rights and freedoms, but the Council has acquired such power through its decision of 1971 in relation to the freedom of association.[5] In this decision, the Council recognised that the Preamble of the Constitution of 1958 had a constitutional value that extends to the other texts referred to in the preamble, viz., the Preamble of the Constitution of 1946, the Declaration of the rights of Man and of the Citizen of 1789, and the Charter of Environment of 2004. Gradually, a 'constitutional block' [*bloc de constitutionnalité*] has been recognised that is considered the source of French fundamental rights and liberties and that consists of a series of texts and principles. First, there are the 'Fundamental principles recognised by the law of the Republic' [*Principes fondamentaux reconnus par les lois de la République]*, mentioned by the Preamble of 1946. These are core principles of French Law, created by the legislator. They are not written down in the Constitution, but raised to the level of a constitutional norm. For their recognition, the Constitutional Council requires that the principle has been created by a legislative text, with a Republican nature, prior to 1946. One example of an act falling in this category is the text relative to the freedom of association and relative to individual freedom. Second, there are the rights listed in the Preamble of the Constitution of 1946, 'politic, economic, and social principles particularly necessary to our time' [*principes politiques, économiques et sociaux particulièrement necessaires à notre temps*], e.g., the right to health, the right to strike, etc. Third, there are the 'principles with a constitutional value', viz., general principles of law recognised in case law, e.g., the continuity of public services and human dignity. Finally, the *bloc de constitutionnalité* consist of 'objectives with a constitutional value'. These elements of the constitutional block draw on societal and social needs, e.g., Public Order. They have to guide normative action, and they usually serve to justify derogations to other constitutional rights.

One realises that the originality of the French system of protecting the public liberties comes from the diversity of its historic sources, some quite old and expressed in much more general terms than the ones contained in more recent constitutions endowed with a specific catalogue of fundamental rights.[6] This constitutes a clear advantage when facing the challenges of the Information Society.

The guarantees of civil liberties are ensured by the Constitutional Council and by the judicial and administrative courts. The Constitutional Council is solely competent to control the constitutional validity of laws; it can do this in two cases: when a proposed law specifies the functioning of the public administration (organic laws) or when 60 deputies and senators present a special request for reviewing the constitutional validity of the law, after its approval but before its promulgation. This means that once a law has been promulgated, it is considered to conform to the Constitution, without any possibility to challenge it. The control realised by the judicial and administrative courts is limited to their scope of competence, i.e., judicial and administrative decisions. Article 66 of the Constitution explicitly attributes the control of individual freedom to the judicial courts. However, they can only control the constitutional validity of judicial decisions. The administrative courts control the respect of constitutional rights by the public administration on *ultra vires* grounds. An *ultra vires* action aims at annulling an administrative decision when this is supposed to violate a legal provision [*règle de droit*].

The Constitution delineates the powers of the legislator and the executive with regard to public liberties. Article 34 attributes to the legislator the power to define fundamental guarantees for the exercise of public liberties, and to determine the right to vote (Art. 3), the principle of judicial authority, the protection of individual freedom (Art. 66), the freedom of administration for local communities (Art. 72) and the special structure of the overseas territories (Art. 74).

---

naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport [Protection of fundamental rights in the digital age. A comparative study to the freedom of information and of communication and privacy in Sweden, Germany, France, Belgium, The United States of America and Canada], Tilburg, Katholieke Universiteit Brabant, 2000, 255 p.

[5] See Decision No. 71-44 DC of 16 July 1971.

[6] Conseil Constitutionnel, *Human Rights and Public order, the main criteria for restricting human rights in the judicial practice of constitutional law*, 8th Seminar of Constitutional Courts, Erevan, 2-5 November 2003, http://www.conseil-constitutionnel.fr/dossier/quarante/notes/libpuben.htm.

At first, the Constitutional Council opted for a strict interpretation of the role of the legislator with regard to public liberties,[7] but this role has been expanded by broadening the concept of 'fundamental guarantees', which now includes all the necessary elements for the exercise of the liberty. The legislator can define when the executive power lacks authority, and it is competent to take certain measures in exceptional circumstances in order to protect Public Order.[8] In addition, the legislator has been attributed the power to conciliate the respect of constitutionally protected individual liberties with the protection of Public Order, whenever it appears necessary to safeguard constitutional rights and principles. However, he can never impose a prior restriction to the exercise of a right or restrictions to vested interests (except when they have been illegally acquired or when it is necessary for the carrying out of an objective with constitutional value).

The French constitutional system is monist and integrates international norms directly into the legal system whenever these have a direct effect. The Constitutional Council considers itself not competent to check the conformity of laws to treaties, and leaves this task to the judicial and administrative courts. In 2004, however, the Constitutional Council has changed its position with regard to European Directives. The Council now accepts that it is competent to check the conformity of a law impementing a Directive with the Directive itself (but not with the Constitution). It recognises the superiority of European norms with regard to the Constitution, in accordance with the jurisprudence of the European Court of Justice (see *infra*, section 4.3).

Finally, regarding the horizontal effect of the constitutional rights, an indirect horizontal effect exists through the interpretation by ordinary courts of general principles in conformity to the Constitution, but direct horizontal effect remains subject to the intervention of the legislators.[9]

4.2. History of digital constitutional rights

The French Government has been very active in promoting the information society since the year 2000. Four developments have to be mentioned in this respect: the inter-ministerial committee, the RE/SO 2007 Action Plan, and the creation of two specific organisms related to the information society, the Forum of Internet Rights [*Forum des droits sur l'Internet*] and ADAE, the Agency for the Development of Electronic Administration [*Agence pour le Développement de l'Administration Electronique*].

The Inter-ministerial Committee for the Information Society, created in 1998, is in charge of defining the major policy orientations and action priorities for the integration and the development of new technologies. It evaluates the initiatives and the state of the development of the information society, and it intervenes in technical, social, and legal questions relative to ICT. The committee is established for a defined period of time and works on a specific theme. So far, these committees have worked on issues such as the entry of France into the information society (1998), electronic administration and the foundations of an information society in solidarity (1999), the public effort of research (2000), and Internet and family (2003). Since July 2006, a new committee is working on the needs of 'Quantity, quality, accessibility, and security'. The objectives of this new committee are to improve the number of Internet users and the quality of their Internet connection through developing WiFi networks and mobile Internet, to develop e-administration, and to protect Internet users against cybercrime and abuses.[10]

At the end of the year 2000, a specific non-profit organisation was created, charged with the task to reflect upon legal concerns raised by the Internet: the Forum of Internet Rights [*le Forum des droits sur l'Internet*]. Its mission is threefold: to concert the different actors of the society, to inform and to make the general public aware of the information society, and to cooperate at an international level. It aims at constructing the *civilité* on the Internet. This organism only consists of members of civil society (such as Internet users, academic professors, professional organisations). In order to guarantee the independence of their recommendations, there are no state officials amongst the members, but public administration collaborates in its activities.

[7] Decision No. 59-1 FNR of 27 November 1959.
[8] Decision No. 85-187 DC of 25 January 1985.
[9] Constance Grewe,'Rights and Fundamental Freedoms', in: R. Blanpin (ed.), *International Encyclopedia of Laws, Constitutional Laws, France* (Deventer, Kluwer law and taxation publ.), p. 237.
[10] See http://www.internet.gouv.fr/.

Permanent reporters from the Independent Administrative Agencies are also represented in the workshops and are informed of the work of the organisation. It is part of the European Internet co-regulation network and it is financed by public subsidies and by contributions of its members. The Forum of Internet Rights has been very active and has issued several reports on privacy, intellectual property, hyperlinks, e-commerce, electronic archiving and electronic signatures, harmful and illegal content, labour relationships and the Internet, e-democracy, conflict resolution on the Internet, and e-administration. Its recommendations are usually followed by the legislators, for examples regarding topics such as labour relations and the Internet, data retention in electronic communications, hyperlinks, electronic archiving, harmful content, e-voting, the disclosure of public data, alternative dispute resolution and the Internet, and e-administration.

Following up Prime Minister Jospin and his Action Plan, Prime Minister Raffarin adopted a new plan in 2002, named 'RE/SO 2007, For a Digital Republic in the Information Society' [*Pour une République numérique dans la Société de l'Information*].[11] This Plan concerns all different levels of the information society and proposes measures for a more effective development of its infrastructures (equipments, Internet access, legal framework) and its uses. It wants to streamline the actual framework regulating the Internet, restore the confidence of Internet users, and clarify the liability of the different actors of the information society.

A first achievement has been made by creating a new Agency to take responsibility for the development of e-administration, viz., ADAE, the Agency for the Development of Electronic Administration. Its work gave way to the Act to Simplify the Law[12] [*Loi de simplification du droit*] in 2004 and to an Ordinance relative to electronic communications between users and administrative bodies[13] [*Ordonnance relative aux échanges entre les usagers et les autorités administratives*] in 2005. Both initiatives have given an important impulse to the development of e-administration and e-processes.

In the legal field, three important developments have to be mentioned. First, the influence of the European Union on French law. The bulk of adaptation of French Law to the concerns raised by new technologies has been achieved through transposing European directives. A complete reform of contract law has been carried out since the year 2000, in order to acknowledge the equivalence of paper-based and electronic documents. As a result, several provisions of the Civil Code have been modified.[14] The Data Protection Act has been completely reviewed and adapted to Directive 95/46/EC. The Electronic Communications and Audiovisual Communications Services Act[15] transposed the Directives of the 'Telecom Pack', modifying the Post and Communications Code, which is now named the Post and Electronic Communications Code, and the Act of 1986 relative to the freedom of communication. The Trust in the Digital Economy Act [*Loi pour la confiance dans l'économie numérique*][16] of 2004 has implemented a general framework for regulating Internet commercial exchanges, modifying the architecture of the Media Law by introducing a general category of communication, 'electronic public communication', divided in two sub-categories, 'audiovisual communications' and 'on-line public communications', and by solving some important questions related to Internet relationships. Finally, Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society has just been transposed in August 2006.[17] All these new laws provide a

[11] See http://www.internet.gouv.fr/.
[12] Law No. 2004-1343 of 9 December 2004 on simplification of the law [*Loi n°2004-1343 du 9 décembre 2004, de simplification du droit*], *JO* No. 287 of 10 December 2004 p. 20857.
[13] Ordinance No. 2005-1516 of 8 December 2005 on electronic exchanges between public agencies and users [*relative aux échanges électroniques entre les usagers et les autorités adminisitratives*], *JO* No. 286, 9 December 2005, p. 18986.
[14] Act No. 2000-230 of 13 March 2000 for adaptating the Evidence Act to information technologies and on electronic signatures [*portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique*], *JO* No. 62 of 14 March 2000, p. 3968.
[15] Act No. 91-646 of 10 July 1991 on the secrecy of electronic communicactions [*Loi relative au secret des correspondances émises par la voie des communications électroniques*], *JO* 13 July 1991.
[16] Act 2004-575 of 21 June 2004 on Trust in the Digital Economy [*Loi 2004-575, du 21 juin 2004 pour la confiance dans l'économie numérique*], *JO* No. 143, 24 June 2004, p. 11168.
[17] Act No. 2006-961 of 1 August 2006 on copyright and related rights in the information society [*relative au droit d'auteur et aux droits voisins dans la société de l'information*], *JO* No. 178 of 3 August 2006, p. 11529.

framework in which the exercise of public liberties in the information society is further described and defined.

Second, there is a development with regard to the balance between privacy and security. Specific issues concerning this balance have been raised through the enactment of the Daily Safety Act,[18] the Public Safety Act,[19] and the Antiterrorism Act[20], e.g., in the field of vehicle searches and seizures, public video surveillance, and accessing and processing passenger and traffic data. All these initiatives have in common that derogations to the right of privacy tend to be broadened in favour of an increased public control for the needs of public safety.

Finally, an initiative and a debate have taken place on the implementation of an electronic Identity Card. The Forum of Internet Rights issued a report to Prime Minister Sarkozy on 16 June 2005 following a large public debate. This report reveals that the public worries about creating a unique ID and about the security of the new card. The French Data Protection Authority, the *Commission Nationale Informatique et Libertés* (CNIL), has been consulted, as the electronic cards are intended for identifying citizens not only by their civil status and the document related to it, but also through biometrics, which raises extra protection concerns.[21] No concrete measures have been taken so far, apart from the Electronic Passport, created in response to the obligations contained of European Regulation 2252/2004 of 13 of December 2004.[22]

4.3. Changes in the constitutional system

Constitutional revisions are not unusual in France. Since 2000, several changes have been made. We will first look at reforms since 2000, and then turn to the case law of the Constitutional Council [*Conseil Constitutionnel*] that has brought some of the most important changes.

4.3.1. The constitutional reforms

None of the constitutional changes after 2000 has altered the constitutional system in a fundamental way. The constitutional law No. 200-964 of 2 October 2000 reduced the number of years of the President's term from seven to five; constitutional law No. 2003-267 of 25 March 2003 created a constitutional basis for the European arrest warrant; constitutional law No. 2003-276 of 28 March 2003 enabled a decentralised organisation of the Republic; and constitutional law No. 2005-205 of 1 March 2005 concerned an Environmental Charter.

A fifth constitutional law, viz. No. 2005-204 of 1 March 2005, on the modifying title XV of the Constitution would without any doubt have changed the French constitutional system if the European Constitution had been approved by the French people. The change would have permitted the National Assembly and the Senate to lodge an appeal before the Court of Justice of the European Communities for violating the principle of subsidiarity.[23]

4.3.2. Evolution of the jurisprudence by the Constitutional Council

The two most important constitutional changes and evolutions have been due to the case law of the Constitutional Council: the examination of constitutional revisions by the Constitutional

[18] Loi No. 2001-1062 of 15 November 2001 relative to daily safety [*relative à la sécurité quotidienne*], *JO* No. 266 of 16 November 2001, p. 18215.
[19] Act No. 2003-239 of 18 March 2003 for internal safety [*pour la sécurité intérieure*], *JO* No. 66, 19 March 2003, p. 4761.
[20] Act No. 2006-64 of 23 January 2006 on the fight against terrorism and with various disposals on security and border controls [*relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers*], *JO* No. 20, 24 January 2006, p. 1129.
[21] CNIL, CNIL Position on national ID card and biometrics [*Position de la CNIL sur la carte nationale d'identité et la biométrie*], 31 May 2005, available at http://www.cnil.fr/index.php?id=1773.
[22] The Regulation has been transposed through Decree No. 2005-1726 of 30 December 2005 on electronic passports [*relatif aux passeports électroniques*], *JO* No. 304 of 31 December 2005, p. 20742.
[23] Article 88-1 of the Constitution, as modified by a constitutional law, states that the Republic 'can participate in the European Union through the conditions provided by the treaty that establishes a Constitution for Europe, signed on 29 October 1994'. The new Article 88-5 stipulates that '[a]ny proposition for law authorising the ratification of a treaty regarding the accession of a State to the European Union and the European Communities is submitted to a referendum by the President of the Republic'.

Council, and the relation between the international legal order and the national legal order, especially regarding the hierarchy of legal norms.

Constitutional revisions by the Constitutional Council

The possibility to examine constitutional revisions by the Constitutional Council has always been a subject of debate. If the Constitutional Council is competent to examine the constitutionality of ordinary law, should then the Constitutional Council also be able to check laws that change the constitution with regard to fundamental constitutional norms, which cannot be revoked? A first response had been given during the constitutional revision of 25 June 1992 that prepared the way for ratifying the Maastricht Treaty. The Constitutional Council confirmed that the constitutional power is sovereign 'with reservations, on one hand, for the limitations regarding the periods in which a revision of the Constitution can be enacted or pursued (…) and, on the other hand, respecting the prescriptions of article 89 that states that 'the constitutional form of the republic cannot be the object of revision''[24].

The reservation made was important and suggested possible limits to constitutional revisions due to the existence of a kind of 'supraconstitutionalism' [*supraconstitutionnalité*], that always has to be respected. Referring to this 'supraconstitutionalism', sixty senators questioned a subsequent constitutional revision regarding the decentralised organisation of the republic. In their appeal, they held that the indivisibility of the Republic was part of the constitutional form of the republic. The Constitutional Council, in its decision of 26 March 2003,[25] denied it had jurisdiction, while specifying that 'it follows not from article 61, nor from article 89, nor from any other constitutional provision, that the Council has the power to pass judgment on a constitutional revision'. The question has therefore been decided. The Constitutional Council does not have the possibility to supervise the constitutional power that is exerted by way of referendum or by Congress.

The second evolution in the constitutional system concerns the hierarchy of the norms in the national legal order, the relationship between the constitution and European law, and the powers of the Constitutional Council. In this period, the Constitutional Council has clarified that laws that transpose European directives benefit from a form of constitutional immunity on the sole condition that they do not contradict an explicit rule of the constitution. Also, the Constitutional Council has considered itself competent to examine the compatibility of the law transposing the directive with the directive itself.

The constitutional immunity of laws transposing European directives

The Trust in the Digital Economy Act intends to regulate the rules applying to the Internet and transpose in the national legal order European directive 2000/31/EC of 8 June 2000 regarding electronic commerce. The new act has triggered a debate about the liability of service providers [*hébergeurs*].[26] The act specified that these are not liable when they do not have knowledge of illegal activities or illicit information, or when, as soon as they receive such knowledge, they immediately act by removing the information or blocking access to it. These provisions were contested and brought before the Constitutional Council, since they allowed for a form of private censorship on the part of hosting providers. Before the Council, this was held to be incompatible with the freedom of information, the rights of the defendant, and the right to a fair trial. In its decision of 10 June 2004, the Constitutional Council observed that provisions in the Act were literal transpositions of the electronic-commerce directive. [27] Striking down transposing provisions that are necessary and in line with the directive would make transposition impossible. In the terms of Article 88-1 of the Constitution, 'the Republic participates in the European Communities and the European Union that has been formed on the basis of States that have freely chosen through

[24] Decision No. 93-312 DC Maastricht II of 2 September 1992.
[25] Decision No. 2003-469 DC of 26 March 2003 on the constitutional revision regarding the decentralized organisation of the Republic.
[26] Natural persons or legal bodies that provide, even free of charge, access to the public to storage of signals, whether they be in written form, images, sound, or any other form designated by the addressee, by on-line public communication services.
[27] Decision 2004-496 DC of 10 June 2004 on the Trust in the Digital Economy Act.

treaties to exert communally a certain part of their competences'. Thus, for the Constitutional Council, transposing in the national legal order a directive is the result of a constitutional requirement that cannot be departed from, unless on the basis on an explicit rule in the constitution itself. In the absence of such a rule, it is up to the European courts, in pending cases through prejudicial questions, to examine conformity of European directives with the respective treaties and with fundamental norms.

The 2004 decision of the Constitutional Council teaches that international norms, at least those of the European Community, rank higher than the constitution in the national legal order. This is expressly the reverse of what the Council had stated before, but it is in line with the case law of the Court of Justice of the European Communities, which denies to national jurisdictions, including constitutional courts, the power to declare derived legislation invalid[28]. European directives share the constitutional immunity that is attached to European law.[29] Only the Court of Justice of the European Communities and the Court of Justice can carry out conformity checks. The Constitutional Council refuses to express itself on legal provisions that implement directives with precise and unconditional terms. The Council has made one important reservation: the transposition of a directive cannot be allowed if there is a provision in the constitution that goes expressly against it.[30]

Due to the growing importance of European law and the increase in transposition laws, the Constitutional Council has had multiple occasions to reaffirm its position.[31] It has had to draw full conclusions. Indeed, for a law to benefit from the aforementioned constitutional immunity, the Council must verify that it truly transposes the directive. Going a step further, that Constitutional Council has affirmed that it has the possibility to examine whether a transposition law has correctly implemented the European directive itself.

The examination of the compatibility of the transposition law and the directive

In 2006, the Council confirmed its competence to examine the compatibility of transposition laws and their directives. In decision No. 2006-535 DC of 30 March 2006 on the law regarding equal opportunities, and again supported by Article 88-1 of the Constitution, the Council repeated that the transposition of the directives in the national legal order is a constitutional requirement. It asserts therefore that it is not up to the Council, when it is has a case pending on the basis of Article 61 of the Constitution, to examine the compatibility of a law and the provisions of a directive this law has not the intention to transpose (cons. 28). *A contrario*, it should be inferred that the Council is competent to decide on the compatability of a law and the directive it transposes. In that decision, the Council indicates aptly the difference between European law and international law, confirming its traditional jurisprudence[32] that it is not competent to check the conformity of a law to a treaty (cons. 27).

Decision No. 2006-540 DC of 27 July 2006 on the law regarding copyright and derivative rights in the information society gave an occasion to the Council to specify the range of its competences while exercising its supervision (cons. 16 et seq.), when the law that is at issue is in fact a transposition law. It is affirmed, this time very explicitly, that it is up to the Council to guard the respect for Article 88-1 of the Constitution, that is to say, a compatibility should exist between the transposition law and the directive, with two limitations. The first, already existing limitation has already been mentioned: the transposition of a directive cannot expressly contradict the Constitution. The second limit is new. The Council asserts that the period granted to it to examine the constitutionality of a law makes it impossible to bring a case before the Court of Justice of the

[28] Commentary on the decision in *Les cahiers du Conseil constitutionnel*, No. 17, p. 5, available at http://www.conseil-constitutionnel.fr/cahiers/ccc17/jurisp496.htm.
[29] *Ibid.*
[30] For the commentator in the journals of the Constitutional Council, it 'cannot be a judicial construction, but it should be an explicit pronouncement in the Constitution that is embedded in the "constitutional block" [*bloc de constitutionnalité*], such as the definition of the electoral body by Article 3 of the Constitution of 1958 or the wording in Article 6 in the Declaration regarding the criteria for access to public services' (*ibid.*).
[31] Decisions No. 2004-497 of 1 June 2004 on the Electronic communications and audiovisual services Act, cons. 18; 2004-498 DC of 29 July 2004 regarding bio-ethics, cons. 4; 2004-499 DC of 29 July 2004 regarding the protection of natural persons in regard to the protection of their personal data and changing Act No. 78-17 of 6 January 1978 regarding informatics, data bases and freedoms, cons. 7 and 8.
[32] See Decision No. 754 DC of 15 January 1975 on the Act regarding the voluntary interruption of pregnancy.

European Communities. As a result, it can only declare a legal provision to be not in conformity with Article 88-1 of the Constitution when it is overtly incompatible with the directive. In addition, its examination does not affect subsequent cases before the Court of Justice of the European Communities, which are brought before it by national jurisdictional authorities.

Since 2000, the evolution of the jurisprudence of the Constitutional Council has altogether been very important. It has caused real changes in the constitutional system, and the powers of the Council have been considerably altered in the field of European law.

However, the analysis of the jurisprudence related to privacy-related rights (section 4.4) and communication-related rights (section 4.5) reveals that concerns related to new technologies are rarely put forward to the Constitutional Council, or before other courts with a reference to constitutional rights. As a consequence, the subsequent section will not only elaborate on constitutional decisions and the scarce relevant jurisprudence from the courts but also on the main decisions of the CNIL.

4.4. Privacy-related rights

4.4.1. Privacy and data protection

The right to privacy does not appear as such in the constitution or in the 'constitutionality block' (see section 4.1). *A fortiori*, nothing is found therein on the protection of personal data.

It is the Constitutional Council that has affirmed that the right to privacy deserves constitutional protection. It has done this implicitly in its decision of 12 January 1977 on the search of vehicles,[33] and subsequently more clearly by adhering to the principle of individual liberty of Article 66 of the Constitution.[34]

Since 1999, the constitutional ground for protecting privacy is Article 2 of the Declaration of Rights of Man and the Citizen, and no longer Article 66. The Constitutional Council affirmed in decision No. 99-416 DC of 23 July 1999 on the law regarding the creation of universal health insurance that 'in terms of Article 2 of the Declaration of Rights of Man and the Citizen, 'the goal of every political association is the conservation of natural and imprescriptible rights of Man. Those rights are freedom, property, security and the resistance to oppression', and that the freedom proclaimed by this article implies the right to privacy.'' This phrasing has been repeated multiple times at subsequent decisions.

The right to privacy is frequently invoked before the Constitutional Council in (a) cases pertaining to the processing of personal data, and (b) matters in which new technologies are being used for the surveillance of persons.

a. Questions regarding the handling of personal data

It is indeed within the framework of the privacy right that constitutional issues regarding data protection have been raised. The Court always first recognises the existence of the right to privacy, and then goes on to insist on the role of the legislator in this area based on article 34 of the constitution.[35] It is the legislator that has to establish the necessary guarantees citizens need when exercising their civil liberties. In practice, however, the Constitutional Council has not been very demanding with regard to the level of precision that legal regulations need to have. In order to uphold certain regulations with privacy implications, the Council insists on the fact that the

[33] Decision 76-75 DC of 12 January 1977 on the Act authorising the search of vehicles as part of an investigation in criminal matters.

[34] Article 66: '(…) The judicial authority, guardian of individual freedom, assures the respect for this principle under the conditions defined by the law.' Decision No. 94-352 DC of 18 January 1995 on the Act regarding orientation and the programming of security measures; Decision No. 97-389 DC of 22 April 1997 on the Act regarding several measures on immigration, and Decision No. 98-405 DC of 29 December 1998 on the financial Act 1999.

[35] Article 34: 'The law is voted by Parliament. The law fixes the rules concerning: civil rights and the fundamental guarantees accorded to the citizens for exercising their civil liberties; the subjections imposed on persons and their goods by the national defence [*Défense Nationale*]; (…).'

legislator has not deviated from the provisions that protect individual freedom in the 1978 Data Protection Act.[36]

This Data Protection Act (*loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*) has therefore received a special status, viz., the status of 'laws that ensure the protection of a constitutional value,'[37] but this has little when examining the constitutionality. In fact, one could say that the recognition of the 1978 Data Protection Act has allowed the Council in practice to be not too demanding with respect to the level of legal regulation in other Acts that have an impact on the right to privacy. The Council often insists on the fact that the text of the law foresees that a decree [*decrét*] enacted by the Council of State [*Conseil d'Etat*], after advice of the CNIL, will set the guarantees surrounding the processing of data,[38] and that this will ensure that the right to privacy is guaranteed. The Council thus finds support in the intervention of the Data Protection Authority (CNIL) installed by the 1978 Data Protection Act for giving these submitted texts a constitutional stamp. One could, however, question whether this institution has the means to enforce its point of view on the regulatory authorities. The sheer existence of the 1978 Act seems to be a sufficient constitutional guarantee. The Council will seldom object to the processing of personal data unforeseen by law but deemed necessary, since the processing – once in operation – will at any rate have to respect the provisions of the 1978 Act .[39] An objection based on the lack of competence of the legislator to enable certain processing will seldom be acknowledged. As a matter of fact, it has only been invoked successfully once by the Council regarding the law of 6 August 2004 on the protection of natural persons in regards to the processing of personal data, which replaced the 1978 Data Protection Act.[40] The provisions that make it possible for firms or legal entities to create data bases with data on people suspected of fraud on behalf of other legal entities, has been invalidated based on these grounds (cons. 12).[41]

A similar latitude of the Constitutional Council can be observed with regard to its supervision of the motives invoked by the legislator to introduce new measures and with regard to the proportionality test between these measures and their stated objectives. The Council gives the legislator a wide margin of appreciation, since it is the legislator who has to reconcile the protection of public order, as a safeguard for the principles and legal rights of the constitution, with respect for privacy and other constitutional rights. In most cases, the Council finds justifications linked to the public interest (e.g., respect for the public order of measures relating to the entry and residence of foreigners) to be sufficient both at the moment when the processing of data is decided and when the processing of data is carried out.

Setting up the processing of personal data

Numerous types of setting up the processing of personal data have been submitted before the Constitutional Council. In the domain of security, it has validated the creation (or the legislative validation *a posteriori*) of several data bases. The files of the judicial police [*police judiciaire*] – Stic and Judex, used respectively by the services of the national police [*police nationale*] and by the state police [*gendarmerie*] – used to be regulated only by decree. This changed with the law devoted to internal security measures. The enactment of the law gave the Council the opportunity to express itself on the constitutional nature of these data bases. It found that these data bases

[36] Decision No. 92-316 DC of 20 January 1993 on the Act regarding the prevention of corruption and the transparency of economic life and public procedures, on the Articles 1 through 6; Decision No. 93-325 DC of 13 August 1993 on the Act regarding the control of immigration, on Article 36, and Decision No. 94-352 DC of 18 January 1995 on the Act regarding orientation and the programming of security measures, on Article 10.

[37] J. Boyer, 'Fichiers de police judicaire et normes constitutionnelles: quel ordre juridictionnel?', *Petites Affiches* 22 May 2003, No. 102, pp. 4 et seq.

[38] Decision No. 84-172 DC of 26 July 1984 on the Act regarding the supervision of the structures for agricultural exploitation and the statute for leasing, on Article 7, and Decision No. 99-419 DC of 9 November 1999 on the civil solidarity pact.

[39] Decision No. 97-389 of 22 April 1997 on the Act regarding several measures concerning immigration, on Article 1 dealing with the certificates of service providers.

[40] Decision No. 2004-499 DC of 29 July 2004 on the Act regarding the protection of natural persons in regard to the handling of personal data and modifying Act No. 78-17 of 6 January 1978 on informatics, data bases and liberties.

[41] The fact that the Act deals with files for the purpose of private persons and not for the State has no doubt played an important role in this decision (see in the same decision, the refusal to invalidate the rule on files in combating certain activities of private persons, cons. 13).

do not form a disproportionate infringement on the right to privacy in comparison with the stated objective: safeguarding the public order and the investigation of offenders.[42]

The Council came to an identical conclusion with regard to the creation of an automated national data base of sexual offenses. This data base includes the most recent addresses of sexual offenders, including young sexual offenders. The stated objective in this case was the protection of the public order, the necessity of investigation, and the prevention of new crimes.[43]

In immigration matters, the Council has also considered in its decision of 22 April 1997[44] that the taking and processing of digital fingerprints of foreigners requesting a residence permit after three months of stay since entering the country or who are in an illegal situation or are confronted with an expulsion order, is not an excessive infringement of individual liberty and therefore does not violate the Constitution.[45] In the same domain, the Council has noted, in its decision of 20 November 2003,[46] that the processing of personal data by mayors of persons wishing to accommodate a foreign person and of their reasons to do so, was justified in the light of all the guarantees incorporated in this measure.

In the medical domain, in 2004, the Council affirmed that the creation of a personal medical file – with a list of diagnostic and therapeutic elements necessary for an integrated-care approach of patients – is not an excessive infringement on the right to privacy in the light of the stated objectives, namely improving the quality of medical care and reducing the financial imbalance of the health insurance system.[47] The Constitutional Council also left a wide margin of appreciation for the legislator with regard to possible consultations by third persons of these medical files.

The consultation of data bases

New measures that allow the consultation of already existing data bases for new purposes have rarely been put in doubt by the Constitutional Council. The Council has, for example, not found unconstitutional elements in measures that allowed the consultation of police records for administrative purposes.

The law for internal security, which was brought before the Council in 2003, allowed the consultation of data collected in the context of a police investigation for certain specific administrative purposes (e.g., deciding on the employment of civil servants participating in the mission of the sovereignty of the State or in positions that concern security or defense, and in investigations when a request for French nationality is made).[48] The Constitutional Council has considered that these consultations do not pose any specific constitutional problem as they serve a legitimate purpose and happen within the strict boundaries of the protection of individual persons and of the fundamental interests of the nation. The persons concerned are informed and the information used is just one of the elements in the decision taken. The Council has specified, at this occasion, that the principle of finality, which is a fundamental principle in data protection, does not have a constitutional value and cannot be opposable to the legislator.

The Council, while accepting the principle of administrative use of police records, emphasised nonetheless that certain guarantees should be upheld and that certain abuse should be prevented, for example, unnecessary consultations or insufficient guarantees, notably concerning the confidentiality of sensitive information. The Council also added some interpretative reservations to its decision, such as no infringement on the right of foreigners or the 'right to be forgotten' for minors.

Other consultations have also been validated by the Constitutional Council,[49] but the only case in which the Constitutional Council has considered the consultation of an existing data base

[42] Decision No. 2003-467 DC of 13 March 2003 on the Act for internal security, cons. 20.
[43] Decision No. 2004- 492 DC of 2 March 2004 on the Act regarding the adaptation of the justice system to evolution in crime, cons. 76 and following.
[44] *Supra*, n. 34.
[45] Decision No. 97-389 of 22 April 1997 on the Act regarding several measures concerning immigration, on Article 3 of the Act.
[46] Decision No. 2003-484 DC on the Act regarding the control of immigration and regarding the residence of foreigners and regarding nationality.
[47] Decision No. 2004-504 DC of 12 August 2004 on the Act regarding health insurance; see, in particular, recital 8. See also Decision No. 99-416 DC of 23 July 1999 on universal health coverage.
[48] Decision No. 2003-467 DC of 13 March 2003 on the Act for internal security.
[49] See for the consultation by the Prefect [*Préfet*] of the files of corporations in charge of the distribution of water, gas,

unconstitutional concerned the hypothesis in which another principle than the right to privacy was in question. It was on the basis of the right of asylum, which forms part of the Preamble of the 1946 Constitution, that the Council refused, in a decision of 22 April 1997,[50] agents of the Ministry of Interior Affairs and the state police to access the files of digital fingerprints kept by the OFRPA, the French Office for the Protection of Refugees and Stateless Persons [*Office Français de protection des réfugiés et des apatrides*].

b. Problems related to the use of new surveillance technologies

New surveillance technologies have not triggered strong constitutional debates. Questions relating to location data or identification of persons through biometrics (*cf.*, section 4.4.3) have not been presented to the Constitutional Council yet. Only three techniques have been the object of jurisprudence by the Council: video surveillance, automated photography, and the placement under electronic surveillance (electronic bracelet). All those techniques are based on the processing of personal data. The Council has had to pronounce itself on the technique being used and on the associated processing system.

The Constitutional Council had to decide upon questions regarding video surveillance in 1995 during the examination of the law on the orientation and the programming of measures regarding security.[51] It considered that the regulation does not constitute a disproportionate infringement of constitutional liberties, in particular the right to privacy as part of that individual liberty, in relation to the stated objective – preventing attacks on the public order and the investigation of infractions. The legislator could therefore allow the agents of the State in the departments to authorise the installation of video surveillance systems that would transmit and record images of the public domain and other places open to the public, as soon as these systems follow the guarantees that ensure the safeguarding of individual liberties. These guarantees concern informing the public, prohibiting the capture of images of private spaces, the intervention by a commission that renders independent advice on the installation of the systems, an exact definition of the persons involved in exploiting the system, the right to access, the right to appeal offered to the persons on tape, a limited duration that the images will be kept, and sanctions surrounding the use of this technique.[52]

Automated photography no doubt infringes the right to privacy to a lesser extent than video surveillance. Nonetheless, this technique is also dangerous, since it requires in general the processing and consultation of personal data that allow for an identification of persons and photographic objects. This issue was at stake in a case examined by the Constitutional Council in its decision No. 2005-532 DC of 19 January 2006 on the law concerning the battle against terrorism and concerning security measures at borders. Article 8 of this law broadened and specified the conditions under which automated photography can be implemented. The technique exists since the law of 18 March 2003 on internal security, of which the constitutionality had, at that time, not been contested. In 2003, automated photography by use of fixed or mobile devices was limited to cars, essentially with the goal to combat car theft. In 2006, the goal was broadened, but it was also more specified in the text of the law. It is now twofold: the objective of the administrative police – the prevention of the disturbance of public order – and the objective of the judiciary police – fighting certain offenses. At the same time, the rules regarding access to the data and the storage period of the data are clearer. The greatest innovation lies in the possibility to photograph not only vehicles, but also the passengers of vehicles. The Constitutional Council did not find this a disproportionate infringement of the right to privacy, considering the guarantees: the objective was more specific compared to the previous text, the storage period of the images is limited, access to the files is only allowed for identifying stolen vehicles (information system of Schengen), and the images can only be further used in case of a positive identification.

---

electricity, and telephone of professional realtors in order to search for useful information on vacant houses, Decision No. 98-403 DC of 29 July 1998 on the Act of orientation concerning the battle against exclusion.

[50] Decision No. 97-389 of 22 April 1997 on the Act regarding several measures concerning immigration.

[51] Decision No. 94-352 DC of 18 January 1995 on the orientation and the programming of measures regarding security.

[52] The Constitutional Council invalidated nonetheless the regulation that foresaw that the silence of the administration during four months equated authorisation.

Finally, there is case law of the Council regarding the placement under electronic surveillance of people, through an electronic bracelet. Again, the measure was considered compatible with the right to privacy and, more in general, the right to individual freedom.[53] In its 2002 judgment, the Council insisted on the fact that the measure had the purpose of avoiding a provisional detention and required the consent of the person concerned (cons. 85). The electronic bracelet could therefore not be seen as presenting an unnecessary cruelty. In consideration 19 of the 2005 desision, the Council insisted on the goal of preventing recidivism through the administration of the punishment for certain strictly defined infractions. The legislator intended to guarantee public order and security, which are necessary to maintain constitutional values. The Constitutional Council also noted the fact that the consent of the person concerned should be obtained, and it considered this measure therefore not to disproportionate to the limits on personal freedom.

4.4.2. Inviolability of the home

The right to respect for the privacy of the residence or, rather, for the inviolability of the home is the object of constitutional protection. The Constitutional Council has, in its first decisions, as it has done for the right to privacy, asserted that this right is part of the individual freedom guaranteed by Article 66 of the Constitution.[54] The inviolability has progressively become more autonomous and is now protected on the grounds of Articles 2 and 4 of the Declaration of Rights of Man and the Citizen.[55]

In relation to new technologies, this right has almost never been invoked. The hypotheses (already very limited) in which inviolability have been cited before the Council concern the regulations regarding house searches[56] or domiciliary visits,[57] but not questions linked to new technologies.

4.4.3. Inviolability of the body

General

The inviolability of the human body is a principle that has featured in the Civil Code [*Code civil*] since the bio-ethics laws of 29 July 1994. From a constitutional point of view, it is not protected as such, but it is connected to the principle of dignity proclaimed by the Preamble of the 1946 Constitution. The Council has thus affirmed in its decision of 27 July 1994[58] that safeguarding the dignity of the person against any form of enslavement or degrading treatment is a constitutional principle (cons. 2). The Council also considered that 'the supremacy of the human person, the respect for the human being from the beginning of life, the inviolability, the integrity, and the absence of a patrimonial nature of the human body, as well as the integrity of the human race (…) intend to assure the respect for the constitutional principle that guards the dignity of the human person' (cons. 18). The inviolability of the human body is therefore what one calls a 'guarding principle' [*principe sentinelle*], a principle that does not have a constitutional status on its own, but which guarantees other constitutional principles. In 1994, the Council did not consider this principle violated when the petitioners asserted that the possibility to do research on embryos constituted a manifest violation.

[53] The Council has decided three times on the subject: Decision No. 2002-461 DC of 29 August 2002 on the Act concerning orientation and the programming of justice; Decision No. 2005-527 DC of 8 December 2005 on the Act concerning the treatment of recidivism in criminal matters; Decision No. 2004-492 DC of 2 March 2004 on the Act concerning the adaptation of justice towards the evolution in crime. In 2004, only questions concerning the criminal procedure were addressed.
[54] See Decision No. 83-164 DC of 29 December 1983 on the financial Act for 1984 and Decision No. 90-281 DC of 27 December 1990 on the Act concerning the regulation of telecommunications.
[55] Decision No. 2004-492 of 2 March 2004 on the Act concerning the adaptation of justice towards the evolution in crime, cons. 4.
[56] See, for example, Decisions No. 83-164 DC of of 29 December 1983 on the financial Act for 1984, No. 90-281 DC of 27 December 1990 on the Act concerning the regulation of telecommunications, and No. 96-377 DC of 16 July 1996 on the Act intending to support the battle against terrorism.
[57] Decision No. 93-325 DC of 13 August 1993 on the Act concerning the control of immigration.
[58] Decision No. 94-343-344 DC on the bio-ethics laws of 29 July 1994.

The principle has been invoked before the Constitutional Council only two times since, with respect to the law revising the bio-ethics laws[59] and the law of 20 September 2003 for internal security. The first decision concerned the possibility of patents on parts of the human body, but this was quickly resolved as the law did nothing more than transpose a directive into the national legal order (*cf.,* section 4.3.2).[60] When the Council considered a case in 2003,[61] the petitioners asserted that the inviolability of the human body was infringed when a judiciary police officer is given the power to take an external sample of any person able to give information on the facts in a certain case or if there are sufficient grounds to assume that the person concerned may have committed a criminal act, and that this procedure would allow for scientific and technical examination and comparison of the sample and traces found at a crime scene. The Council rejected these arguments, since taking an external sample does not imply any internal bodily intervention, nor is it a painful procedure or does it infringe the personal dignity (cons. 55). In fact, for DNA testing, a simple sample of saliva suffices.

The principle of the inviolability of the human body has not been invoked in relation to new technologies for identifying persons. A debate has not yet taken place in this domain, since the right to privacy and the right to personal freedom have been at the forefront (see section 4.1.1 under b), and since no relevant cases have yet been put forward to the Council. The controversy on biometrics as a means for identification has been raised within the Commission on Informatics and Liberty [*la Commission informatique et liberté*] and has now begun to reach the courts.[62]

Bio-ethics laws

In 1994, three Bio-ethics Acts were adopted after long debates in Parliament:

- law No. 94-548 of 1 July 1994 relative to the processing of personal data for purposes of health research;[63]
- law No. 94-653 of 29 July 1994 relative to the respect of human body;[64]
- law No. 94-654 of 29 July 1994 relative to donation and use of parts and products of the human body, to medical assistance for procreation and to pre-birth diagnostics.[65] This law foresaw its own modification in the light of future developments, which were realised in 2004 (see below).

In the debate over these laws, two different conceptions of the human body were contested: one based on human dignity and the non-patrimonial nature of the body, and one based on utilitarianism. The bio-ethics laws are the result of a compromise in which the first approach is dominant, and they incorporate into French law the main principles of the inviolability of the body. Human dignity is conceived as transcending the human being, contrary to the British meaning based on the freedom to make use of one's own body.[66]

---

[59] Decision No. 2004-498 DC of 29 July 2004 on the Act concerning bio-ethics.

[60] The Constitutional Council does not even mention in its Decision No. 2004-498 DC of 29 July 2004 the question of the conformity of the law with the principle of respect for human dignity; see the text of the action before the court at http://www.conseil-constitutionnel.fr/decision/2004/2004498/saisine1.htm.

[61] Decision No. 2003-467 DC of 13 March 2003 on the Act regarding internal security

[62] Only one decision can be cited in this domain: the decision by the TGI of Paris on 19 April 2005.

[63] Act no 94-548 of 1 July 1994 relative to the processing of personal data with purposes of research in the field of health [*relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés]*, *JO* 2 July 1994. The conditions of processing have been recently specified by the CNIL: processing must only contain indirect personal data relating to patients, who can only be identified by their initials or a specific number; personal data must be collected directly from patients or by medical people; only limited categories of personal data can be collected; the CNIL must be informed of the purpose(s) and the function of the processing; the categories of persons who can process or access the data are strictly limited by the document issued by the CNIL. Furthermore, data controllers must provide information and ask for patients' consent in the form of notices adopted by the CNIL and included in the guidance. They also impose compulsory retention periods and security measures, and controllers must implement a security and confidentiality policy, as well as organise training sessions for employees who can access the data. Moreover, only coded or anonymous data relating to patients can be transferred outside the European Union. See H. Lebon, *French Data Protection Authority (CNIL) guidance concerning biomedical research*, 23 March 2006, available at http://www.twobirds.com/english/people/Helene_Lebon1.cfm.

[64] Act No. 94-653 of 29 July 1994 on the respect of the human body [*relative au respect du corps humain*], *JO* 30 July 1994.

[65] Act No. 94-654 of 29 July 1994 relative to the donation and use of parts and products of the human body, to medical assistance for procreation, and for pre-birth diagnostics [*relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal*], *JO* 30 July 1994.

[66] F. Dreifuss-Netter and G. Moutel, *Les lois de bioéthiques et leur réactualisation*, available at

As a consequence, the law can protect the individual also against himself, banning contracts related to the human body, whether they refer to the body in general or only to one part. This principle intends to avoid the creation of a market of human body parts such as exists in the United States, where women sell egg-cells on the Internet. The only exceptions lie in donations on the condition that they remain anonymous.[67] The bio-ethics laws of 1994 do not only introduce the general principles of protection of the human being but also regulate new medical activities (such as medical assistance to insemination and transplants), refuse dumping affecting public health, and to protecting individuals participating in medical research.

The enactment of a new bio-ethic law[68] in 2004 has provided an answer to two fundamental issues:

- therapeutic cloning, which is allowed, although cloning in general is forbidden;
- the conflict between non-patentability of the human genome and the need to stimulate research through patents on sequences of human genes. Research on embryos and embryonic cells has been forbidden, except in certain cases, but inventions arising from the technical application of a function of the human body have been allowed.

Finally, a Biomedicine Agency has been created. It aims at participating in the formulation of the regulation but also to control and follow up medical and biologic activities of its competences and to recognise practitioners and research protocols.

Processing biometric data

The use of biometrics is debated in France but has not been put forward to the Constitutional Council yet. CNIL's powers regarding biometric systems increased under the new data-protection law, since all biometric systems have to be authorised by the CNIL before implementation. The CNIL is thus dealing with the task of balancing the increasing pressure to use biometrics for identification purposes with the need to protect privacy.

Solutions will depend on the technology used and on the purposes of the processing. The CNIL is more willing to authorise processing based on hand geometry or iris recognition than on fingerprints, as such data cannot be collected as easily as fingerprints and thus are less dangerous for individual liberties. The CNIL approved a hand-geometry recognition system for a school dining hall, noting that the use of such a system better respected the rights of the individuals concerned than a fingerprint system. In addition, French police traditionally use fingerprints to identify offenders. The use of a non-fingerprint recognition system therefore guarantees that the data cannot be linked to police databases.

CNIL will only authorise processing based on fingerprints where such creation is justified by an undeniable security imperative. For example, it approved a fingerprint recognition system to allow employee access to secure areas of Orly and Roissy airports in Paris. However, it rejected a request by a hospital to implement a fingerprint recognition system in order to monitor and control its employees' working hours. The decision was based on the ground that the biometric data were stored in a data base, which is not a method that protects the data subject against inappropriate use of the data, and because the aim of better management of working hours, while legitimate, does not justify the collection and storage of fingerprints. Nevertheless, the processing may be authorised when the fingerprint template is solely stored in a personal item, e.g., a badge or smart card, because this limits the risk of function creep: a processing of identification data of website users was authorised because it incorporated an individual reader owned and controlled by the user.

In each case of biometric data use, the CNIL considers whether the use is adequate and proportionate to the purpose. Furthermore, although it agrees that in certain cases, biometric systems can be justified because of safety considerations, the CNIL requires adequate security measures, e.g., encrypting fingerprints stored in the data base. For example, the CNIL has

---

http://infodoc.inserm.fr/ethique/cours.nsf/bccd132de8453295c125685b004bb3a8/03b36f2ea90e3cf380256cb500370db5?OpenDocument.

[67] French movement for family planning, *A societal question: bioethics, adapting legislation* [Mouvement français pour le planing familial, *Question de société : bioéthiques, la révision des lois*], available at http://www.planning-familial.org/themes/theme16-bioethique/fiche01Precision01.php.

[68] Act No. 2004-800 of 6 August 2004 relative to bio-ethics [*relative à la bioéthique*], *JO* 7 August 2004.

accepted the implementation of biometric systems to control access to certain places for security reasons, including the offices of the French Central Bank.

4.5. Communication-related rights

The secrecy of communications is an essential part of the more general right to privacy in French law. Concerns raised by the protection of e-mail as private correspondence, the retention of traffic data, and the protection of anonymity have therefore been dealt with in the light of privacy rules (section 4.5.1).

Constitutional protection of freedom of expression is based on Art. 11 of the Declaration of the Rights of Man and the Citizen, and on two Acts of 1881 and 1886. The existence of these two legal regimes is not without problems. A complete reorganisation of the categories of communications has been called for, since different regimes exist for the written press and for audiovisual communications and the Internet does not fit either of them. Moreover, new legislation has been adopted with regard to the perpetration of press offenses through the Internet, the liability of webmasters regarding the content published by its users and the protection of minors against harmful content (section 4.5.2). However, most of the legal modifications are based on solutions given by jurisprudence, usually approved by the Constitutional Council.

4.5.1. Secrecy of communications

The object of right to secrecy of communications is to protect against fraudulently obtaining the content of a communication, not against the use of the information itself. This right is explicitly protected. Art. 1 of the Act No. 91-646 of 10 July 1991 relative to the secrecy of electronic communications,[69] as modified by Act No. 2004-669 of 9 July 2004,[70] stipulates that 'secrecy of mail issued through electronic communications is guaranteed by the law'. Article 32 paragraph 3 of the Post and Electronic Communications Code [*Code des postes et des communications électroniques]* compels webhosters to respect the secrecy of communications. Articles 226-15 and 432-9 Criminal Code (hereinafter: CC) prohibit the interception of correspondence, irrespective of the means of communication. Two types of conduct are criminally punishable: illegal wiretapping and recording (Art. 226-1 CC) and maliciously opening, destroying, delaying, or diverting correspondence sent to a third party, or fraudulently gaining knowledge of it (Art. 226-15 CC).

This protection is not absolute. In order to carry out criminal investigations, the examining magistrate [*juge d'instruction*] can command police officers competent to investigate crimes [*police judiciaire*] to intercept a private communication (Art. 100 to 100-7 Code of Criminal Procedure). This first exception has been broadened by Act No. 2004-204,[71] which extends the power of the police in the context of the fight against serious crime: wiretapping is now also allowed in the preliminary stage of investigation or in *flagrante delicto* cases, under the sole condition of prior authorisation by the judge of liberties [*juge des libertés*]. Wiretapping and recording of communications without prior consent are also tolerated when they are justified by national security or by a national interest.

The definition of the secrecy of communications is thus not limited to a special means of communication but refers to the guarantee of the secrecy of the communications as such. It has not been necessary to adapt the text to new technologies. Nevertheless, various specific concerns related to the Internet had to be solved. The integration of e-mails into the concept of private communication has implied acknowledging the private nature of this type of mail, which had been a point of important debate in the context of labour relationships. In response to terrorist

[69] Act No. 91-646 of 10 July 1991 on the secrecy of electronic communicactions [*relative au secret des correspondances émises par la voie des communications électroniques*], *JO* 13 July 1991.
[70] Act No. 2004-669 of 9 July 2004 on electronic communications and audiovisual communications services [*relative aux communications électroniques et aux services de communication audiovisuelle*], *JO* 10 July 2004.
[71] Act No. 2004-204 of 9 March 2004 for adapting justice to the evolution of crime [*portant adaptation de la Justice à l'évolution de la criminalité*], *JO* 10 March 2004, p. 4567.

attacks, an obligation to retain traffic data has been introduced, which had to fit within the right to secrecy of communications. Finally, the right to keep certain information secret is part of the right to privacy, and thus a balance between public interests and confidentiality had to be found in specific circumstances. We will now explain these issues in more detail.

E-mail as private correspondence

Important issues regarding the right to secrecy of communications in the field of new technologies have been discussed relative to the application of existing rules to electronic mails. The concerns raised by e-mail relate to the easiness of their interception and to the difficulty of proving infringements.

The Constitutional Council faced the question whether e-mail could be acknowledged as private correspondence. The Trust in the Digital Economy Act introduced a technical definition of e-mail messages given by Directive 2002/58/EC: any text, voice, sound, or image message sent over a public communications network that can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient. The avoidance of expressly mentioning e-mail as private correspondence by the French National Assembly has been understood by some parliamentarians as withholding the protection of the secrecy of communication from e-mail, and thus this matter has been referred to the Constitutional Council.

The Constitutional Council considered that the definition in the Trust in the Digital Economy Act, strictly technically speaking, does not restrict or affect the concepts of 'private correspondence' and 'secrecy of correspondence' as contained in Act No. 91-646 of 10 July 1991 on the secrecy of electronic communications. The competent judge should analyse each case in order to determine whether an e-mail should be considered as private or public communication.[72] The Constitutional Council referred to existing jurisprudence, which had already established a presumption that e-mails are private communications unless their nature made this impossible.[73] For instance, if a service intends to diffuse e-mails with a content that can not be qualified as 'personal' to undefined persons, these e-mails will fall under the rules of public communication and will not be protected by the secrecy of communications.[74]

The same interpretation has been followed in the context of labour relationships, in relation to an employer monitoring employees' private e-mails. The Supreme Court [*Cour de Cassation*] has ruled that an employee does not lose his right to privacy at the workplace.[75] This was based on the right to privacy and not on the secrecy of correspondence, which only applies to the transport of the message.[76] In its decision, the Court recognised that workers have a right to privacy at the workplace. This right does not prevent employer control of employee correspondence, but it does stand in the way of secret processing or control.[77] This case follows the case-law of the European Court of Human Rights, which only allowed employers to control employee communication on the condition that they were aware of it.[78]

Altogether, an adaptation of French law has not been necessary to acknowledge e-mail as private correspondence. Applying existing provisions appeared sufficient to guarantee the protection of private correspondence, irrespective of the technology used.

Retention of traffic data

As a consequence of the terrorist attacks of 11 September 2001, the French government introduced amendments to the Daily Safety Act. This Act had created an obligation for the telecommunication operators to retain the traffic data of electronic communications,[79] i.e., data relating to electronic communications, even if the application Decree, defining the type of data to

[72] Decision No. 2004-496 DC of 10 June 2004.
[73] Cass. Soc., 2 October 2001, *Bulletin* 2001 V No. 291, p. 233.
[74] Cass. Crim., 25 October 2000, *Bulletin criminel* 2000 No. 317, p. 318.
[75] Cass. Soc., 2 October 2001, *Bulletin* 2001 V No. 291, p. 233.
[76] P. Langlois, 'Courrier électronique et vie privée au travail', in : *Traçage électronique et libertés, Problèmes politiques et sociaux*, No. 925, June 2006.
[77] See Cass. Soc., 14 March 2000, *Bull. Civ*. V. No. 101.
[78] EctHR 27 June 1997, *Halford* v. *United Kingdom*, Rec. 1997 III.
[79] Benoît Tabaka, 'Le décret sur la conservation des données de connexion enfin publié !', *Juriscom.net*, 26 March 2006.

be retained, was not published until 2006.[80] In its Annual Report of 2001, the CNIL observed that this obligation constituted an important derogation to the principles of proportionality and of self-restraint established by the 1978 Data Protection Act, which was intended by the legislator to limit the power of the State. However, it approved the limitation constituted by incorporating in the definition the purposes and the duration of the retention set by the law.[81]

Art. L.34-1 of the Post and Electronic Communications Code guarantees the secrecy of electronic communications and establishes a general obligation to erase or anonymise traffic data. However, this obligation has a series of exceptions, which were broadened by the Public Safety Acts of 2003 and of 2006. The Constitutional Council has been called upon to consider the Act of 2006, which introduced an administrative requisition procedure for obtaining connection and traffic data, without prior judicial authorisation, for purposes of prevention and repression of terrorist attacks. The Constitutional Council censured the processing of traffic data by the administrative police for purposes of repressing terrorists attacks, on the ground that the legislator had violated the principles of separation of powers.[82] Indeed, even if crime prevention enters into the obligations of the administrative police, repression can not be incorporated in this category, which is restricted to the judicial police. It is noteworthy that the constitutional supervision here is not based on the protection of fundamental rights such as privacy but on the separation of powers.

As a consequence, and according to Articles L.34-1 and L.34-1-1 of the Post and Electronic Communications Code, traffic data can now be retained by telecommunication operators up to one year, for purposes of billing or of the security of information systems, and by judicial authorities for purposes of investigation or prosecution of criminal offenses, and by the administrative police for purposes of preventing terrorist attacks.

The application Decree of 24 March 2006 fixes the term of retention and clarified what data are to be retained. This Decree also implements the recent European Directive 2006/24/EC of 15 March 2006 on data retention.[83]

Retention requirements vary, depending on whether traffic data are retained for prosecution, invoicing, or security purposes. Moreover, the Decree imposes the traffic-data retention obligation not only on telecommunications operators and Internet Service Providers, but also on any person who offers to the public access to online communications through a network. This means that cyber-cafés, for instance, have to comply with the provisions of the Decree.

In relation to the prosecution of suspects (including terrorists), there is an obligation to retain for a one-year period the following data: data allowing identification of the user, data allowing identification of the hardware used for the communication, data relating to the technical features, the date, time, and duration of the communication, data relating to any complementary service requested or used and to the provider of such a service, and data allowing identification of the recipient of the communication. As regards telephony services in particular, telecommunications operators are also required to retain for a year any data that allows the identification of the origin and location of the communication.

Any costs incurred by telecommunications operators to comply with a request by judicial authorities will be compensated. However, the details of how compensation will work in practice will require a further ministerial order.

As regards invoicing or payment purposes, electronic communications operators are granted a right (as opposed to an obligation) to retain any technical data that allow the identification of the user, data relating to the peripheral equipment used for the communication, data relating to the technical features, the date, time, and duration of the communication, data relating to any complementary service requested or used and the provider of such a service. With regard to telephony services in particular, telecommunications operators are also entitled to retain data

[80] Decree No. 2006-358 of 24 March 2006 on the retention of electronic communications data [*relatif à la conservation des données des communications électroniques*], *JO* No. 73 of 26 March 2006, p. 4609.
[81] CNIL, *21st Report of Activity*, 2000, p. 22.
[82] Decision No. 2005-532 DC of 19 January 2006.
[83] The following description of the decree is extracted from J. Méhaud, *"Traffic data" to be retained for one year by French electronic communications operators and Internet Service Providers*, 24 May 2006, available at http://www.twobirds.com/english/publications/articles/Traffic_data_retained_one_year.cfm.

allowing the identification of the origin and location of the communication, as well as data identifying the recipient of the communication, and data pertaining to invoices. Any such data may only be retained insofar as they are necessary for payment and invoicing of the services provided. Moreover, retention is limited to the time strictly necessary for that purpose and cannot exceed a one-year period.

In relation to the purposes of security of networks and equipment, operators may retain data allowing the identification of the origin of the communication, data relating to the technical features, the date, time, and duration of the communication, data that allow the identification of the origin and location of the communication, and data relating to any complementary service requested or used and the provider of such a service.

One question remains unresolved under French law. Pursuant to Article 6-II of the Trust in the Digital Economy Act of 2004, Internet Service Providers and webhosts are required to retain and store any data that allow the identification of web content publishers. A decree was due to specify the details of this obligation, but the Decree of 24 March 2006 was silent on this point. A further decree is expected shortly to complete the legislation relating to traffic-data retention.

Confidentiality and anonymity

The Constitution does not recognise a right to anonymity. Partly, anonymity is protected through the right to privacy, which – in French law – does not only include the right to be left alone but also the right to be different, to be unpredictable, and to lead one's life as one wishes.[84] This conception implies the right to keep some information secret, e.g., the address of a domicile cannot be revealed without consent of the person who actually lives in it.

Also, the freedom to come and go anonymously should be preserved against the tracking of individuals that is enabled by the development of location-data processing and other surveillance systems. This liberty, protected by Articles 2 and 4 of the Declaration of Man and the Citizen, will fall under data-protection rules, and thus the control will mainly be operated by the CNIL. The Constitutional Council has not yet had to take a position on these specific questions.

In order to illustrate how anonymity is protected by French law in the field of new technologies, two specific cases decided by the CNIL must be brought to attention. First, in the context of peer-to-peer networks, the secrecy of communication protects users to a certain extent. Article 9.4 of the revised Data Protection Act allows societies for the collection and distribution of royalties of authors, performers, and phonogram and videogram producers to act by virtue of the rights that they administer or on behalf of victims of infringements of intellectual-propriety rights and for the purposes of ensuring the defense of these rights. It also allows them to process personal data for these purposes. Two societies had asked an authorisation from the CNIL in order to process the IP address of users of P2P networks and to send them e-mail warnings. The CNIL allowed the processing of IP addresses only if they remain anonymous until the judicial procedure. It authorised the communication of the owner of the IP address only in the cases foreseen in Art. L34-1, i.e., when a judicial authorisation exists. In other cases, this processing would excess the scope of the exceptions in this article.

Second, in cases when companies create hotlines for the purpose of whistle-blowing, confidentiality is preferred to anonymity. The CNIL has had to balance the right of the whistle-blower to keep his identity secret with the rights of the accused. The CNIL has not been favorable to anonymous warnings, because it considers that it would not protect the sender of the warning and could lead to the development of a culture of 'anonymous letters' and thus create a bad atmosphere at the workplace. Therefore, the CNIL prefers confidentiality to anonymity.

Finally, for anonymity, the field of cryptography is relevant. Here, there has been a departure of the severely restrictive intentions behind the French regulation of cryptography. In 1996, a first step towards liberalising the use and the import of cryptography for the purpose of confidentiality and private uses by natural persons was taken through the Telecommunication Act.[85] In 1999, as

[84] C. Colliards and R. Letteron, *Libertés publiques*, Dalloz, 2005.
[85] Act No. 96-659 of 25 July 1996, *JO* 27 July 1996, p. 11384.

a result of an Inter-ministerial Committee, the French government committed itself to free the use of cryptography. As a result, two decrees of 17 March of 1999 raised the maximum allowed length of symmetric crypto keys to 128 bits and allowed the sale of PGP software. In 2004, the Trust in the Digital Economy Act missed its opportunity to establish a completely free cryptography market: even if Article 30 liberalises the use of cryptography and its export within the European Union, the supply, import, and export of these technologies, if they are not limited to authentication and integrity control functions, remains subject to prior declaration to the Prime Minister.

4.5.2. Freedom of expression

The Internet is a major instrument for the freedom of expression: everyone has the possibility to publish his or her own opinion or run one's own website, without any limits – but also without any control. Since freedom of expression is not an absolute right and finds its limits in the respect of the rights of third parties, in human dignity, and in public-order considerations, the Internet can not be used for abuse.

The French constitutional right to freedom of expression recognises the free communication of thoughts and opinions as one of the most important human rights, specifying that every citizen can speak, write, or print freely, being responsible for the abuses specified by the Law (Art. 11 Declaration of the Rights of Man and the Citizen). A general freedom of expression is thus recognised, leaving to the legislator the task to limit its exercise according to other constitutional principles and values. As a result, the essence of the protection of freedom of expression remains the communication in itself, irrespective of the means used.

However, in the field of audiovisual communication, to which the Internet belongs, French legislation had established different rules according to the means of communication used, based on the scarcity of the frequencies that can be allocated. The resulting regulation was not adapted to the Internet and had to be modified. Furthermore, three main legal problems have been raised by legal doctrine regarding the use of the freedom of expression on the Internet: the legal regime of press offences committed on the Internet, defining the liability of the various actors on the Internet, and protecting minors against harmful content. The courts have successfully applied existing legislation in most of these cases, followed by the incorporation of this case-law into legislation. These developments are now described in more detail.

Creation of a new category of communications: 'on-line communications'

The French regulation on the freedom of speech is contained in two basic Acts: the Act of 29 July 1881 on freedom of the press, and the Act of 30 of September of 1986 on freedom of communication, which adapts the disposals of the Act of 1881 to the technical features of audiovisual communications, in particular regarding the right to reply to a statement and liability. This latter Act gives a broad definition of audiovisual communication, which includes every communication that uses a communication network and that does not fall under the regime of private correspondence (Article 2). It poses a general principle of freedom, and defines rules according to the means used to convey the communication (radio, cable, satellite, telephony, etc.), and not according to its content. Three different regimes are foreseen: authorisation (radio and television, because the electromagnetic frequencies for these are scarce), written agreements (cable), and declaration (others). The Supreme Audiovisual Council (*Conseil Supérieur de l'Audiovisuel*) is the agency in charge of regulating and controling audiovisual media. Two reasons are forwarded for creating this control organism: the fact that public space is being distributed in the form of telecommunications frequencies, and the possibility of influencing public opinion given to companies that have been granted frequencies.

It is debatable whether these reasons justify control on the Internet, where everyone can participate without technical restrictions. On this basis, legal doctrine progressively claims the establishment of a different regime for the Internet. The Report on Liberties and the Internet of 2000[86] suggested creating a new category of communication, 'on-line communication', in addition to audiovisual communication, both ruled by the general principle of freedom of communication.

[86] C. Paul, *Du droit et des libertés sur Internet, Rapport au Premier Ministre*, Documentation Française, 2001.

These suggestions find an echo in a 1982 decision of the Constitutional Council stating that 'the legislator is in charge of conciliating, in the current state of the art of technology, the exercise of the freedom of communication as expressed by Article 11 of the Declaration of Man and the Citizen, with, on the one hand, technical constraints inherent to audiovisual communications means, and on the other hand, the objectives with constitutional values such as the public-order safeguard, the respect of the freedom of others, and the preservation of the pluralistic nature of the ways of expressions that these means are likely to harm through their large influence.'[87]

Recently, the Trust in the Digital Economy Act (2004) incorporated these suggestions and restructured the media-law architecture by creating a general category of communications named 'electronic public communication', divided in two sub-categories: 'audiovisual communications', subject to the Act of 1986, and 'on-line public communications' subject to the provisions of the Trust in the Digital Economy Act. This new distinction could be interpreted as new conciliation between the state of the art of the technology and the respect of the constitutional values mentioned in the decision of the Constitutional Council. French law seems to be moving from legal solutions based on different technical factors to solutions based on the nature of content.

Offences committed on the Internet

'Press offenses' on the Internet and their reparation have raised a series of questions regarding the application of existing rules to the specificities of this new means of communication. The jurisprudence has had to solve the problem of defining the public nature of an offense committed on the Internet, of the starting point of the prescription period, and of the liability of webmasters for the opinions published on their websites. In the Trust in the Digital Economy Act, the legislator has explicitly recognised a right to reply to a statement made on the Internet.

A first issue concerns the public nature of the offense. The appreciation in cases of defamation and tort by the judge whether a statement is public is made on a case-by-case basis. For instance, the Higher District Court [*Tribunal de Grande Instance*] of Paris, in a judgement of 25 October 1999, has considered that the diffusion of a defamatory text to a distribution list that has members only on the basis of their membership to an organisation or through patronage, did not constitute a public defamation.[88] In another case, the District Court [*Tribunal d'instance*] of Puteaux, in a judgement of 28 September 1999, considered that as long as the defamatory terms were published on a website that everyone could access without any restriction or selection, the defamation was public.[89]

A second concern regarded applying the starting point of the limitation-of-legal-proceedings period to an offense committed on the Internet. Article 65 of the Act of 1881 establishes a period limiting the possibility of legal proceedings to within three months from the date of publication. Article 6 of the Trust in the Digital Economy Act extended the application of criminal and criminal-procedure provisions of the Act of 1881 to on-line public communication services, but established a different limitation-of-legal-proceedings period than the one stated by Article 65. In cases where the on-line content does not reproduce in identical terms a written message, the starting point would be defined by the moment when the offence ceases.

This provision tried to reverse the jurisprudence and go back to the case-law of the ordinary courts. These courts made a first interpretation of Article 65 of the Act of 1881, and considered publication on the Internet as a continuous offense.[90] This implied that the starting point of the limitation-of-legal-proceedings period was the moment when the offense ceases. However, the Supreme Court did not follow this interpretation and opted for a more protective approach of freedom of expression, applying the same regime to off-line and on-line public defamation. According to this jurisprudence, the starting point of the limitation-of-legal-proceedings period is the moment of the publication on the website:[91] ignorance of the victim could not delay this starting point. This interpretation limits the possibility of remedy for the victims.

---

[87] Decision 82-141 DC of 27 July 1982.
[88] Not published, available at http://www.juriscom.net/txt/jurisfr/cti/tgiparis19991025.htm.
[89] Emmanuel Tois, 'Internet et libertés, quelques repères', Report 2001, Cour de Cassation.
[90] Tribunal Correctionnel de Paris, 17ème Ch., 6 December 2000, JCP Ed. G 2001, II, 10515, and CA Paris, 15 December 1999, JCP Ed. G 2000, II, 10281.
[91] Cass. Crim. 30 January 2001, JCP Ed. G 2001, II, 10515.

The Constitutional Council censured this specific rule introduced by the Trust in the Digital Economy Act, because it created unjustified differences in legal regime between the written press and the Internet.[92] In its decision, the Court admitted that the principle of equality does not constitute an obstacle to different regimes for on-line and written contents, whenever it is directly related to the purpose of the law establishing it, and if it is not excessive in view of the purpose of the measure, in this case, the fight against press offenses. In the case at stake, it considered that the difference was clearly unbalanced and would violate the principle of equality in front of the law.

A third issue was the right of response. The original version of the Trust in the Digital Economy Act (Art. 6-IV) established a specific right to respond. Deviating from the regime of prescription established for the written press, it was said that the right could be exercised as long as the content remains available on-line. The Constitutional Council censured this provision for the same reasons it had censured the prescription rules.[93] According to the new version of this article, every person named or designated on the Internet (on a website, a forum, etc.) now has a right of reply under the same conditions as those claiming a right to reply with regard to the written press. The extension of this right to all information published on the Internet irrespective of its format is consistant with the assimilation of webmasters to editors in the system of liability, as we will now explain.

Liability of actors on the Internet

Another important point of debate concerned the liability of actors on the Internet for information published on their websites, even if they are not the authors. The issue of liability is of course very important for the actual exercise of the freedom of expression. Persons will tend to apply censorship under a strict liability regime in order to protect themselves. This necessitates a delicate balancing exercise.

A first issue is the civil liability of webmasters. The French system is based on a system of 'cascade' liability [*responsabilité en cascade*] established by the Act of 1881 and modified by the Act of 1986 to audiovisual communications when it comes to civil prosecution of press offences. The legally responsible persons for the offence are, in order, the publication director when the information published has been recorded before its public communication, the author, and the producer (or in the written press: the printer and the advertiser).

A first legal difficulty regarded the question whether a website could be equated with an audiovisual communication means. Does the Act of 1986 apply? Some courts observed that a website could hardly be equated with a periodical because of the permanent nature of the latter, and therefore could not be considered to have been published by a publishing company with a publication director.[94] However, this interpretation had not been followed by the Supreme Court, which equated a website, and therefore also blogs, to a periodical.[95] The system of 'cascade' liability is therefore applicable to a website, and the director of the publication – in the case of a website, the webmaster – will be liable for the content of the website.

Blogging has triggered legal questions about the requirement of transparency and the obligation for editors of a publication to identify authors in the publication for the sake of prosecuting press offences. Often, bloggers wish to remain anonymous to their audience, but this might endanger effective prosecution of offences. Again, a compromise was struck: when a blogger informs his webhoster of his identity, he can choose to remain anonymous on the website. In that case, he is only obliged to give information on his website about the contact details of his ISP (Art. 6-III Trust in the Digital Economy Act).

A second issue relates to criminal liability of webmasters for hyperlinks. Several decisions have been issued by the courts on this, but none of the questions have been put forward before the Constitutional Council. For example, the High District Court of Epinay stated that the webmaster

[92] Decision No. 2004-496 of 10 June 1994.
[93] *Ibid.*
[94] Cour Administrative d'Appel de Paris, 24 January 2002, No. 99PA03034 (M.O.), mentioned in Colliards and Letteron, op. cit. n. 84.
[95] Cass. Crim. 6 May 2003, *Bull. crim.* No. 94, p. 359; Cass. Crim. 10 May 2005.

was liable for hyperlinks to a website allowing illegal downloading of MP3, as he expressly warned users of the illegal source of MP3s that could be downloaded from this website.[96] The Supreme Court convicted an online newspaper for facilitating through a hyperlink the obtaining of a work which was prohibited in France, because it was considered as advertising products, objects, and methods advocated to commit suicide.[97] This topic has also been the object of a Recommendation by the Forum of Internet Rights. The Forum emphasised that webmasters can only be liable for hyperlinks on their websites in two cases: when the intentionality of the webmaster can be proved, or when the webmaster maintains the link despite knowing the illicit content of the linked website.[98]

A third issue is the liability of webhosts regarding the content published by their users. For this issue, the legislator defined a completely new system in 2000,[99] which was completed in 2004. In 2000, the legislator had foreseen two cases of liability: when the webhost, after being commanded by the judicial authority to remove or block access to illegal content, did not do anything to prevent the access, and when, despite questions by a third party to remove certain content that they consider illegal or harmful, the webhost refrains from taking 'appropriate measures' [*diligences appropriées*].

The second type of liability was censured by the Constitutional Council because the expression'appropriate measures' was imprecise.[100] The legislator had not defined the conditions under which judicial authorities should command the webhost to remove the content in question, nor the essential elements of the conduct of webhosts which lead to criminal liability. Therefore, the legislator had exceeded his competences and violated Article 34 of the Constitution. Once again, the Constitutional Council did not censure on the basis of a violation of a constitutional right but on an *extra vires* (beyond the scope of power) of the legislator.

This liability system has been completed by the Trust in the Digital Economy Act of 2004, which literally transposes the provisions of the European e-commerce directive. The liability regime for webhosts was extended to providers of 'caching' services (Art. 9 Trust in the Digital Economy Act). This time, the Constitutional Council could not censure the provision as it was a direct transposition of a European directive.[101] However, the Council stressed that the liability regime established by Articles 6.I.2 and 6.I.3 should not imply the liability of a webhost that has not withdrawn information claimed as illicit by a third party, when this information is not overtly illicit, or if its withdrawal has not been ordered by a judge. It will be for the courts to define the notion of 'overtly illicit information'.

In a recent case, the Committee for the Defense of the Armenian Cause sued the Turkish consul and the webhost of their website because of publishing information in denial of the genocide against Armenians by the Turkish.[102] The Committee asked the webhost to block the content. The webhost did not comply, arguing that the information did not have an overtly illicit content. We recall that, at that time, French law recognised the Armenian genocide, but did not consider its negation as a crime. The court did not consider that the webhost was liable: to decide whether the content was overtly illicit requires a legal analysis incumbent to the court and not the webhosts.

Protection of minors

The Forum of Internet Rights has issued two Recommendations, one regarding the protection of minors on the Internet against harmful content[103] and another regarding pornography and

---

[96] TGI Epinal, 24 October 2000, available at http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=215.
[97] Cass. Crim. 13 November 2001, *Bull. Crim.* 2001, No. 234, p. 756.
[98] Forum des droits sur l'Internet, *Which liability for the originator of hyperlinks to illicit contents?* [*Quelle responsabilité pour les créateurs d'hyperliens vers des contenus illicites?*], 23 October 2003.
[99] Act No. 2000-719 of 1 August 2000, modifying Act No. 86-1067 of 30 September 1986 on the freedom of communication.
[100] Decision No. 2000-433 DC of 27 July 2000.
[101] Decision No. 2004-496 of 10 June 1994.
[102] CA Paris, 11e Ch., 8 November 2006, available at http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=1114.
[103] Forum des droits sur l'Internet, *Les Enfants du Net (1) – Les mineurs et les contenus préjudiciables sur l'Internet*, [*Children of the Net (1). Minors and harmful content on the Internet*], Recommendation of 11 February 2004.

pedophilia.[104] In the former, the Forum expressed itself in favour of combining technical (e.g., an e-identity card proving age), legal, and educational measures, rather than an approach that focuses solely on legal reform. The latter recommendation was different in tone, and contained a call for debate on adapting the Criminal Code and the Code of Criminal Procedure, as well as reinforcing international cooperation.

The protection of minors is first ensured, at a preventative level, by the obligation of Internet Service Providers to inform their users of the possibility of using technical means in order to limit access to certain services (Art. 6-I Trust in the Digital Economy Act). Moreover, at the repressive level, harmful behaviour against minors by technological means is combated by two new crimes that were introduced in the Criminal Code to protect minors against harmful content and pornography. Since 2000, the diffusion of harmful content to minors is punishable by three years' imprisonment and a fine of €75,000. Incorporated in the section 'Of minors and family protection', Art. 227-24 CC prohibits 'the manufacture, transport, and distribution by whatever means and however supported, of a message bearing a pornographic or violent character or a character seriously violating human dignity, or the trafficking in such a message'. This article stipulates that 'cascade' liability will only apply when the message is carried by the written press or by audiovisual communication means. As a consequence of the reform of the Media Law by the Act of 2004, the responsibility of editors of a website is not subject to the 'cascade' liability system. They can only be punished in their quality of editor of a website if they have produced the harmful content themselves or editorially exploited it, or through their quality of webhost provider under the conditions previously mentioned.[105] The Criminal Code also punishes exploiting the representation of a minor when it has a pornographic content (Art. 227-23). The Trust in the Digital Economy Act of 2004 has modified this article in order to adapt French law to the Convention on Cybercrime of the Council of Europe. Now, this article does not only punish the processing, recording, or transmitting of the image of a minor, but also the import, export, and the direct or indirect displaying of a minor in a pornographic way.

4.6. Other and new constitutional rights

The massive use of new technologies has influenced the exercise of certain rights, which in turn has led to an adaptation of the law, usually following solutions established by case-law. The most important fundamental right in this respect appears to be the freedom to come and go anonymously through the development of location-data processing (4.6.1), and a substantial modification can be expected to the right to vote through the introduction of new technologies (4.6.4).

Other rights that are important in a democratic society but that do not have a constitutional status in France should be also mentioned: the legal equivalence of paper-based and electronic documents (4.6.2) and the right to communicate with the Administration by electronic means (4.6.3).

4.6.1. The freedom to come and go anonymously

The freedom to come and go anonymously has been recognised as a principle with a constitutional value by the Constitutional Council in its 1979 decision regarding the law on implementing road toll.[106] The formulation of the freedom has evolved to become a part of individual liberty. The implementation of technologies for tracking individuals (biometric imprints, Internet tracking, profiles of Internet surfing, electronic mails, location-based services) are restraining this freedom by registering every movement of the user. If these issues are dealt with as data-protection issues, the CNIL has explicitly stated that, for example in the case of location-

[104] Forum des droits sur l'Internet, *Les Enfants du Net (2) – Pédo-pornographie et pédophilie sur l'Internet* [*Children of the Net (2). Child pornography and pedophilia on the Internet*], Recommendation of 25 January 2005.
[105] Forum des droits sur l'Internet, *Loi pour la Confiance dans l'économie numérique, Un nouveau cadre juridique pour Internet*, [*Trust in the Digital Economy Act, a new legal framework for the Internet*], June 2004, available via http://www.foruminternet.fr.
[106] Decision 79-107 DC of 12 July 1979.

based services, data-protection rules protect the freedom to come and go anonymously. The CNIL and more rarely jurisprudence are balancing the need for using these new technologies with the protection of the fundamental rights of individuals.

4.6.2. The legal value of electronic documents

French law has entered into a large process of reviewing the provisions of contract law in order to ensure legal equivalence of paper-based and electronic documents, following the French jurisprudence. The Act implementing the European E-signature Directive has modified the Civil Code, defining written evidence independently from the carrier, allowing the production of electronic evidence during a civil judicial procedure. Authentic deeds have also been taken into account, and two decrees regulate the use of electronic documents by civil-law notaries and bailiffs[107].

4.6.3. The right to communicate with the Administration by electronic means

The right to access administrative documents is guaranteed by law. The exercise of this right is mediated through the Commission of Access to Administrative Documents (*Commission d'accès aux documents administratifs*, CADA), an independent authority that issues non-binding recommendations and annual reports.

As part of the whole process of adapting the law to ensure the legal equivalence of paper-based and electronic documents, the Act to Simplify the Law (*Loi de simplification du droit*) was passed in 2004,[108] followed by an Ordinance on electronic communications between users and administrative bodies (*Ordonnance relative aux échanges entre les usagers et les autorités administratives)*[109] in 2005. The Ordinance establishes the equivalence of electronic and ordinary mail, the possibility to communicate with the Administration by electronic means, the creation of a special electronic space for users in order to send required documentation, and the possibility for administrative bodies to use electronic signatures. The French Administration has also developed a set of 'teleprocedures' [*téléprocédures*], which permit citizens and companies to exchange documents, such as tax and social-security forms, by electronic means with the Administration, and creates a secured environment in order to fill in the sometimes mandatory declarations online. Some information inherent to Public Procurement, such as candidature and offers, can be sent to companies by electronic means with the use of electronic signatures.[110]

This Ordinance has also adapted the right of access to public documents to the use of new technologies. For example, the document requested can be communicated by e-mail without any cost when the document is available in electronic form.

4.6.4. E-voting

Electronic voting has been debated over the past years. In 2003, the Forum of Internet Rights issued a Recommendation[111] in which it suggested a progressive plan of implementation, and conceiving electronic voting in any case when distance voting is allowed, as a complementary means of exercising one's right to vote. The CNIL issued a document on the state of the art of e-

[107] Decree No. 2005-973 of 10 August 2005 amending Decree No. 71-941 of 26 November, 26 1971 on acts issued by civil-law notaries [*relatif aux actes établis par les notaires*] and Decree 2005-972 of 10 August 2005 amending Decree No. 56-222 of 29 February 1956 in application of Ordinance of 2 November 1945 on the statute of bailiffs [*relative au statut des huissiers de justice*] .

[108] Act No. 2004-1343 of 9 December 2004 on simplification of the law [*de simplification du droit*], *JO* 10 December 2004.

[109] Ordinance No. 2005-1516 of 8 December 2005 on electronic exchanges between public agencies and users [*relative aux échanges électroniques entre les usagers et les autorités adminisitratives*].

[110] Decree of 30 April 2002 on the dematerialisation of public-procurement procedure [*relatif à la dématérialisation des procédures de passation des marchés publics*], *JO* 3 May 2002.

[111] Forum des droits sur l'Internet, *Which future for electronic voting in France?* [*Quel avenir pour le vote électronique en France?*], Recommendation of 26 September 2003, available at http://www.foruminternet.org/recommandations/lire.phtml?id=651.

voting on 23 May 2006 in order to contribute to the debate and to explain the main factors bearing upon its development.[112]

There have been some experiments with e-voting at the local level and for electing the representatives of the French living abroad. The results of these experiments were moderate, since few voters opted for these procedures because of their complexity.

4.7. Conclusion

The general formulation of French constitutional rights and their interpretation by the Constitutional Council has allowed the French legal system to answer the main legal problems raised by the information society and the use of the Internet in a satisfactory way. Even if some adjustments were required, no radical changes were called for in order to fit new technologies into the existing legal framework. The Courts have been able to apply existing rules to new concerns raised by the Internet, solutions usually followed by the legislator *a posteriori*. The French legal system has appeared flexible enough in its formulation to be able to absorb the changes operated and the new challenges raised by the information society. The general assertion made by the State Council in its report *Internet and Digital Networks* of 1998,[113] in the sense that the whole legal framework is applicable to Internet and that there is no need for a specific regulation for Internet and digital networks, seems to be confirmed.

Despite the importance of the rights at stake, the control of these developments is mainly left to administrative bodies such as CNIL, since fundamental rights are rarely put forward to the judicial and administrative courts. Questions directly linked to new technologies are rarely referred to the Constitutional Court, whose scope of action is limited by the definition of constitutional control, which is *a priori* and thus abstract. As highlighted in this chapter, the concerns are usually raised in the field of the concrete applications of the law, e.g., in decrees and other norms applying laws in the public sector, and in contracts, self-regulation, and other instruments of regulation of private relationships in the private sector. As a consequence, the current control is mainly realised by bodies like the CNIL.

Moreover, an increasing influence of international law, and particularly European law, can be observed in French law. The recent modification of the position of the Constitutional Court with regard to European law, in particular its refusal to control the constitutional validity of transposition laws whenever they literally transpose a directive, also reduces the scope of French constitutional control with regard to fundamental rights triggered by new technological developments.

New constitutional challenges are expected, in particular with regard to the balance between national safety and privacy, as state authorities push for more and more processing of personal data. Another source of tension is the trend towards incorporating new technologies for identification purposes and the freedom to come and go anonymously. Finally, the unlimited freedom of expression caused by the Internet and the difficulty of controlling the Internet facilitate the development of illegal and harmful content. These new concerns require joint solutions at the international level.

References

Boyer J., 'Fichiers de police judicaire et normes constitutionnelles: quel ordre juridictionnel?', *Petites Affiches* 22 May 2003, No. 102, pp. 4 et seq.

Colliards C. and Letteron R., *Libertés publiques*, Dalloz, 2005.

Conseil d'Etat, *Internet et les réseaux numériques*, La documentation française, 1998

Consitutional Council, *Human Rights and Public Order, the main criteria for restricting human rights in the judicial practice of constitutional law*, 8th Seminar of Constitutional Courts,

[112] CNIL, *Internet voting in political elections, points of debate* [*Le vote par internet aux élections politiques, les éléments du débat*], 23 May 2006, available at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/e-administration/Note_vote_internet_VD.pdf.

[113] Conseil d'Etat, *Internet et les réseaux numériques*, La documentation française, 1998.

Erevan, 2-5 Novembre 2003, available at http://www.conseil-constitutionnel.fr/dossier/quarante/notes/libpuben.htm.
Dreifuss-Netter F. and Moutel G., *Les lois de bioéthiques et leur réactualisation*, available at http://infodoc.inserm.fr/ethique/cours.nsf/bccd132de8453295c125685b004bb3a8/03b36f2ea90e3cf380256cb500370db5?OpenDocument.
Grewe C.,'Rights and Fundamental Freedoms', in: R. Blanpin ed., *International Encyclopedia of Laws, Constitutional Laws, France*, Deventer: Kluwer law and taxation publ., 1999, pp. 51-69.
Hamon A., *Une approche de la liberté d'expression sur Internet*, Thesis, DEA Droits de l'homme et libertés publique, Université Paris X Nanterre (France), 2000.
Langlois P., 'Courrier électronique et vie privée au travail', in: *Traçage électronique et libertés, Problèmes politiques et sociaux* No. 925, June 2006, La Documentation française.
Lambert N. and Lebon H., *CNIL clarifies use of biometric ID systems in the workplace*, 30 June 2004, available at http://www.twobirds.com/english/publications/articles/CNIL_clarifies_biometric_ID_systems.cfm?renderForPrint=1.
Lebon H., *French Data Protection Authority (CNIL) guidance concerning biomedical research*, 23 March 2006, available at http://www.twobirds.com/english/people/Helene_Lebon1.cfm.
Mallet-Pujol N., *Traçage électronique et libertés*, *Problèmes politiques et sociaux* No. 925, June 2006, La documentation française.
Méhaud J., *"Traffic data" to be retained for one year by French electronic communications operators and Internet Service Providers*, 24 May 2006, available at http://www.twobirds.com/english/publications/articles/Traffic_data_retained_one_year.cfm.
Paul C., *Du droit et des libertés sur Internet, Rapport au Premier Ministre*, Documentation Française, 2001.
Tabaka B., *Le décret sur la conservation des données de connexion enfin publié!*, Juriscom.net, 26 March 2006.
Tois E., *Internet et libertés, quelques repères*, Report 2001, Cour de Cassation.

Chapter 5. Constitutional Rights and New Technologies in Germany

Thomas Hoeren and Anselm Rodenhausen*

5.1. Introduction

The progressive digitalisation of virtually all sectors of German society has had deep impact on the constitutional-rights system. Before describing how these developments affect the interpretation and implementation of several constitutional rights or whether those rights even have an active influence on the use of ICT, we shall briefly outline the German system of constitutional rights.

In Articles 1 to 19, the German Constitution (*Grundgesetz*, hereinafter: GG) guarantees several fundamental rights – so-called basic rights – which bind the legislature, the executive, and the judiciary as directly applicable law. Beside these federal rights, most Constitutions of the sixteen federal states of Germany contain their own basic rights. According to Article 31 GG, federal law has precedence over the law of the individual federal states; therefore, the basic rights of the federal states are of minor importance and shall be omitted in this chapter.

The main function of the basic rights warranted by the German Constitution is to protect the individual from the state[1] – that is why these basic rights are also described as *defensive rights*. One way of enforcing these individual rights is to appeal on an institutional issue to the Federal Constitutional Court (*Bundesverfassungsgericht*, BVerfG); this is called 'Verfassungsbeschwerde'.[2] In addition to their primary function as defensive rights, a third-party effect of basic rights ('mittelbare Drittwirkung') has been constructed.[3] This means that these basic rights may also have an impact on the interpretation of private law.

It involves three steps to ascertain whether a basic right has been violated or not: determination of the extent of protection of the relevant basic right; identification of an encroachment; and potential justification of the encroachment.

5.2. History of digital constitutional rights and changes in the constitutional system

In spite of ICT's high development status, a term like 'digital constitutional rights' has yet not been added to German legal terminology. Only a few publications deal exclusively with this specific issue. In fact, the impact of new information and communication technologies has generally been analysed in the course of broad discourses about separate basic rights. The studies of Alexander Roßnagel et al. in the late eighties were the first to solely but comprehensively cover this topic.[4]

Examining the impact of ICT not as a whole but in conjunction with each basic right has continued in the new millennium. Hence, the history of interpreting basic rights with regard to ICT and the changes to the constitutional system will be shown for each basic right.[5]

---

* Prof. Dr. Thomas Hoeren is Professor in Information, Media and Business Law at the Faculty of Law, University of Münster, and Head of the Institute for Information, Telecommunications and Media Law (ITM). Mag. jur. Anselm Rodenhausen is Junior Researcher at ITM.

[1] See BVerfG 15 January 1958, *BVerfGE* 7, 198, 204.

[2] See Art. 93 para. 1 No. 4a GG.

[3] See BVerfG 11 May 1976, *BVerfGE* 42, 143, 148; BVerfG 12 November 1997, *BVerfGE* 96, 375, 398, and also H. Jarass, 'Bausteine einer umfassenden Grundrechtsdogmatik', 120 *AöR* (1995) p. 345, 352.

[4] See, for example, A. Roßnagel et al., *Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik* [Digitalisation of the Basic Rights? A contribution to the constitutionality of information and communication technology] (Opladen, Westdeutscher Verlag 1990), p. 308, for further references.

[5] For the major changes concerning the inviolability of the home, see *infra*, section 5.3.2.

5.3. Privacy-related rights

5.3.1. Privacy and data protection

Neither privacy nor data protection is explicitly mentioned in the German Constitution. Although both are not specifically codified, they are part of a fundamental right that is considered to be expressed in Article 2 paragraph 1 and also in Article 1 paragraph 1 of the German Constitution: the 'general right of personality'.[6] Article 2 paragraph 1 GG reads:

> [e]very person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law.

This broad phrasing leaves room for interpretation and underlines the function of this basic right as a catch-all element. Due to the jurisdiction of the Federal Constitutional Court, the extent of protection of the general right of personality contains diverse items, such as the account of a person in public,[7] the protection of personal honor,[8] portrait rights, the right of informational self-determination,[9] the privilege against self-incrimination,[10] and also privacy.[11] The right of informational self-determination is based on the Constitution; it is also referred to as the fundamental right of data protection.[12]

Generally speaking, an act of state that restricts these rights is justified if it is has a legal basis and if it is proportional. Whether the act is proportional or not must be assessed by appreciation of the values at stake. Since the development of the general right of personality, the courts and literature have always stressed the relationship of this basic right to the guarantee of human dignity in Article 1 paragraph 1 GG, which is the highest value of the German Constitution.[13] This affects the relationship of the general right of personality to other values like public security or the inviolability of the body.

Although privacy and data protection coincide in some cases of legal practice, they will be analysed separately.

Current developments concerning privacy

The right to privacy as part of the general right of personality includes matters typically considered as private because of their informational content; it also includes a spatial area in which the individual can relax and find peace.[14] The Federal Constitutional Court discerns different levels of protection: the *private sphere* and the *intimate sphere*. Only the intimate sphere is fully protected.[15]

Before describing how some new technologies actually affect the constitutional protection of privacy, we shall first give a brief overview of the most frequently discussed topics concerning privacy and ICT in Germany. Both aspects of privacy protection – matters that are private because of their content and the private spatial area – face interferences due to recent developments in different ICT areas.

---

[6] As an autonomous fundamental right, it was evolved by the Federal Court of Justice (*BGHZ* 13, 124 – *Leserbrief*) and was later adopted by the Federal Constitutional Court (*BVerfGE* 6, 32, 41 – *Elfes-Urteil*).
[7] See BVerfG 8 December 1983, *BVerfGE* 63, 131, 142; BVerfG 3 June 1980, *BVerfGE* 54, 148, 155.
[8] See BVerfG 3 June 1980, *BVerfGE* 54, 208, 217; BVerfG 14 January 1998, *BVerfGE* 97, 125, 147; see also the Federal Administrative Court [BVerwG] 23 May 1989, *BVerwGE* 82, 76, 78.
[9] See BVerfG 15 December 1983, *BVerfGE* 65, 1, 43 – *Volkszählung*; BVerfG 11 June 1991, *BVerfGE* 84, 192, 194.
[10] See BVerfG 8 July 1997, *BVerfGE* 96, 171, 181; see also C. Starck, in: H. von Mangoldt, F. Klein, and C. Starck, *Das Bonner Grundgesetz 1* [Commentary of the Basic Law – Volume 1], Vol. 1, 4th edn, (München, Vahlen 2005), Art. 2 I, ¶ 100.
[11] See BVerfG 26 April 1997, *BVerfGE* 90, 255, 260.
[12] E.g., E. Gurlit, 'Die Verfassungsrechtsprechung zur Privatheit im gesellschaftlichen und technologischen Wandel', *RDV* (2006), p. 43.
[13] See BVerfG 12 November 1997, *BVerfGE* 96, 375, 398; see also P. Kunig in: P. Kunig and I. von Münch (Eds.), *Grundgesetz-Kommentar* [Commentary of the Basic Law], Vol. 1, 5th edn. (München, Beck 2000), Art. 1 I, ¶ 4.
[14] See BVerfG 15 December 1999, *BVerfGE* 101, 361, 382.
[15] See BVerfG 14 September 1989, *BVerfGE* 80, 367, 373; BVerfG 14.12.2000, *BVerfGE* 103, 21, 31.

General appreciation of privacy versus security

In 2001, when the threat of terrorist assaults became eminently visible, political discussions began in Germany on how new technologies could be used to fight these menaces. By the end of 2001, the German parliament had already adopted two anti-terrorism measures, which changed seventeen bills and transferred, *inter alia*, more authority to the German intelligence services and effected the implementation of biometric identification measures – such as facial scans and fingerprints – in passports.[16] In the run-up to the FIFA World Cup 2006 in Germany, a number of public institutions demanded advanced measures, but these were not adopted. However, when two abortive bomb attacks on German regional trains were revealed, the discussion started again and is continuing to date.[17] Besides anti-terrorism measures, there have also been discussions, some major court decisions, and several changes in bills regarding how to use ICT – particularly surveillance technology – in the battle against organised crime.[18]

Whether such measures violate or respect the fundamental right to privacy depends on the relation between privacy and security in each particular case. As mentioned before, privacy is part of the general right of personality and is therefore related to the guarantee of human dignity in Article 1 paragraph 1 GG. The right of human dignity cannot be subjected to amendments by basic law.[19] This argument can often be heard by those opposing the security measures. Privacy is claimed to be one of the fundamental liberties of the German democratic society, and the reluctance to taking severe security measures can be ascribed to historic experiences during the Third Reich and the German Democratic Republic. On the other hand, there is also the question of the value of security, which is backed by the constitutional right to life and physical integrity in Article 2 paragraph 2 GG. This article was consciously inserted at the beginning of the Constitution again as a reaction to the occurrences during the Third Reich and to demonstrate its tremendous value and importance in the system of constitutional rights.[20] The basic right expressed in Article 2 paragraph 2 GG also contains an active duty ('Leistungspflicht') of the German State to protect life and physical integrity against illegitimate encroachments of other civil persons.[21] This means that the public authorities are obliged to take action in order to guarantee these fundamental rights.

Even after the recent discussions about terrorism and organised crime, the simple conclusion can not be drawn that either privacy or security has prevailed over the other. In fact, the Federal Constitutional Court has repealed some electronic-surveillance measures and accepted others under certain licensing requirements.[22] It is all about the proportionality of a measure in the individual case.

Video surveillance

One example of the conflict between privacy and security is video surveillance of public spaces by the police. In 2003, the Higher Administrative Court of Baden-Württemberg was the first upper court to assess the legitimacy of a pilot project in which several streets and squares in a German city centre were monitored round-the-clock by eight video cameras. Images were saved on a digital video server and deleted after 24 hours.[23] In its decision, the court struck a compromise between the advocates of such observations and the guardians of privacy. Video surveillance of public spaces is legitimate under strict preconditions as a precautionary measure for ensuring safety. The main condition is the objective unsafeness of the place to be monitored. This means that there must be facts that provide an informative basis to assume the place will be the site of a crime. The degree of probability of crimes being committed there should be higher than in most

[16] Those were installed in October 2005; see press release of the Federal Ministry of the Interior: http://www.bmi.bund.de/cln_028/nn_662928/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/2005/06/G8__Innen__Justizminister.html.
[17] See declaration of the German Federal Secretary of the Interior, Dr. Wolfang Schäuble, http://www.bmi.bund.de/cln_028/nn_662928/Internet/Content/Nachrichten/Pressemitteilungen/2006/08/Statement__Kofferfunde.html; for the legislative procedure of a counterterrorism data base, see *infra*, section 5.3.1.5.
[18] See *infra*, section 5.3.2.
[19] See Article 79 III GG.
[20] See BVerfG 1 August 1987, *BVerfGE* 49, 12, 53.
[21] See BVerfG 21 June 1977, *BVerfGE* 45, 187, 254; BVerfG 28 January 1992 *BVerfGE* 85, 191, 192 for the protection of life; and BverfG 14 January 1981, *BVerfG* 56, 54, 78 for the protection of physical integrity.
[22] See BverfG 3 March 2004, *BVerfG*, NJW 2004, 999 et seq.
[23] VGH Mannheim 21 July 2003, *NVwZ* 2004 p. 498.

other places in the same city. The court took into consideration that video surveillance of public places is an encroachment of privacy and of the right of informal self-determination of passers-by. Only the preconditions made the measure proportional. In principle, this compromise has been accepted by the literature.[24] This meant that for a long time, an expansion of video surveillance such as occurred in London did not seem to be admissible. However, after the abortive bomb attacks, politicians have called for a more intensive observation of stations and trains.

The discussion about video surveillance of work places is closely related to this. Whether or not monitoring by the employer violates the general right of personality of the employees also depends on the proportionality.

In 2004, the Federal Labour Court (*Bundesarbeitsgericht*, BAG) decided that the video surveillance of a postal distribution centre where some letters had disappeared was not proportional.[25] In this particular case, the court stated that permanent surveillance pressure can strongly affect the employees' privacy and is not in proportion to the risks of the employer.[26]

Application of GPS for criminal prosecution

Another example of the constitutional relationship between privacy and security is the application of new technologies in preliminary proceedings, i.e., during the stage prior to a criminal charge in the sense of Article 6 ECHR. In 2001, the Federal Court of Justice had to decide whether GPS data that had been recorded in the preliminary proceedings could be used as evidence in a trial against a terrorist suspect.[27] The court decided that the use of GPS is included in the German Code of Criminal Procedure (*Strafprozessordnung*, hereinafter: StPO), but this can also involve other surveillance measures such as an 'all-around surveillance', which would be an encroachment of privacy that could not be legitimated. In the same case, the Federal Constitutional Court emphasised that the use of new technologies in preliminary proceedings can strongly affect the general right of personality – in particular when those measures are unknown to the suspect.[28] Therefore, these measures require certain procedural regulations in order to be proportional. Because of rapid technical developments, the German legislator must keep a close eye on developments and, if necessary, enact new laws to maintain a high level of privacy protection.[29]

Consideration of privacy in relation to communication-related rights

Another, completely different, aspect is the conflict between the general right of personality – including the individual's portrait rights, the right of the spoken word, and the account of a person in public – and communication-related rights. The starting point for our considerations is the relation between the general right of personality and the basic rights in Article 5 GG. These are, among others, the freedom of expression, the freedom of the press, and the freedom of art. In the leading decision, the Federal Constitutional Court affirmed the high value of the general right of personality and approved the proscription of a novel that portrayed the life of a famous German actor and his role in the Third Reich.[30]

Meanwhile, the position of the communication-related basic rights is sustained by a right called 'the information interest of the citizen'. Several media-related decisions refer to this right.[31] Nevertheless, the constitutional basis for this right is very loose and is disputable. The fundamental decision made in 1973 categorised it in the freedom of reporting by means of broadcasts and films (Art. 5 para. 1 s. 2 German Constitution);[32] others see the freedom of the

[24] See M. Ogorek, 'Anmerkung VGH Mannheim, Urteil vom 21.7.2003 – 1 S 337/02', *JA* (2004) p.608; see also C. von Stechow and M. von Foerster, 'Vereinbarkeit der Videoüberwachung öffentlicher Räume mit dem Recht auf allgemeine Persönlichkeit', *MMR* (2004) p. 202.
[25] BAG 29 June 2004, *BB* 2005 p. 102.
[26] See BAG 29 June 2004, *BB* 2005 p. 102 at p. 107; see also H. Wolf, 'Anmerkung BAG, Beschluss vom 29.6.2004 – 1 ABR 21/03', 02 *BB* (2005) p. 108.
[27] BGH 24 January 2001, *BGHSt* 46, 266.
[28] BVerfG 12 April 2005, 08 *CR* 2005 p. 569 at p. 572.
[29] See again BVerfG 12 April 2005, 08 *CR* 2005 p. 569 at p. 572.
[30] BVerfG 24 February 1971, *DÖV* 1971 p. 554 – *Mephisto*.
[31] See BVerfG 5 June 1973, *AfP* 1973 p. 423; BVerfG 8 July 1997, *NJW* 1997 p. 2669; BVerfG 25 August 2000, *ZUM* 2001 p. 232.
[32] See again BVerfG 5 June 1973, *AfP* 1973 p. 423 – *Lebach-Urteil*.

media or the freedom of information (Art. 5 para. 1 s. 1 German Constitution) as the constitutional setting.[33] In any case, in literature and jurisprudence, the information interest of the citizen is seen as a constitutional right or, as the case may be, a constitution-related right.

Although the relation between privacy and communication-related rights is relevant to many cases involving new technology, and new media in particular, this relation is rarely visible in specific legal provisions. In most cases, such as the violation of the right to an individual's picture on the Internet, conflicts can be solved through general constitutional and civil law (one only has to mention the decision of the European Court of Human Rights in 2004 concerning Princess Caroline, which partly contravened the prior jurisprudence of the Federal Constitutional Court and the Federal Court of Justice, and therefore caused a stir in Germany).[34] Now, we will discuss two recent problems concerning specific digital technologies.

Publishing personal information by a search engine

An example of Internet privacy protection is the legal evaluation of the entries that result from a search via a meta-search engine. This issue may be very specific, but it clarifies how the protection of privacy and the general right of personality are also influenced by technical feasibilities.

In 2004, a German television presenter filed a meta-search engine for injunctive relief ('Unterlassungsklage', i.e., filing a complaint for having neglected to do something). When entering the name of the presenter together with 'nude' as search terms, the search engine produced several entries giving the impression that corresponding pictures were available on the Internet. The county court sustained the claim: since the entries violated the general right of personality, the operator of the search engine should adapt the system so as to avoid future encroachments by, for example, using adequate filter software.[35] In this instance, not only the hyperlink but also the 'snippet' – the text in the results lists of an Internet search – was considered a violation.[36]

However, in the appeal procedure in 2006, the upper court had a closer look at the characteristics of a meta-search engine, which only reproduces the search results of other engines. It considered that it would not be reasonable to expect the search engine operator to check each search result for possible encroachments of the general right of personality of individuals.[37] In fact, the operator would only be liable, if he notices violating entries and neglects his duty to remove them. In this particular case, such a breach of duty was not detected.

At first, this legal practice may seem to be restrict the protection of the general right of personality. In fact, it is not a restriction of the basic right itself, but of the number of persons who can be held responsible for violations of this right. This case-law recognised that not every member in a chain that leads to a violation has the same technical abilities to prevent further violations.

Personal information and pictures in computer games

The plot of computer games is not always entirely fictional; some of them use as models events and persons from real life, for instance, in sport simulations. The use of the name or prominent physical features of real-life persons can violate their general right of personality. It is doubtful whether in such a case, the evaluation is the same as in cases concerning films or books. Unlike publishing companies and film studios, the computer games industry cannot rely on the constitutional rights in Article 5 paragraph 1 GG.[38] It is even more difficult to say whether

[33] See F. Fechner and S. Popp, 'Informationsinteresse der Allgemeinheit', 03 *AfP* (2006) p. 213.
[34] H. Gersdorf, 'Caroline-Urteil des EGMR: Bedrohung der nationalen Medienordnung', *AfP* (2005) p. 221; however, see also R. Stürner, 'Caroline-Urteil des BGH: Rückkehr zum richtigen Maß', *AfP* (2005)p. 213.
[35] See LG Berlin 7 March 2005, *K&R* 2005 p. 334 at p. 335 et seq.
[36] Affirmative in this respect, O. Köster and U. Jürgens, 'Die Haftung von Suchmaschinen für Suchergebnisse', *K&R* (2006) pp. 108 et seq.
[37] See KG 20 March 2006, *MMR* 2006 p. 393 at p. 394; see also I. Stenzel, 'Über die Haftung des Metasuchmaschinenbetreibers für die Wiedergabe rechtswidriger Inhalte', *ZUM* (2006) pp. 405 et seq.
[38] See G. Zagouras and T. Körber, 'Rechtsfragen des Game-Designs – Die Gestaltung von Computerspielen und -animationen aus medien- und markenrechtlicher Sicht', 06 *WRP* (2006) pp. 680, 681; however, see also A. Lober and O. Weber, 'Entgeltliche und freie Nutzung von Persönlichkeitsrechten zu kommerziellen Zwecken im deutschen und englischen Recht', *ZUM* (2003) p. 658 at p. 674, holding a different view.

computer games are protected by the freedom of art (Art. 5 para. 3 GG). In the first decision of a county court on this issue, LG Hamburg argued that because of its creative elements, a computer game could be partly protected under Article 5 paragraph 3 GG.[39] However, the higher court in this case decided that the consent of the person at issue – in this case, the German National Soccer Team's goalkeeper – is needed to use his name, even if the game is considered as art.[40] Designing a virtual character who imitates a prominent sportsman is not driven by artistic intentions, but by the exploitation of the celebrity of the portrayed person. Therefore, the only basic rights that could justify an encroachment of the general right of personality are the freedom of occupation (Art. 12 para. 1 GG) and the guarantee of property (Art. 14 para. 1 GG).[41]

Current developments concerning data protection

The right of informational self-determination protects the individual against unbounded inquiry, storage, utilisation, and transmission of his personal data.[42] As in other legal systems, in Germany, data protection is also provided and implemented by a number of non-constitutional laws. Mostly, the Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG) applies, which regulates the general data responsibilities of the federal authorities and private individuals. Special rules concerning new technologies can be found in, for instance, the Telecommunications Act (*Telekommunikationsgesetz*, TKG), the Telecommunications Interceptions Ordinance (*Telekommunikationsüberwachungsverordnung*, TKÜV), and the Teleservices Data Protection Act (*Teledienstedatenschutzgesetz*, TDDSG). One of the most important changes in legislation was the implementation in 2004 of Articles 91-107 TKG, which contain rules about data transfer and reporting requirements of telecommunication providers.[43]

In principle, the basic right of informal self-determination is of significance for the interpretation of all of these laws. We go into two issues concerning new technology to show the constitutional data protection in detail. During a Data Protection Symposium in Cologne in 2005, the Federal Data Protection Commissioner gave an overview of more cases under discussion in Germany, such as an automatic emergency call system for motor vehicles, an electronic health card, and the collection of data for motorway toll levying.[44]

RFID

The right of informational self-determination includes the right of each individual to withhold the publication of personal facts.[45] Accordingly, the use of RFID technology, for example in passports, membership cards, or merchandise, could encroach upon this right. This is why public authorities need an Act of Parliament as a basis to authorise the use and analysis of RFID data. Such an Act would limit RFID's vast technical opportunities, in order to ensure constitutional proportionality.[46] At any rate, it is unconstitutional to generate a complete personality profile.[47]

In the business-customer relation, the consumer-goods industry does not require a basis of authorisation to use RFID in products. This means that, in contrast to public authorities, companies do not need a law that expressly empowers them to use RFID. However, the use of this technology by companies is limited by the Federal Data Protection Act. Up to now, it seems that this law covers all possible applications of RFID.[48]

Digital counterterrorism data base

[39] See LG Hamburg 25 April 2003, *ZUM* 2003, 689 – Oliver Kahn/Electronic Arts.
[40] Cf., S. Ernst, 'Zum Namensschutz bekannter Sportler bei Einsatz des Prominenten in einem Computerspiel', *CR* (2004) p. 227.
[41] See OLG Hamburg 13 January 2004, *ZUM* 2004 p. 309 at p. 310.
[42] See BVerfG 15 December 1983, *BVerfGE* 65, 1, 42; BVerfG 17 July 1984, *BVerfGE* 67, 100, 143; BVerfG 9 March 1988, *BVerfGE* 78, 77, 84; BVerfG 14 December 2000, *BVerfGE* 103, 21, 33.
[43] Before 2004 those duties were part of the Telecommunications Data Protection Ordinance.
[44] See P. Schaar, 'Datenschutz im Spannungsfeld zwischen Privatsphärenschutz, Sicherheit und Informationsfreiheit', 01 *RDV* (2006), pp. 1 et seq.
[45] See BVerfG 15. December 1983, 08 *NJW* (1984) p. 419.
[46] See U. Eisenberg and J. Puschke and T. Singelnstein, 'Überwachung mittels RFID-Technologie', 01 *ZRP* (2005) pp. 9, 10.
[47] See BVerfG 3 March 2004, 14 *NJW* (2004) p. 999 at p. 1004 and yet BVerfG 15 December 1983, *BVerfGE* 65, 1, 53.
[48] See B. Holznagel and M. Bonnekoh, 'Radio Frequency Identification – Innovation vs. Datenschutz?' 01 *MMR* (2006) p. 17 at pp. 19 et seq.

In September 2006, the federal states of Germany agreed on a draft law for implementing a counterterrorism data base, which had been under discussion since 2001. This data base would contain information on terrorism suspects' religion and their travel abroad. Under certain circumstances, these data would be available to the police and the intelligence services, as well as to the Customs Criminological Office. In spite of this having been discussed for almost five years, the measure is still very controversial – most notably concerning the constitutional right of informal self-determination. Several opposition parties described the draft as unconstitutional.[49] Meanwhile, the Federal Government has voted on the draft law.[50] The current draft bill seems to be a combination of two models: on the one hand, inserting full texts in the data base, and, on the other, inserting only an index in the data base. Each version is supported by one of the two parliamentary parties in the present large coalition.[51] This combination of models is both a political compromise and an attempt to ensure that the planned measures are proportional under constitutional law. Further developments are yet to be observed. However, regarding the relation of the right of informal self-determination to security and the proportionality of preventative measures, we refer to a decision of the Federal Constitutional Court of July 2005.[52] In this verdict, the Court set out patterns to determine when measures of prevention and preparatory prosecution measures ('Vorfeldmaßnahmen') are proportional. According to these, an important criterion is the precise and well-defined wording of the law that authorises such measures. The more important the fundamental right is that the measures infringe upon, the more precise the laws have to be.

5.3.2. Inviolability of the home

According to Article 13 paragraph 1 GG, the home is inviolable. The intention of this basic law is to secure a spatial sphere in which the individual can develop his private life.[53] This description of its aim shows the affinity of this basic right to privacy; as such, Article 13 GG is a *lex specialis* in relation to the general right of personality.

Yet the extent of protection does not only cover flats (including basement and attic), hotel rooms, and sleeper cabins, but also workrooms, service rooms, and offices.[54] Article 13 paragraphs 2-7 GG contains explicit rules when an encroachment on the right is justified; paragraph 2, for instance, stipulates that searches may be authorised only by a judge or, when speed is essential, by other authorities designated by law, and that they are carried out only in the manner therein prescribed.

Therefore, this basic right is said to be the most detailed in the German Constitution. Because of this, ICT measures encroaching on the rights granted by Article 13 paragraph 1 GG have to exactly fulfill the requirements of the codified exceptions. This may pose problems when new technologies emerge that provide new modes of observation, for example, electronic eavesdropping.

Electronic eavesdropping

The introduction of competences for the prosecution authorities to use wiretaps, bugs, and similar equipment in the domicile of suspects was similar to the cases concerning the general right of personality. The measures should be used for fighting organised crime. In 1998, the German Parliament had already changed Article 13 GG to pave the way for adopting these competences in the Code of Criminal Procedure. The change was necessary because the limits to the fundamental right of Article 13 paragraph 1, as stated in paragraphs 1 to 7, are very strict and exact. As electronic eavesdropping did not match one of the existing limits, new paragraphs covering the measures had to be set up in Article 13. In 2004, the Federal Constitutional Court

[49] See http://www.linksfraktion.de/pressemitteilung.php?artikel=1226929225 and http://fdp-fraktion.de/webcom/show_article.php/_c-334/_nr-486/_p-1/i.html.
[50] See http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2006/09/Antiterrordatei.html.
[51] See http://www.heise.de/newsticker/meldung/print/77693.
[52] BVerfG 27 July 2005, *DVBl* (2005) pp. 1192 et seq. – *Telekommunikationsgesetz Niedersachsen*.
[53] See BVerfG 26 May 1993, *BVerfGE* 89, 1, 12.
[54] See H. Jarass, in: J. Jarass and B. Pieroth, *Grundgesetz für die Bundesrepublik Deutschland – Kommentar* [Commentary of the Constitutional Law of the Federal Republic of Germany] (München, Beck 2004), Art. 13 ¶ 2.

decided that implementing acoustic domicile surveillance in the Code of Criminal Procedure, in its form at that time violated the general right of personality because the surveillance did not infringe an inner circle , which is the 'core of the relevant constitutional right' (*Kernbereich*). The inviolability of human dignity in Article 1 paragraph 1 GG demands the absolute protection of the inner circle within which private life is arranged.[55] This decision can be seen as modifying the hitherto existing system of different levels of protection of the general right of personality:[56] not only the intimate sphere, but also a certain part of the private sphere is inviolable.[57] This means that a clause enabling authorities to use new technologies to observe citizens – like the one in the StPO that implemented electronic eavesdropping – is only in agreement with the German Constitution if it does not touch upon the inner circle of privacy. Those clauses must contain regulations to immediately stop recording if the observed individual begins a private activity, such as a personal conversation with a family member, a soliloquy, or sexual intercourse. Furthermore, there must be regulations to ensure that if such data are recorded, they may not on any account be used and have to be deleted.[58] Critics of this prominent decision by the Federal Constitutional Court have noted that a clause that meets these demands cannot be practically implemented in criminal procedure.

Meanwhile, the clause concerned has been changed. Following the new Article 100c paragraph 4 StPO,[59] electronic eavesdropping may only be implemented if there are specific indications regarding the premises to be observed as well as the relationship between the persons to be observed, and if any utterances made within the person's most private sphere will not be subject to surveillance. Conversations within offices or other places of work will generally not be seen as part of a person's most private sphere. This is also valid for any conversations regarding criminal offences or any utterances by which criminal offences may be committed.

This new legislation has, again, met with some criticism. Some hold that even in its new version, the law violates constitutional rights.[60] In August 2005, the Federal Court of Justice (*Bundesgerichtshof*, BGH) decided on the first case affected by the new clause.[61] A soliloquy of a patient in his sickroom was considered part of the totally protected inner circle of the basic rights of the inviolability of the home in connection with the general right of personality.[62] As a result, the recorded data could not be used as evidence in a criminal proceeding.[63]

5.3.3. Inviolability of the body

Article 2 paragraph 2 GG underlines the importance of this fundamental right. It reads:

> [e]very person shall have the right to life and to physical integrity. The freedom of the person is inviolable. These rights may be interfered with only pursuant to a law.

In the following, we will concentrate on the developments of the right to life and the right to physical integrity.

Article 2 paragraph 2 GG has not been as closely examined in relation to the influence of ICT as other articles of the Constitution. We will therefore review a typical ICT issue, using new technology for searching the body, but we will also give some attention to biotechnology. Biomedical sciences are becoming more and more important in this context; for instance, deciphering the human genome would not have been possible without the accelerated progress of ICT. This is why we will also consider the main discussions concerning biotechnology with respect to Article 2 paragraph 2 GG.

---

[55] See BVerfG 3 March 2004, 14 *NJW* (2004) p. 999 at pp. 1003 et seq.
[56] See *supra*, section 5.3.1.1.
[57] For the further development of the dogmatics of the fundamental right to privacy by this decision, see also C. Gusy, 'Lauschangriff und Grundgesetz', *JuS* (2004) pp. 457 et seq.
[58] See BVerfG 3 March 2004, 14 *NJW* (2004) p. 999 at pp. 1005 et seq.
[59] As amended on 24 June 2005.
[60] See S. Leutheusser-Schnarrenberger, 'Der Gesetzentwurf der Bundesregierung zum „großen Lauschangriff"', 01 *ZRP* 2005 p. 1 at pp. 2 et seq.
[61] Based on the prior version of Art. 100c para. 4 StPO, but considering the decision of the Federal Constitutional Court.
[62] See BGH, 45 *NJW* (2005) p. 3295 at pp. 3296 et seq.
[63] Ibid. at pp. 3298 et seq.

New technology for searching the body

There has not been an extensive discussion in Germany whether measures like face recognition or terahertz cameras violate the right to physical integrity. The main focus of the discussion on these measures is their compatibility with the general right of personality and the right of informational self-determination.

Nevertheless, of course, the basic principles of the right to physical integrity can be adapted to such technologies. Physical integrity in terms of Article 2 paragraph 2 GG is the absence of pain, of infertility, and of deformation as well as of physical injuries.[64] Measures neutral to health, like taking a blood sample, as well as measures related to medical treatment, such as medical X-ray scans, are considered encroachments of the right to physical integrity.[65] Whether or not such an encroachment is justified depends again on an evaluation of rights and the proportionality in the concrete case.

A similar evaluation is required to determine the legitimacy of new identification measures with regard to the basic right to physical integrity. Again, there has not been a great deal of discussion in Germany so far, but this may change. After the successful implementation in November 2005 of electronic passports (ePass) with a chip containing a digital photograph, as of March 2007, these chips will also include digital fingerprints.[66] Moreover, the Federal Government has plans to introduce an electronic card for foreigners (*Elektronische Ausländerkarte*), which will contain similar data and biometric signatures as the ePass, and which will act as a digital residence permit.[67]

Biomedical sciences and biotechnology

The latest developments in biomedical sciences, like the decrihpering of the human genome or pre-implementation diagnostics, do not only affect the guarantee of human dignity in Article 1 paragraph 1 GG, but also the right to life and the right to physical integrity.[68] According to the prevailing opinion, the constitutional protection of life covers unborn life – starting with the nidation of the embryo.[69] Nidation is the implantation or 'nesting' of the early embryo in the uterus. With regard to the use of biotechnology, an important question is whether prenatal life is considered to be protected at the same level as postnatal life. Some constitutional lawyers argue that the full amount of protection is given only after birth, and they plead for protection to be divided into levels, in which the intensity of protection should rise progressively with the growth of the embryo.[70] Others argue that the Parliamentary Council that drafted the German Constitution did not take progressive extension of protection into consideration.[71]

Reproductive medication and pre-implementation diagnostics have given rise to special problems. To what extent do those technologies conform to Article 2 paragraph 2 GG? One part of the German jurisprudence wants to apply the same graded levels of protection used in the legal provisions regarding abortion.[72] However, the prevailing opinion probably distinguishes between *in vivo* and *in vitro* fertilisation: the protection of life *in vitro* would be even stronger, because in default of a physical connection to the womb, the constitutional right of self-determination of the mother cannot be regarded in the evaluation of rights.

---

[64] See BVerfG 17 January 1957, *BVerfGE* 6, 55; BVerfG 10 February 1960, *BVerfGE* 10, 322.
[65] See Hoffmann, in: B. Schmidt-Bleibtreu et al., *Kommentar zum Grundgesetz* [Commentary of the Basic Law], 10th edn. (Neuwied, Luchterhand 2004), Art. 2 ¶ 62.
[66] See the announcement by the Federal Ministry of the Interior on http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Themen/Informationsgesellschaft/DatenundFakten/Biometrie.html.
[67] This was recently announced by State Secretary August Hanning on 29 September 2006; see http://www.heise.de/newsticker/meldung/78841/.
[68] See Hoffmann, loc. cit. n. 65, Art. 2 ¶ 61.
[69] See BVerfG 28 May 1993, *NJW* (1993) p. 1751 at p. 1753; see also D. Lorenz, in: Isensee, *Handbuch des Staatsrechts für die Bundesrepublik Deutschland* [Manual for the Constitutional Law of the Federal Republic of Germany], Bd. 6, § 128 ¶ 12.
[70] See H. Dreier, 'Stufungen des vorgeburtlichen Lebensschutzes', 09 *ZRP* (2002) p. 377.
[71] See Roth-Stielow, 'Stufungen des vorgeburtlichen Lebensschutzes', 12 *ZRP* (2002) p. 530.
[72] See Art. 218 et seq. German Criminal Code (*Strafgesetzbuch*). See also T. M. Spranger, 'Biomedizin und vorgeburtlicher Lebensschutz', *SuP* (2003), p. 71.

Both pre-implementation diagnostics and reproductive medicine are prohibited, with criminal sanctions, by the Embryo Protection Law (*Embryonenschutzgesetz*, ESchG), .[73] Also, reproductive cloning is considered strictly unconstitutional.[74]

5.4. Communication-related rights

5.4.1. Secrecy of communications

The secrecy of communication has a constitutional source in Article 10 paragraph 1 GG, which reads:

> [t]he privacy of correspondence, posts and telecommunications shall be inviolable.

According to paragraph 2, restrictions may be made only pursuant to law. If the restriction serves to protect the free democratic basic order ('freiheitliche demokratische Grundordnung') or the existence or the security of the Federation or of a Federal State, the law may provide that the person affected shall not be informed of the restriction and that recourse to the courts shall be replaced by a review of the case by agencies and auxiliary agencies appointed by the legislature. Though the wording may suggest that this article contains several basic rights, the courts and legal scholars agree that Article 10 paragraph 1 GG covers one collective basic right. It is the right to confidentiality of individual communications, which – due to spatial distance – is dependent on a third party for transmission.[75] Thus, Article 10 paragraph 1 GG also protects the right of privacy, but it is a *lex specialis* in relation to the general right of personality.

In terms of Article 10 paragraph 1 GG, telecommunication is defined as any individual non-material transmission of information.[76] Only acts of individual communication are covered, not acts of mass communication like television or radio. The fundamental right in Article 10 paragraph 1 GG is not linked to a specific communication technology. Each electromagnetic and other immaterial forms of transmission are covered by the extent of protection, no matter if they are analogue or digital.[77] The scope of this constitutional right is dynamic, and so, new media are automatically included.[78]

This is unproblematic and without controversy as long as the new technology is a medium of individual communications, such as e-mail. The question whether a technology like the Internet at large, which is used for individual as well as for mass communications, is protected by Article 10 paragraph 1 GG has been discussed in greater detail. This discussion refers to the cumulative integration of networks and media services described as convergence, which may gradually implicate a merging of individual and mass communications.

Some argue that the extent of protection covers each medium as far as the technical method of transmission enables individual communications, no matter if the medium is also used for mass communications. Otherwise, one would have to differentiate according to the content of communication, and this would contradict the main intent of Article 10 GG, because one could only decide whether an act of communication is protected by this basic right *after* the content has been revealed and thus the right at issue has already been encroached.[79] In this view, the Internet as a whole would be protected by Article 10 paragraph 1 GG.

Others claim that such an enlargement of the extent of protection is only necessary when – due to digitisation – it is no longer possible to technically differentiate between individual and mass communications. However, such a differentiation is still feasible if the diverse media

---

[73] Embryonenschutzgesetz, last amended by Art. 22 of the Law of 23 October 2001.
[74] See M. Frommel, 'Stufungen des vorgeburtlichen Lebensschutzes', 12 *ZRP* (2002) p. 530.
[75] See BVerfG 9 October 2002, 14 BVerfGE 106, pp. 28 et seq. at p. 36.
[76] See Jarass, loc. cit. n. 54, Art. 10 ¶ 5.
[77] BVerfGE 106, 28, 36; see also C. Gusy, in: H. von Mangoldt, F. Klein and C. Starck, *Kommentar zum Grundgesetz, Band 1* [Commentary of the Basic Law – Volume 1] (München, Vahlen 2005), Art. 10 ¶ 40.
[78] See Löwer, in: I. von Münch and P. Kunig, *Grundgesetz-Kommentar, Band 1* [Commentary of the Basic Law, Vol. 1] (München, Beck 2000), Art. 10 ¶ 18.
[79] See Hermes, in: H. Dreier and H. Bauer, *Grundgesetz – Kommentar, Band 1* [Commentary of the Constitutional Law of the Federal Republic of Germany, Vol. 1] (Tübingen, Mohr Siebeck 2004), Art. 10 ¶ 35.

services are based on different transmission channels,[80] like broadband. In that case, protection under Article 10 paragraph 1 GG would cover only certain services of individual communication that use the Internet for transmission – like e-mail or VoIP – but not the Internet at large.

It is undisputed that Article 10 GG also protects the possibility of communicating without revealing one's identity.[81] Both the content of communications and the attendant circumstances – such as the time and the method of communication – are protected.[82] This holds for any new communication technology. For new technologies, however, specific problems may arise in determining when a communication starts and when it ends. This can be illustrated best with the legal practice concerning mobile phones, which we discuss below.

There is also a discussion in the literature whether and to what extent there is a more general right to anonymity.[83] However, the constitutional source discussed for such a right is not Article 10 GG or any other communication-related right, but the right of informational self-determination (Art. 2 para. 1 in conjunction with Art. 1 para. 1 GG). Therefore, the 'right to anonymity' – this term is hardly ever used – is seen as a specific part of data protection.

Requesting information from mobile radio providers

In 2000, an Administrative Court had to decide whether the request for data concerning an owner of a mobile phone was an encroachment of Article 10 paragraph 1 GG. The police authorities wanted to locate the owner's position using this information because they had lost his position and he was prone to suicide. The responsible authorities asked the telecommunication company with whom the missing person had a contract to pinpoint the location using the stand-by mode of this individual's mobile phone. To determine whether such a request requires an Act of Parliament as a legal basis, it had to be clarified when exactly the protection of Article 10 paragraph 1 GG begins. The court stated that the identification of the radio cell where the owner of a mobile phone is located is the result of an act of communication that has already started.[84] As a reason for expansion in time of the extent of protection, the court argued that the owner of a mobile phone is prepared for receiving a certain expected message or for phone calls in general. If he had to keep in mind that even the preparation for a communication act – i.e., taking his mobile phone in stand-by mode with him – could be used to locate his position, the freedom of communication would be diminished. In principle, this opinion was shared by some other courts and even the Federal Court of Justice.[85]

However, in August 2006, the Federal Constitutional Court decided that positioning a mobile phone via an IMSI catcher (a pseudo-network cell used to intercept identifying numbers of mobile phones in the vicinity) is not an encroachment of Article 10 paragraph 1 GG.[86] When using an IMSI catcher to locate the current radio cell of a mobile phone, only machines are communicating, and no exchange of information is made by humans, nor references to the content of communications. The mere fact of the technical function of a device as a communication medium and the emission of the device in its stand-by mode would not be considered as acts of communication in themselves, but only as the pre-condition of an act of communication. Moreover, it is true that the use of an IMSI catcher is an encroachment on the personal freedoms of Article 2 paragraph 1 GG, but whether such a measure is an unjustified infringement is mainly a question of proportionality. This depends on the individual case.

Another case, illustrating when the protection of Article 10 paragraph 1 GG ends, was also decided in 2006 by the Federal Constitutional Court. Public-prosecution authorities had confiscated an individual's mobile phone from their flat in order to view the SMS messages on that phone. According to this individual, this violated the right to secrecy of communication, among other fundamental rights. However, the court stated that when the transmission of data to

[80] See Löwer, loc. cit. n. 78, Art. 10 ¶ 18
[81] See Hoffmann, loc. cit. n. 65, Art. 10 ¶ 9.
[82] See Jarass, loc. cit. n. 54, Art. 10 ¶ 9.
[83] See H. Bäumler, 'Gibt es ein Recht auf Anonymität? Macht Anonymität heute noch Sinn?', *DuD* 2003, 160, as well as S. Klewitz-Hommelsen, 'Recht auf Anonymität?', *DuD* 2003, 159.
[84] See VG Darmstadt, *NJW* 2001, 2273, 2274.
[85] See BGH, *NJW* 2003, 2034, 2035, and BGH, *NJW* 2001, 1587.
[86] See BVerfG 22 August 2006, available at http://www.bverfg.de/entscheidungen/rk20060822_2bvr134503.html.

the mobile phone has ended, this transmission is no longer protected by Article 10 paragraph 1 GG but by the right of informational self-determination, and possibly by the inviolability of the home.[87] The main argument of the court was that when the process of data transmission has been completed, the data that are saved on the end device are no longer threatened by the same specific risks typical for using telecommunications.

5.4.2. Freedom of expression

Among other communication-related constitutional rights, the freedom of expression is guaranteed by Article 5 GG. Article 5 paragraph 1 reads:

> [e]very person shall have the right freely to express and disseminate their opinions in speech, writing, and pictures and to gather information themselves without hindrance from freely accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship.

According to paragraph 2, these rights are limited by the provisions of general laws, provisions for the protection of young persons, and by the right to personal honour. The freedom of expression is considered one of the most important fundamental rights;[88] it is said to be constitutive for a liberal democratic community.[89]

A recently discussed issue is the impact of Article 5 GG on the civil and criminal liability for hyperlinks. In April 2006, OLG Stuttgart had to decide whether Alvar Freude, a self-appointed multimedia artist, had committed a crime according to Article 86 of the German Criminal Code (*Strafgesetzbuch*), the distribution of propaganda items of unconstitutional organisations. The artist's website contained several links to pages of right-wing extremists displaying national-socialist symbols and texts. His own webpage also showed a documentary about freedom of speech, some statements against racism, and an appeal for an objective discussion with right-wing extremism. It was undisputed that the content of the extremist pages was liable to prosecution. However, Alvar Freude referred to the freedom of speech and the constitutional right to freedom of art. The court adjudicated that Alvar Freude had used the content of the linked websites with the purpose to facilitate forming an opinion.[90] In this case, the hyperlinks were therefore protected by the freedom of expression, and the court found the artist not guilty. This verdict shows how the constitutional right to freedom of speech has adapted to the different ways of expressing an opinion on new media like the Internet.

5.4.3. Freedom of assembly

Article 8 paragraph 1 GG states that all Germans shall have the right to assemble peacefully and unarmed without prior notification or permission. This basic right contributes to the development of citizens' personality as well as to political decision-making.[91]

Recently, the question has been raised whether online demonstrations are protected by Article 8 paragraph 1 or by any other basic right. The term 'online demonstration' (also known as 'virtual sit-ins') describes the coordinated, simultaneous request of data from a certain website by a large number of Internet users, with the intent to shut down the server of that site. Unlike DDoS attacks (distributed denial-of-services attacks), the initiators of an online demonstration do not use other people's computers without their consent, but they start a public appeal to other Internet users to join the 'demonstration'. In 2005, a local court stated that such an online demonstration is not protected by the freedom of assembly.[92] Although the relevant online activity was declared to the City Department of Public Order, the gathering of electronic signals caused by several humans to one server was not considered comparable to a real gathering of several people in one physical place. The judgement was annulled by the appellate court, but for other reasons than the

[87] See BVerfG, *NJW* 2006, 976, 979.
[88] See BVerfGE 62, 230, 247.
[89] See BVerfGE 82, 272, 281.
[90] See OLG Stuttgart, *MMR* 2006, 387, 390.
[91] See BVerfGE 69, 315, 344.
[92] AG Frankfurt 22 July 2005, unpublished.

applicability of Article 8 paragraph 1 GG.[93] The question whether or not such online demonstrations are protected by the freedom of assembly or the freedom of expression therefore remains unanswered.[94]

5.5. Conclusion

As we have shown, the wording of most privacy and communication-related basic rights of the German Constitution can be interpreted broadly. This facilitates an interpretation of the basic rights in order to incorporate new information and communication technologies. In particular, Article 2 paragraph 1 GG offers a flexible instrument to protect the individual from the application of new technologies by the state. Not as flexible as this comprehensive element are the special basic rights of Article 5 paragraphs 1 and 3 (including the freedom of expression and the freedom of art), Article 13 paragraph 1 (inviolability of the home), or Article 10 paragraph 1 GG (secrecy of communication), but that is also because these rights provide a higher level of protection. In fact, the extent of protection of Article 13 paragraph 1 GG – due to its closely-formulated restrictions in paragraphs 2 to 7 – is high and is still interpreted broadly. However, Article 10 paragraph 1 GG will probably only protect direct acts of communication. Therefore, Article 2 paragraph 1 GG and the general right of personality have an important back-up function.

This system of special basic rights ('spezielle Freiheitsrechte') and a catch-all basic right ('allgemeines Freiheitsrecht') enables a comprehensive and at the same time flexible approach to new information and communication technologies. Thus, there is no need for adapting the basic rights themselves. Any changes to the fundamental rights might even restrict their application regarding the further development of ICT, because they might be limited to current technology.

However, that does not imply that no action has to be taken by the legislator. The Federal Constitutional Court has declared that due to the fast process of technical development, the German legislator needs to be very attentive and must pass new (non-constitutional) laws swiftly when needed, in order to maintain a high standard of fundamental-rights protection.[95] We fully agree with the court's statement. It is important to keep a close watch on developments in ICT and to react promptly with appropriate legal measures.

References

Helmut Bäumler, 'Gibt es ein Recht auf Anonymität? Macht Anonymität heute noch Sinn?', *DuD* (2003) p. 160.

Horst Dreier and Hartmut Bauer, *Grundgesetz – Kommentar, Band 1* [Commentary of the Constitutional Law of the Federal Republic of Germany, Vol. 1] (Tübingen, Mohr Siebeck 2004).

Horst Dreier, 'Stufungen des vorgeburtlichen Lebensschutzes', 09 *ZRP* (2002) pp. 377-383.

Ulrich Eisenberg, Jens Puschke and Tobias Singelnstein, 'Überwachung mittels RFID-Technologie', 01 *ZRP* (2005) pp. 9-12.

Christian Engel, 'Auf dem Weg zum elektronischen Personalausweis: Der elektronische Personalausweis als universelles Identifikationsdokument', *DUD* (2006) pp. 207-210.

Stefan Ernst, 'Zum Namensschutz bekannter Sportler bei Einsatz des Prominenten in einem Computerspiel', *CR* (2004) pp. 227-228.

Frank Fechner and Susanne Popp, 'Informationsinteresse der Allgemeinheit', 03 *AfP* (2006) pp. 213-216.

Monika Frommel, 'Stufungen des vorgeburtlichen Lebensschutzes', 12 *ZRP* (2002) pp. 530-531.

Hubertus Gersdorf, 'Caroline-Urteil des EGMR: Bedrohung der nationalen Medienordnung', *AfP* (2005) pp. 221-227.

[93] OLG Frankfurt, *MMR* 2006, 547.

[94] See also Welp, *DFN Info-Brief*, September 2006, available at http://www.dfn.de/content/fileadmin/3Beratung/Recht/1infobriefearchiv/Infobrief-sept06.pdf.

[95] BVerfG, 08 *CR* 2005, 569.

Elke Gurlit, 'Die Verfassungsrechtsprechung zur Privatheit im gesellschaftlichen und technologischen Wandel', *RDV* (2006) pp. 43-50
Christoph Gusy, 'Lauschangriff und Grundgesetz', *JuS* (2004) pp. 457-262.
Bernd Holznagel and Mareike Bonnekoh, 'Radio Frequency Identification – Innovation vs. Datenschutz?', 01 *MMR* (2006) pp. 17-23.
Josef Isensee, *Handbuch des Staatsrechts für die Bundesrepublik Deutschland* [Compendium of the Constitutional Law of the Federal Republic of Germany] (Heidelberg, Müller 2004).
Hans Jarass, 'Bausteine einer umfassenden Grundrechtsdogmatik', 120 *AöR* (1995) pp. 345-381.
Hans Jarass and Bodo Pieroth, *Grundgesetz für die Bundesrepublik Deutschland – Kommentar* [Commentary of the Constitutional Law of the Federal Republic of Germany] (München, Beck 2004).
Sayeed Klewitz-Hommelsen, 'Recht auf Anonymität?', *DuD* (2003), p. 159.
Oliver Köster and Uwe Jürgens, 'Die Haftung von Suchmaschinen für Suchergebnisse', *K&R* (2006) pp. 108-112.
Sabine Leutheusser-Schnarrenberger, 'Der Gesetzentwurf der Bundesregierung zum "großen Lauschangriff"', 01 *ZRP* (2005) pp. 1-3.
Andreas Lober and Olaf Weber, 'Entgeltliche und freie Nutzung von Persönlichkeitsrechten zu kommerziellen Zwecken im deutschen und englischen Recht', *ZUM* (2003) pp. 658-675.
Hermann von Mangoldt, Friedrich Klein and Christian Starck, *Kommentar zum Grundgesetz – Band 1* [Commentary of the Basic Law – Volume 1] (München, Vahlen 2005).
Ingo von Münch and Philip Kunig, *Grundgesetz-Kommentar, Band 1* [Commentary of the Basic Law, Vol. 1] (München, Beck 2000).
Markus Ogorek, 'Anmerkung VGH Mannheim, Urteil vom 21.7.2003 – 1 S 337/02', *JA* (2004) pp. 608-610.
Alexander Rossnagel, Peter Welde, Volker Hammer and Ulrich Pordesch, *Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik* [Digitalisation of the Basic Rights? On the Constitutionality of Information and Communication Technology] (Opladen, Westdeutscher Verlag 1990).
Klaus Roth-Stielow, 'Stufungen des vorgeburtlichen Lebensschutzes', 12 *ZRP* (2002) p. 530.
Peter Schaar, 'Datenschutz im Spannungsfeld zwischen Privatsphärenschutz, Sicherheit und Informationsfreiheit', 01 *RDV* (2006) pp. 1-6.
Bruno Schmidt-Bleibtreu, Franz Klein and Hans Bernhard Brockmeyer, *Kommentar zum Grundgesetz* [Commentary of the Basic Law of the Federal Republic of Germany], 10th edition (Neuwied, Luchterhand 2004).
Fabian Schuster and Ulf Müller, 'Entwicklung des Internet- und Multimediarechts von Juli 2000 bis März 2001', 07 *MMR* (2001) pp. 1-40 (insert).
Fabian Schuster, Birgit Kemper, Ralf Oliver Schlegel, Marc Schütze, Jens Schulze zur Wiesche and Axel Sodtalbers, 'Entwicklung des Internet- und Multimediarechts im Jahre 2002', 05 *MMR* (2003) pp. 1-48 (insert).
Fabian Schuster, Birgit Kemper, Marc Schütze, Jens Schulze zur Wiesche, Sabine Charge and Laura Dierking, 'Entwicklung des Internet- und Multimediarechts im Jahre 2004', 05 *MMR* (2005) pp. 1-37 (insert).
Fabian Schuster, Birgit Kemper, Marc Schütze, Jens Schulze zur Wiesche, Sabine Charge and Laura Dierking, 'Entwicklung des Internet-, Multimedia- und Telekommunikationsrecht im Jahre 2005', 05 *MMR* (2006) pp. 1-48 (insert).
Tade Matthias Spranger, 'Biomedizin und vorgeburtlicher Lebensschutz', SuP (2003) pp. 71-78.
Igor Stenzel, 'Über die Haftung des Metasuchmaschinenbetreibers für die Wiedergabe rechtswidriger Inhalte', *ZUM* (2006) pp. 405-407.
Rolf Stürner, 'Caroline-Urteil des BGH: Rückkehr zum richtigen Maß', *AfP* (2005) pp. 213-221.
Constantin von Stechow and Michael von Foerster, 'Vereinbarkeit der Videoüberwachung öffentlicher Räume mit dem Recht auf allgemeine Persönlichkeit', *MMR* (2004) p. 202.
Hunold Wolf, 'Anmerkung BAG, Beschluss vom 29.6.2004 – 1 ABR 21/03', 02 *BB* (2005) p.108.
Georgios Zagouras and Thomas Körber, 'Rechtsfragen des Game-Designs – Die Gestaltung von Computerspielen und –animationen aus medien- und markenrechtlicher Sicht', 06 *WRP* (2006) pp. 680-690.

Chapter 6. Constitutional Rights and New Technologies in Sweden

Cecilia Magnusson Sjöberg[1]

6.1. Introduction

The constantly growing use of information and communications technologies (ICT) in Sweden has challenged constitutional rights in both expected and unexpected ways. It is, for instance, no surprise that the computerisation of society gives rise to questions concerning general technological adjustments of the fundamental laws of a nation's jurisdiction. To mention just a few core issues, law-making bodies need to take a position on (a) whether the legacy of constitutional rules should at all be applicable in a digital environment, (b) whether there is a need for adjustments, and (c) to what extent completely new legislation is required. Merely to determine the scope of a notion like 'official document' throughout the eras of a paper-based public sector to today's e-government[2] requires legal investigations of many varieties.

An obvious effect of modern ICT from a constitutional point of view is related to infrastructural changes. The use of ICT implies, namely, new conditions for division of powers, means for legal decision-making, complaints, remedies, etc. Yet another aspect concerns the impact of fundamental laws on legal information supply. Constitutional rights governing the powers of general administration set the framework for system architecture and design with consequences for both public and private actors on the legal information market.

The focus here is on the constitutional rights in Sweden. This calls for a brief introduction of the current legal framework. Sweden has a written constitution comprising the following four fundamental laws:

- the Instrument of Government,
- the Act of Succession,
- the Freedom of the Press Act, and
- the Fundamental Law on Freedom of Expression.

In addition to these fundamental laws, mention should be made of the Riksdag[3] Act, which may be referred to as a hybrid of a fundamental law an ordinary law.

With regard to the impact of ICT, the focus of this chapter will be on the following parts of the Swedish Constitution:

The Instrument of Government (SFS 1974:152)[4]
Chapter 1: Basic principles of the form of government
Chapter 2: Fundamental rights and freedoms
Chapter 8: Acts of law and other provisions
Chapter 11: Administration of justice and general administration

The Freedom of the Press Act (SFS 1949:105)
Chapter 2: On the public nature of official documents

The Fundamental Law on Freedom of Expression (SFS 1991:1469)
Chapter 1: Basic provisions

[1] Professor of law and informatics, LL.D., Director of the Swedish Law & Informatics Research Institute, Stockholm University, and Researcher at the Royal Swedish Academy of Sciences.
[2] A set of different models for public administration are presented in Petersson, Olof and Söderlind, Donald, *Förvaltningspolitik* [Public Administration Politics] (Stockholm 1993).
[3] The Swedish Riksdag may be conceived of as a parliamentary institution. See http://www.riksdagen.se.
[4] SFS stands for Svensk Författningssamling, i.e., the Swedish Code of Statutes.

Within the Swedish normative system, the fundamental laws take precedence over all other legal regulations. At the hierarchical levels below, there are (ordinary) laws decided by the Riksdag, government ordinances, and other provisions issued by public authorities. This structure implies that rules contained in the above-mentioned legislative cluster may not conflict with the provisions of the fundamental laws.

In order to protect the expressions for democracy manifested in the fundamental laws, the procedure for amendments is relatively more complicated than is the case with ordinary laws. An alteration of a fundamental law must be based on two identical decisions by the Riksdag separated by a general election.[5]

In this chapter, relatively much attention is paid to the constitutional right of access to official documents, given its central role in Swedish legal culture and society dating back to the 18th century. This does not, however, imply that privacy protection, which in practice often conflicts with the right of access, would not be conceived of as an important aspect of human rights currently being challenged by new technologies.

6.2. History of digital constitutional rights

Given the fact that the legal effects of new technologies in Sweden cannot in a meaningful way be associated with specific years, historical reflections will here be made over a broader time span. Generally speaking, there has over the years been a political consensus that new technologies should not be allowed to infringe upon constitutional rights. Of particular concern has been safeguarding the Swedish principle of openness, which dates back to 1766. A core feature of this principle is that the general public – as a major rule – is guaranteed a right of access to official documents, secrecy being applied only by way of exception.

During the 1970s, case law in combination with regulatory adjustments of Chapter 2 of the Freedom of the Press Act (FPA), which took place during the 1980s together with some supplementary amendments coming into force in 2003, have served as a means to accomplish this overall political goal. In fact, the scope of the Swedish principle of openness is considerably broader in a digital environment compared to a traditional paper-based administration.[6] At the same time, the other side of the coin shows the conflicting interest of privacy protection (see below).

There is no doubt that Sweden has a long and extensive tradition of using personal identification numbers for all kinds of data-base registrations, record linkages, and information exchange.[7]

Although privacy protection does not have as strong a constitutional position as the principle of openness,[8] the Instrument of Government explicitly states in Chapter 2, Article 3, paragraph 2, that

> (e)very citizen shall be protected, to the extent set out in more detail in law, against any violation of personal integrity resulting from the registration of personal information by means of automatic data processing.

The requirement of detailed regulation in law was first fulfilled by the Data Act – 'Datalagen' (SFS 1973:289). Today, the Personal Data Act (SFS 1998:204) is in force, representing Sweden's implementation of the Data Protection Directive (EC/95/46).

Actually, a critical factor in terms of constitutional rights has been Sweden's membership in the European Union. A sign of this was when the Data Protection Directive was decided and Sweden took an active part in the negotiations, resulting in consideration No. 72 in the Directive's preamble:

> [w]hereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive.

[5] More information about these procedures can be found at the official website of the Riksdag, http://www.riksdagen.se.
[6] See in more detail *infra*, section 6.5.
[7] Read more about Sweden as a surveillance society in, e.g., Flaherty, David, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (North Carolina Press 1989).
[8] In this context, more precisely, the right of access to official documents (see Ch. 2 FPA).

The major reason why Sweden took an explicit position in this matter was evidently the potential clash between the Swedish principle of openness and the privacy protection principles that the European Union requires a member state to implement.

In summary, the official regulatory approach to new technologies has over a long time period been to emphasise what has come to be referred to as technically neutral legislation. For example, when law-making bodies are faced with a need to adjust formal requirements for documents of different kinds to be conceived of as signed in a digital environment,[9] legal admissibility is expressed using wordings such as 'sufficiently secure' or 'using technical means ensuring control of sender, receiver, and data integrity'. A more technically oriented approach, on the other hand, would be to explicitly regulate the use of a particular technical method, for example PKI (Public Key Infrastructure) solutions or information standards like XML.[10] A drawback of the current approach to national regulation, i.e., the technically neutral one, is the inherent vagueness of this kind of legislation.

In this context, mention should be made of the fact that the National Archives, a public agency, recently published a report addressing long-term archiving of electronically signed documents.[11] The contents give rise to questions concerning a possibly new category of constitutionally relevant documents in relation to already existing ones. More precisely, it concerns what is to be conceived of as electronically signed data to be stored in public archives.

6.3. Changes in the constitutional system

No radical changes have been made to the constitutional system of Sweden since 2000. However, one should consider the internationalisation of society as such where legally relevant actions to a growing extent take place in global digital networks of different kinds. Of course, web technologies and telecommunications – with Internet in focus – have had a major impact on the freedoms of information and expression. From the year 2000 up till now, this has become particularly apparent in public awareness and general debates. Furthermore, today's parliamentary investigations into regulatory amendments with constitutional implications generally take new technologies into consideration either as a major or a peripheral aspect of the considerations being made.[12]

6.4. Privacy-related rights

6.4.1. Privacy and data protection

As mentioned above, the Instrument of Government sets out a requirement for privacy protection[13] in national law (Ch. 2, Art. 3, para. 2). This constitutional requirement has been

[9] See further EC Electronic Signature Directive, 1999/93/EC, and Magnusson Sjöberg, Cecilia and Nordén, Anna, 'Managing Electronic Signatures: Current challenges', *Scandinavian Studies in Law* Volume 47, *IT Law*, pp. 79-95 (Stockholm 2004).

[10] XML stands for eXtensible Markup Language. See further 'Main page for World Wide Web Consortium (W3C) XML activity and information': http://www.w3.org/XML/. About standardised markup languages in the legal domain, see Magnusson Sjöberg, Cecilia, *Critical Factors in Legal Document Management: A study of standardised markup languages*. The Corpus Legis Project (Stockholm 1998).

[11] *Elektroniskt underskrivna handlingar* [Electronically Signed Documents], Riksarkivet rapport 2006:1.

[12] For example SOU 2001:28, *Yttrandefrihetsgrundlagen och nya medier. Yttrandefrihetsgrundlagen och Internet. Utvidgat grundlagsskydd och andra frågor om tryck- och yttrandefrihet. Betänkande från Mediegrundlagsutredningen* [The Fundamental law on Freedom of Expression and new media. The Fundamental law on Freedom of Expression and Internet], SOU 2002:18, *Personlig integritet i arbetslivet. Betänkande från Integritetsutredningen* [Privacy Protection in working life], and SOU 2006:11, *Spel i en föränderlig värld, Betänkande av Lotteriutredningen* [Gaming in a changing world].

[13] Like in most other jurisdictions, there exists no official definition of how the notion of privacy is to be interpreted in the Swedish legal context. Reference is commonly made to a right of individuals to be left alone (under certain circumstances), a right to a private sphere, as well as a right to one's own personal data. Sometimes, privacy protection depends on the context, for instance, privacy protection differs in working life from that in private life. Furthermore, the strength of privacy protection might be related to the kind of data being processed. This implies that it is more important to protect sensitive personal data (race, ethnic origin, religious beliefs, etc.) than harmless personal data (a person's name, professional affiliation etc.). See further Öman, Sören and Lindblom, Hans-Olof, *Personuppgiftslagen: en kommentar* [The Personal Data Act; A Commentary] (Stockholm 2001); Prop. 2005/06:173, *Översyn av personuppgiftslagen* [Governmental Proposition, Overview

fulfilled by way of ordinary law, which does not only refer to the Instrument of Government but also reflects Sweden's membership of the European Union. As a matter of fact, the implementation of the European Data Protection Directive into the Personal Data Act (SFS 1988:204) has given rise to a number of issues of balancing the privacy-protection rules with other constitutionally manifested rules.

In order to clarify how the national rules on privacy protection stand against other constitutional principles, the Personal Data Act (hereinafter: PDA) contains a set of clarifying rules. Under the heading 'Relationship to freedom of the press and freedom of expression', Section 7 PDA states that:

> [t]he provisions of this Act are not applied to the extent that they would contravene the provisions concerning the freedom of the press and the freedom of expression contained in the Freedom of the Press Act or the Fundamental Law on Freedom of Expression.

In order to adjust data-protection rules to today's digital environment with Internet communications very much in focus, the Personal Data Act has been amended towards a so-called misuse model. Instead of regulating in detail under what conditions personal-data processing is allowed, the general goal of a regulatory approach based on misuse is to place an emphasis on general privacy-protection principles, letting law play a reactive role when things have gone wrong. The law-maker's intention is to facilitate personal-data processing in the context of, for example, ordinary word processing and web publications of pictures. The new rules will come into force on 1 January 2007.[14]

From a general point of view, this legal amendment is much sought after. However, the legal-technical solution has been questioned because of anticipated practical difficulties to distinguish so-called structured personal data processing from the unstructured processing to which the misuse model will apply. Yet another question mark may be raised as to whether the new reading of the Personal Data Act (Art. 5a) fully complies with the legal framework set out in the EC Data Protection Directive.

Privacy protection versus freedom of expression

A case decided by the Supreme Court of Sweden highlights the conflicting interests between privacy protection and freedom of expression.[15] The case concerned a private individual, Ramsbro, who availed himself of the Internet to express his disappointment regarding economic advice he had received from his private bank. Under the heading 'Foundation against Nordbanken' (i.e., the financial institution in question), he published an 'electronic pillory' of directors who in his opinion had neglected their advisory duties. The major legal issue in this case, through its progress from lower courts to the Supreme Court, concerned whether the homepage constituted an infringement of the provisions contained in the Personal Data Act (in particular rules regulating transfer of personal data to third countries) or whether the publication of personal data had occurred exclusively for journalistic purposes (Article 7 para. 2 PDA).

The Supreme Court reached the conclusion, with reference to Article 9 of the EC Data Protection Directive and Articles 8 and 10 of the European Convention of Human Rights that the insulting statements published on the Internet fell within the scope of the exception for journalistic purposes, as interpreted in relation to underlying rules of freedom of expression, given the fact that the aim was to inform, criticise, or initiate a debate concerning issues of relevance for society and the general public.

In a similar case concerning privacy protection versus freedom of expression, a Court of Appeal[16] explicitly referred to the reasoning in the above-mentioned Ramsbro case. Here, the issue concerned the publication of a 'gallery of criminals' on the Internet. The background was claimed economic losses as a result of road-traffic works and allegedly destroyed privately-owned woods in connection with this. The 'gallery of criminals' included names and photos of contractors

---

of the Personal Data Act]; SOU 2004:6, *Översyn av personuppgiftslagen* [Overview of the Personal Data Act].

[14] See further Prop. 2005/06:173, *Översyn av personuppgiftslagen* [Governmental proposition, Overview of the Personal Data Act].

[15] NJA 2001, p. 409.

[16] Hovrätten för västra Sverige, Mål T 2505-01, June 2002.

and public officials of the Swedish Road Administration. The Court of Appeal found that publication of personal data on the homepage was not illegitimate, as the exception for journalistic purposes applied. However, the processing in this case was deemed to be in conflict with the rule of defamation[17] in the Criminal Code, and a fine was set at 5,000 SEK (approximately 545 EUR).

These two cases illumistrate that the expression 'journalistic purposes' is to be interpreted broadly in the direction of freedom of expression, in contrast to a narrower meaning associated with work carried out by professional journalists affiliated with mass-media enterprises. Additionally, this case-law shows how the rules contained in the Personal Data Act can be marginalised and how, at the same time, other legal rules, here the Criminal Code, come into the picture.

The very scope of the EC Data Protection Directive as implemented into national privacy legislation was under consideration in the *Lindqivst* case. More precisely, it was the first time that the Court of Justice of the EC ruled on the movement of personal data on the Internet.[18] The history of this case began in 1998 when Lindqvist, a voluntary parish worker, practiced her newly acquired HTML skills, by designing a homepage (on her own personal computer) with data about herself and 18 of her colleagues. The overall purpose was to easily provide young parishioners preparing for Confirmation with information that they might need. To exemplify, Lindqvist published names, contact data, work carried out, and her colleagues' hobbies – described in mildly humorous terms – mentioning also that one of her colleagues had injured her foot and was working part-time on medical grounds.

Lindqvist's homepage – which was linked to the Swedish Church's web server for only a few days – led to quite strong reactions among some of her colleagues, and in order to clear herself from having done anything illegal she reported herself to the police. The unexpected effect of this, from her point of view, was that the District Court found her guilty of several offences against the Personal Data Act and she was fined 4,000 SEK (approximately 450 EUR). Lindqvist appealed against the decision, and the Court of Appeal asked[19] the EC Court of Justice a set of questions which lead to the following clarifications (2003).

- Referring to individuals on a homepage in terms of, e.g., name, telephone numbers, working place, and hobbies, is to be regarded as wholly or partly automated processing of personal data.
- The EC Data Protection Directive does not presume a direct connection with the free movement in every processing situation, as the scope of application then would be too vague.
- Publications on the Internet cannot be defined as processing of a purely private nature, as the personal data are made public and accessible for an unlimited number of people.
- The expression 'personal data concerning health' should be given a broad meaning, implying that data about an injured foot and part-time work on medical grounds are to be regarded as sensitive personal data.
- Publication of personal data on a homepage does not necessarily constitute a third-country transfer.[20] Decisive factors in this respect are the location of the server and the required measures for accessibility.

Considering the focus of this chapter – constitutional rights and new technologies – it is interesting to note also that the Lindqvist case illuminates the question whether the EC Data Protection Directive would be in conflict with the freedom of expression. The European Court of Justice clarified that the provisions of the directive do not in themselves restrict the principle of

[17] Chapter 5, Article 1 CC states: '[a] person who points out someone as being a criminal or as having a reprehensible way of living or otherwise furnishes information intended to cause exposure to the disrespect of others, shall be sentenced for *defamation* to a fine.'
[18] European Court of Justice 6 November 2003, Case C-101/01 (*Lindqvist*).
[19] Göta hovrätt (2001), Case No. B 747-00.
[20] It has not been intended that the expression 'transfer of data to a third country' should comprise every kind of Internet publication even if data thereby are made accessible to persons in third countries. In the follow-up case of *Lundsberg*, the Supreme Court of Sweden (NJA 205, p. 361) adhered to the reasoning of the European Court of Justice concerning third-country transfers.

freedom of expression or any other fundamental right for that matter. At the same time, the court made a point of the principle of proportionality being central not least in legal assessments made by national authorities and courts where there is an overall obligation to ensure a fair balance between the rights and interests in question, including fundamental rights.

The case was sent back to the Göta Court of Appeal, and it was finally settled that a crime against the provision of notification to the national supervisory authority had been committed, as well as unlawful processing of sensitive personal data. These acts, however, were regarded as petty offences.[21] Furthermore, Lindqvist claimed that the exception for personal processing exclusively for journalistic purposes ought to apply to her case, but the court rejected this because of the personal data processing in question being of a too general character (cf., above).

Privacy protection versus right of access to official documents

Under the heading 'Relationship to the principle of public access to official documents', Section 8 of the PDA states that

> [t]he provisions of this Act are not applied to the extent that they would limit an authority's obligation under Chapter 2 of the Freedom of the Press Act to provide personal data.
>
> Nor do the provisions prevent an authority from archiving or saving official documents or that archive material is taken care of by an archive authority. The provision of Section 9, fourth paragraph,[22] does not apply to the use by an authority of personal data in official documents.

In spite of the formal clarification that the constitutional Swedish principle of openness should be given priority over privacy-protection rules laid down in an ordinary law, a rather delicate rule interpretation and rule application have occurred in practice. An underlying reason for this is that a provision in Chapter 7, Article 16 of the Secrecy Act introduces privacy protection as a secrecy ground. In cases where the general public take advantage of their right of access to public documents and the required public document in question contains personal data, the public agency should – given indications of doubt – consider whether the future processing of those personal data will comply with the rules in the Personal Data Act.

At first glance, it might appear as if the privacy rules will in all cases be an obstacle to the principle of openness having any real effect. However, the formal construction of the applicable secrecy rule is that of a so-called explicit (straightforward) condition for secrecy, which implies publicity as a major rule and secrecy as the exception. In practice, this means that a public official should only consider the rules in the PDA when there are particular circumstances that call for attention, for instance, with regard to the kind and quantity of data requested.

Furthermore, not everyone who takes advantage of the principle of publicity falls within the application area of the PDA. Section 6 PDA states that the Act 'does not apply to such processing of personal data that a natural person performs in the course of activities of a purely private nature'. Furthermore, major rules of the PDA do not apply to such processing of personal data as occurs exclusively for journalistic purposes or for artistic or literary expression. At the same time, the constitutional right expressed in terms of the principle of openness is challenged by the application of Chapter 7, Article 16, in that it creates more situations where it is legitimate for a public official to infringe upon the otherwise protected anonymity of an individual and acknowledges the former's right not to state the reason for his or her request.

At a more fundamental level, it might be questioned how the government's official standpoint that the principle of publicity should not be infringed upon by Sweden's membership in the European Union – and the associated obligation to implement EC directives – complies with the rule of the Secrecy Act allowing for the Personal Data Act (under certain circumstances) to be a basis for secrecy. The current national legal situation may be explained with reference to the construction of the Swedish principle of publicity, which was evidently designed in such a way as to explicitly include secrecy; a so-called official document may be either public or secret. From that point of view, it is reasonable that also privacy rules may be a foundation for secrecy, as

[21] Göta hovrätt, Decision 2004-04-07, B 747-00.

[22] Section 9 para. 4 reads as follows: 'Personal data that are processed for historical, statistical, or scientific purposes may be used in order to take measures as regards the person registered only if the person registered has given his/her consent or there is extraordinary reason having regard to the vital interests of the registered person.'

these fall into the generally accepted exceptions to openness, namely, the protection of personal or economic circumstances of private subjects (see Chapter 2, Article 2 FPA).

A case decided by the Supreme Administrative Court illustrates the current balancing between the right of access to public documents on the one hand and the need for privacy protection on the other.[23] The case concerns dissemination of a file kept by the Swedish National Board of Student Aid (CSN) containing data on students receiving study loans. The purpose of the request by the company Mecenat AB was to use the data for direct-marketing activities. In contrast to the lower instances, the Supreme Administrative Court found that the file should be made public, having considered the kind of personal data involved and the purpose of the planned processing.

The legal reasoning in this case proceeds from the premise that the requested data comply with the conditions of what constitutes an official document (here a recording of compiled data) according to Chapter 2, Article 3 of the Freedom of the Press Act (see further below). The next step in the legal assessment concerns whether the recording is to be considered public or secret (wholly or partly). This is where Chapter 7, Article 16 comes into the picture, which leads the court to assess whether the anticipated personal-data processing by Mecenat AB was legitimate according to the provisions of the PDA. The court weighed the relevant interests as prescribed by Section 10(f) PDA, which reads as follows.

> Personal data may be processed only if the registered person has given his/her consent to the processing or if the processing is necessary in order (…)
>
> (f) that a purpose that concerns a legitimate interest of the controller of personal data or of such a third party to whom personal data should be able to be satisfied, if this interest is of greater weight than the interest of the registered person in protection against violation of personal integrity.

Having considered that the request concerned direct marketing of discount offers for students which cannot be said to infringe upon privacy (merely one marketing activity per academic term), and that the kind of personal data to be processed were not sensitive (name, address, etc.), the court reached the conclusion that the legitimate interest of the company to process the data was stronger than the need for privacy protection. Furthermore, the court pointed to the rule (Section 11 PDA) stating that personal data may not be processed for purposes concerning direct marketing, if the registered person gives notice in writing to the controller of personal data that he or she opposes such processing.

In conclusion, the current situation in Sweden is that the legal system guarantees access to official documents containing personal data that are not sensitive regardless of the commercial purpose of such a request involving processing that falls within in the scope of the Personal Data Act.

6.4.2 Inviolability of home and body

The core constitutional right concerning inviolability of home and body is laid down in Chapter 2, Article 6 of the Instrument of Government:

> Every citizen shall be protected in his relations with the public institutions against any physical violation also in cases other than cases under Articles 4 and 5. He shall likewise be protected against body searches, house searches and other such invasions of privacy, against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications.

Technological developments have gradually come to challenge these aspects of privacy protection. Of particular interest today is collection of geographical position data and the use of Radio Frequency Identifiers (RFID). It is important to realise that it is not new technologies as such that constitute risks of privacy infringements, but rather the infrastructural changes associated with implementing and using digital applications. This is similar to saying that in order to investigate the factual or potential inviolability of home and body, also legal and organisational infrastructures need to be taken into consideration.

With regard to legal infrastructures, a challenge from the point of view of rule interpretation is of course that the provisions in the catalogue of fundamental rights and freedoms in Chapter 2 of

[23] RÅ 2002 ref. 54.

the Instrument of Government were drawn up before the current digital information society, where immaterial objects and circumstances are much more in focus. Evidently, the Act about general camera surveillance[24] serves the purpose of privacy protection by requiring adequate consideration of individuals' needs in this respect. For instance, these are met by means of posters and other information signs announcing the surveillance. Application for permission is only required when a surveillance camera is to be used in public places. Furthermore, a sign of changed organisational infrastructures is ICT-supported distance-working, which gives rise to issues concerning the borderline between working place and the private sphere at home, when personal computers and mobile phones are common commodities.

Noteworthy in this context is the research project 'Privacy in the Making' (the Prima Project),[25] which investigates how ICT enables electronic projections of identities, encompassing also physical boundaries, physical artefacts, etc. Mention should also be made of an interdisciplinary research project concerning biobanks data and the law.[26] One key issue in this context is how to legally define the contents of a biobank. Of particular interest is the Act about Genetic Integrity etc.,[27] which prohibits using genetic examinations and information as a condition for contractual agreements. According to this Act, the search for and use of genetic information must be founded on legal regulations. The genetic-integrity law also prohibits unauthorised access to genetic information.

6.5. Communication-related rights

6.5.1. Secrecy of communications

The Instrument of Government guarantees every citizen protection against examining mail or other confidential correspondence, and against eavesdropping and recording telephone conversations or other confidential communications (Chapter 2, Article 6). Evidently, new technologies provide different kinds of actors with tools that, depending on their use, may challenge the right to secrecy of communications.

In Sweden, there is, for instance, a growing concern about how to uphold the secrecy of communications in working-place environments. Private use of employers' information systems, including Internet services, have been in focus for public inquiries,[28] which have not, so far, led to any revisions of the privacy legislation. A key issue in this context concerns the right – if any – of an employer to read an employee's private e-mail messages.[29] The legal situation may be summarised as follows. The starting point is the right of management founded on general labour-law principles, for example, a right to direct and divide work tasks. Given the fact that an information system (including hardware, software and communications facilities) is to be conceived of as equipment belonging to employers, they have the right to decide which equipment to use and how. Of utmost importance though is that these management rights are carried out pursuant to law and good practices.

From the above, it follows that an employer is free to set up an Internet policy prohibiting private e-mail correspondence. In practice, though, it is impossible to fully prevent the incoming of private e-mail messages and, therefore, it is necessary, in spite of a possibly prohibitive Internet policy, to take into consideration the applicable legal rules concerning rights of access to private messages. There is no doubt that an employer may be inclined to access all kinds of electronic messages, and in particular e-mail. To begin with, the rules in the Personal Data Act apply to the processing of personal data involved in an employer's – or an associate's – reading of a private

[24] *Lagen om allmän kameraövervakning*, SFS 1998:150.
[25] The project is hosted at the Swedish Institute of Computer Science with the Swedish Institute for Law and Informatics as one of the partners. See further http://www.sics.se/prima.
[26] Read more in Sanna Wolk ed., *Biobanksrätt* [Biobanks Law] (Lund 2003). See also the homepage of the Swedish National Biobank Program: http://www.biobanks.se.
[27] *Lagen om genetisk integritet m.m.*, SFS 2006:31.
[28] See in particular SOU 2002:18, *Personlig integritet i arbetslivet. Betänkande från Integritetsutredningen* [Privacy Protection in working life]. See also Westregård, Annamaria, *Integritetsfrågor i arbetslivet* [Personal Privacy Issues in Working Life].
[29] See further Datainspektionen, *Personuppgifter i arbetslivet* [Personal Data in Working Life], Datainspektionen informerar Nr 7, 2001.

message[30] in electronic format. This gives rise to considerations of what can make the personal-data processing legitimate.

In principle, the processing could be based on a data subject's consent (see Art. 10 PDA). It is, however, difficult to obtain valid consent due to the requirement of a voluntary expression in an employment situation, where the voluntariness may be debatable. In practice, the legitimacy of an employer's processing of private e-mail therefore primarily depends on the outcome of a weighing of interests as set out in Article 10(f) PDA (see above, section 6.4.1). One such a legitimate interest concerns the need to uphold information security within an organisation. Another critical factor in the weighing of interests concerns the way in which the employer (or his or her representative) accesses the messages. Here, a distinction can be made between going through a log of transmitted mail as opposed to actually reading the contents of separate messages. In all circumstances, the controller must comply with the duties to inform the data subjects according to Articles 23-26 PDA.

Of relevance in this context, but without certainty as regards applicability in a digital environment, is also the regulation of intrusion into a safe depository in Chapter 4, Article 9 CC:

> [a] person who, in a case not covered by Section 8,[31] unlawfully opens a letter or a telegram or otherwise obtains access to something kept under seal or lock or otherwise enclosed, shall be sentenced for *intrusion into a safe depository* to a fine or imprisonment for at most two years.

Another complicating factor is that the mere convention for sending e-mail messages implies private communication, and from that point of view, might trigger applicability of this provision of the Criminal Code. More precisely, by placing an individual's name before the associated organisation (private enterprise, public authority, etc.), privacy is signaled. It has therefore been recommended, for instance by the Swedish Ombudsmen of Justice (JO), to request authorisation from the employees to facilitate the lawful handling of e-mail messages.

Depending on the permissive or prohibitive character of an Internet policy governing the conditions for private use of computers, yet another rule in the Criminal Code must be taken into consideration, namely the provisions regulating breach of data secrecy (Ch. 4, Art. 9c CC):

> [a] person who, in cases other than those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for *breach of data secrecy* to a fine or imprisonment for at most two years. A recording in this context includes even information that is being processed by electronic or similar means for use with automatic data processing.

From a constitutional point of view, it is furthermore important to point out the fundamental right to convey information for the purpose of publication in print and production of public recordings. This is laid down in Chapter 1, Article 1 FPA[32] and Chapter 1, Article 2 of the Fundamental Law on Freedom of Expression (FLFE).[33] These rules apply also in a situation where an employee uses e-mail for this kind of messaging. Given the fact that e-mail is commonly quite a public means for communication, it might not be the wisest tool for an individual. However, should an employer (or his or her representative), when reading a private e-mail message for a legitimate reason, find that the employee in question takes advantage of his or her right to convey information for publication, the employer must 'stop reading', as the constitutional rights in the FPA and FLFE take precedence over the provisions of ordinary laws, such as the Personal Data Act.

---

[30] Of course, it is not always obvious what constitutes private information on the one hand and work-related information on the other. This is typically the kind of legal assessment that digitally supported working-place environments give rise to.

[31] Chapter 4, Article 8 of the Criminal Code: '[a] person who unlawfully obtains access to a communication which a postal or telecommunications firm delivers or transmits in the form of mail or as a telecommunication, shall be sentenced for *breach of postal or telecommunication secrecy* to a fine or imprisonment of at most two years.'

[32] 'All persons shall likewise be free, unless otherwise provided in this Act, to communicate information and intelligence on any subject whatsoever, for the purpose of publication in print, to an author or other person who may be deemed to be the originator of material contained in such printed matter, the editor or special editorial office, if any, of the printed matter, or an enterprise which professionally purveys news or other information to periodical publications' (Ch. 1, Art. 1 FPA).

[33] 'Every Swedish citizen is guaranteed the right to communicate information on any subject whatsoever to authors and other originators, as well as to editors, editorial offices, news agencies and enterprises for the production of technical recordings for publication in radio programmes or such recordings. He also has the right to procure information on any subject whatsoever for such communication or publication. No restriction of these rights shall be permitted other than such as follows from this Fundamental Law' (Ch. 1, Art. 2 FLFE).

In addition to the above-mentioned legal considerations, there are more general discussions in Sweden concerning interception and (secret) surveillance, for instance by way of cameras (see above). Prior to the shift of political power as a result of the general election in Autumn 2006, the socialist government manifested rather strong politics in favour of different kinds of surveillance methods. The new right-wing allied government has stated that it will postpone the prior government's proposals within this area, pending the reports of a set of public inquiries addressing, for example, a possible obligation to inform intercepted subjects of the surveillance in question and general needs for privacy protection in society.[34]

6.5.2 Freedom of expression

The Fundamental Law on Freedom of Expression (SFS 1991:1469) states in its basic provisions (Ch. 1, Art. 1) that

> every Swedish citizen is guaranteed the right under this Fundamental Law, vis-à-vis the public institutions, publicly to express his thoughts, opinions and sentiments, and in general to communicate information on any subject whatsoever on sound radio, television and certain like transmissions, films, video recordings, sound recordings and other technical recordings.

There is no doubt that technical developments challenge the provisions contained in this fundamental law, which has already been adjusted in order to more adequately mirror modern society. For instance, the application area of the rule offering constitutional protection for data bases (Ch. 1, Art. 9) has been extended in order to cover printing-on-demand activities as well as the use of push technologies used in order to fulfil requests for information by the general public that has been agreed upon beforehand.

A public inquiry has yet again investigated the need for amending the constitutional framework of freedom of the press and freedom of expression. In its report,[35] the public inquiry presents three alternatives for how to strengthen the rights. According to the first alternative, the Freedom of the Press Act and the Fundamental Law on Freedom of Expression (FLFE) will cease to exist as specific fundamental laws. Instead, the major principles laid down in these to laws will be transferred, in somewhat other wordings, into the Instrument of Government, placing an emphasis on excluding censorship and safeguarding the freedom of expression. The second alternative is rather similar to the first one, in that the FPA and the FLFE would be repealed and the freedom of expression would be directly protected by the European Convention of Human Rights. More detailed rules would, according to this alternative, be enacted in an ordinary law. The third alternative, finally, proposes a merger of the FPA and the FLFE to constitute a new fundamental law on freedom of expression. The next step in this law-making procedure is for the report to be sent out for referral to a wide cross-section of Swedish public and private organisations.

As regards the current application of the FLFE in a digital context, certain provisions of Chapter 1 call for attention, in particular with regard to Internet publications. In this context, it is important to note that the FLFE is only applicable to static services, and not to interactive applications such as chat sites.[36] According to Chapter 2, Art. 9.2 FLFE, a non-interactive publication by an editorial office is protected by the so-called data-base rule:

---

[34] In this context, the following two rules in the Criminal Code should be mentioned. First, the provision about eavesdropping in Chapter 9a CC: '[a] person who, in a case other than as stated in Section 8, unlawfully and secretly listens to or records by technical means for sound reproduction, speech in a room, a conversation between others or discussions at a conference or other meeting to which the public is not admitted and in which he himself does not participate, or to which he has improperly obtained access, shall be sentenced for *eavesdropping* to a fine or imprisonment of at most two years.' Second, the supplementary provision of Chapter 4, Article 9c, section 9b: '[a] person who employs technical means with the intention of committing a breach of telecommunication secrecy in the manner stated in Section 8 or to commit a crime as defined in Section 9a, shall be sentenced for preparation of such a crime to a fine or imprisonment for at most two years if he is not responsible for a completed crime.'

[35] SOU 2006:96, *Ett nytt grundlagsskydd för tryck- och yttrandefriheten* [A new constitutional protection for freedom of the press and freedom of expression].

[36] In this context, mention should also be made of Chapter 1, Art. 7, para. 2 FPA, which offers protection for (unaltered) electronic versions of periodicals: '[i]f the owner of a periodical disseminates or causes to be disseminated the contents of the periodical, or parts thereof, in the form of a radio programme or technical recording under the Fundamental Law on Freedom of Expression, the programme or technical recording shall be equated, in respect to the application of Chapters 1 to 14, with a supplement to the periodical, insofar as the version disseminated in such form reproduces the contents of the periodical in

> [t]he provisions of this Fundamental Law concerning radio programmes apply also in cases in which the editorial office of a printed periodical or a radio programme, an enterprise for the professional production of printed matter or matter equated with printed matter under the Freedom of the Press Act, or of technical recordings, or a news agency, with the aid of electromagnetic waves
>
> 1. supplies to the general public, in response to a special request, information taken from a data base the content of which can be modified only by the person carrying out the activity, either by direct transfer, or indirectly by the production of a technical recording, written document or picture; or
>
> 2. otherwise, in accordance with a prior agreement, supplies information to the public by direct transfer from a data base under 1.

Chapter 1, Article 9, section 2 FLFE offers protection for non-interactive electronic services, on the condition that a valid certificate[37] – after application – has been granted a qualified responsible editor. Further conditions for a certificate to be issued are accessibility for the general public, a certain connection to Sweden, and that the service has a name that does not pose a risk of being easily confused with another activity (regulated by the FLFE).

The most important effect of adhering to the legal framework of the FLFE is protection against interventions by the public that might restrain the freedom of expression. This is similar to saying that the Personal Data Act is not applicable and, consequently, the Data Inspection Board is not authorised to carry out any supervisory activities concerning a website protected under the FLFE. Furthermore, criminal responsibility for what has been published is directed to a singular person, i.e., the responsible editor. Mention should here be made also of a quite burdensome rule, stating that the responsible editor is obliged to document all changes of the protected service.

An examination of the application of this fundamental law in practice shows that quite a few public agencies have applied for and also received certificates. As a matter of fact, this procedure may be questioned from a constitutional point of view. After all, the very basis for the FLFE is to offer every Swedish citizen rights vis-à-vis public institutions. To extend this right of protection to be applied also within the public sector is definitely not in obvious compliance with the constitutional legal framework.

In addition to this formally oriented comment, any organisation considering applying for a certificate should assess whether the service in focus will remain static or whether it will include interactive functions. If a service develops into not being exclusively static, the organisation will end up having to comply with both rules contained in the FLFE and the provisions of the PDA.

6.6. Other constitutional rights

6.6.1. Access to official documents and the Swedish principle of openness

The constitutional framework of the public nature of official documents in Sweden implies that openness is the major rule, offering the general public a right of access to official documents (Ch. 2 FPA). Under certain circumstances, an official document may be withdrawn from publicity with reference to a specified rule in the Secrecy Act (SFS 1980:100). It should be noted, however, that the right of access to official documents may be restricted only if it is necessary with regard to the following interests of secrecy:

1. the security of the Realm or its relations with another state or an international organisation;
2. the central fiscal, monetary, or currency policy of the Realm;
3. the inspection, control, or other supervisory activities of a public authority;
4. the interest of preventing or prosecuting crime;
5. the economic interest of the public institutions;
6. the protection of the personal or economic circumstances of private subjects;
7. the preservation of animal or plant species (Ch. 2, Art. 2 FPA).

---

unaltered form and indicates how the contents have been disposed. A special obligation to record such programmes, and retain technical recordings and keep them available, may be laid down in law. Rules concerning the right to broadcast are contained in Chapter 3 of the Fundamental Law on Freedom of Expression.'

[37] A certificate is valid for 10 years at a time by the Swedish Radio and TV Authority.

The conditions for what constitutes an official document are found in Chapter 2, Article 3 FPA. This provision illustrates an approach where the law-making bodies have chosen to incorporate new technologies into a legal framework with a long historical tradition:

> [d]ocument is understood to mean any written or pictorial matter or recording which may be read, listened to, or otherwise comprehended only using technical aids. A document is official if it is held by a public authority, and if it can be deemed under Article 6 or 7 to have been received or drawn up by such an authority.

In fact, this provision contains two parallel sets of legal conditions: one aiming at traditional paper documents and the other bringing in new ICTs referred to as 'recordings'. There is no doubt that this provision deserves particular attention because of its constitutional importance and legal-technical complexity.

To begin with, the target of the principle of openness is 'documents', which is a fairly understandable notion in a paper-based public sector. The corresponding e-government term is 'recording which may be read, listened to, or otherwise comprehended only using technical aids'. In more practical terms, a 'recording' may be explained as 'a meaningful collection of data'. This is similar to saying that the notion of a document is comparatively more dynamic in a digital environment, which commonly is manifested by using the expression 'potential document'. Furthermore, it should be noted that the perspective of 'meaningful' is that of the general public and not that of an authority. This means that the collection of data with no (prior) interest to a public authority may fall within the right-of-access scope.

A second requisite for a document to be deemed official is that it is held by a public authority. In a paper-based document management system, a document's physical location is decisive. In an electronic system for data exchange, the demand for physical availability has been replaced by a digital requirement expressed in the following way:

> [a] recording under paragraph one is deemed to be held by a public authority, if it is available to the authority using technical aids, which the authority itself employs, for communication in such form that it may be read, listened to, or otherwise comprehended. A compilation of information taken from material recorded for automatic data processing is however regarded as being held by the authority only if the authority can make it available using routine means.

Attention should be paid to the fact that only technical aids used by the authority itself are to be considered when assessing a recording's availability. This implies that the technical infrastructure of a public authority is decisive for the access right in practice. For instance, the more advanced information-retrieval features, data-processing capacities, etc., a public authority acquires, the broader the access rights offered to the general public will be.

Not least with regard to the need to balance openness with privacy protection, a public authority ought to analyse and integrate legal aspects already at the stage of system design and programming. In fact, this is formally required according to Chapter 15, Section 9 of the Secrecy Act, which states that a public agency should organise its use of automatic data processing in compliance with the right of access to public documents as laid down in the Freedom of the Press Act.

In addition to a document or recording being kept by or available to a public authority, it must be either received or drawn up by such an authority in order to obtain the status of official. In a digital environment, technical availability also applies to the requirement of a recording being received (Ch. 2, Art. 6 FPA). However, there are no particular ICT adjustments to the 'drawn-up' condition. Instead, the major rule is that

> [a] document is deemed to have been drawn up by a public authority when it has been dispatched. A document which has not been dispatched is deemed to have been drawn up when the matter to which it relates has been finally settled by the authority, or, if the document does not relate to a specific matter, when it has been finally checked and approved by the authority, or has otherwise received final form.

Furthermore, Article 3, paragraph 2 FPA distinguishes between two types of recordings, namely so-called ready-made ones and compilations. The wording is not that precise, and application of this provision requires preparatory works and case-law to be taken into consideration. Examples

of what typically is understood by a ready-made recording are a specific e-mail message, a memorandum in electronic format, and an electronically documented (administrative) decision. A compilation, on the other hand, is, for instance, created as a result of record linkages between different data bases. The important thing in this context is that a public authority is only obliged to process a compilation for the general public if this can be accomplished by routine measures. Obviously, 'routine measures' is a vague expression that currently should be interpreted with reference to what may be conceived of as a relatively limited effort by the public authority in question. In practice, this means a couple of working hours, possibly even including programming efforts.

Worth mentioning in this context is also how the Freedom of the Press Act in a certain sense restricts the scope of the right of access. Article 3, paragraph 3 relates to privacy protection in the following way:

> [a] compilation of information taken from material recorded for automatic data processing is not however regarded as being held by the authority if the compilation contains personal data and the authority is not authorised in law, or under a statutory instrument, to make the compilation available. Personal data is understood to mean any information which can be referred back directly or indirectly to a private person.

In spite of the wording, the provisions of the Personal Data Act are not as such referred to.

Having briefly presented the legal foundations of the right of access to official documents, a few comments ought to be made on how the principle of openness may be taken advantage of in practice. It is important to note that, as a general rule, the right of access may be used anonymously without stating the purpose of a particular request. Only if a public official needs to know the identity of a person and the aim of a request in order to fulfil a compulsory secrecy assessment, does the anonymity not prevail.

In spite of the already implemented and relatively wide-ranging ICT adjustments to the principle of openness, some steps have not (yet) been taken. Chapter 2, Article 13, paragraph 2 FPA states that a 'public authority is however under no obligation to release material recorded for automatic processing in any other form than a printout except for insofar follows from an act of law.' Evidently, the right of access does not comprise digital releases, but the wording opens up for the Riksdag to issue an ordinary law expanding the forms for the principle of openness.

6.6.2. Management of official documents

Of major concern, not least from an administrative point of view, is how to comply with rules concerning long-term storage on the one hand, and sorting out official documents on the other. Although the Freedom of the Press Act does not in detail regulate this, an explicit reference is made to what is laid down in law (Ch. 2, Art. 18 FPA). The major principle is that official documents are to be preserved and that disposal must be authorised either by a specific legal decision or with reference to an applicable legal rule. The kinds of measures that constitute a disposal from a formal point of view vary considerably between a traditional, paper-based environment and an electronic one.

Naturally, shredding papers is a fundamental way of disposal. In digital settings, disposal occurs from a legal point of view also as the result of functional alterations, such as new means of data processing and information-retrieval methods as well as replacement of data-storage media, e.g., from a hard disk to a USB memory device. That many more activities constitute a disposal from a formal point of view in a digital environment does not imply that these kinds of activities are prohibited. On the contrary, ICT as a tool for document management comprises all kinds of inherent disposal measures. Still, the applicable legal framework needs to be considered carefully.

There is, for instance, no doubt that disposal activities may take place both unintentionally and intentionally. Attention should here be paid to the fact that, even if an intentional act of disposal has been carried out, it cannot be taken for granted that the data in question cannot be (re)compiled by routine measures and thus, after a request from the general public, could re-appear as an official document (cf., Ch. 2, Art. 3, para. 2 FPA). After all, the technical possibilities of recreating deleted documents are considerable today. Furthermore, this implies that the nature of many of the aforementioned disposal activities must be conceived of as merely making a copy,

as long as there are means for recreation. This reasoning shows that there is a need for proactive legal analyses,[38] not least because once installed technical platforms can, in a truly long-term perspective, in future turn out to create publicity requirements for documents now considered disposed of.

Yet another issue, which has been briefly touched upon above, concerns the storage of electronically signed documents. Such storage gives rise to questions related to the growing use of information standards such as XML (eXtensible Markup Language) and associated storage objects: signed data, contextual data, and signature data. In Sweden, there are indications that a new document type aimed at electronically signed data is emerging which may be referred to as a 'fixed data collection'.

6.6.3. Acts of law and other provisions

Information and communications technologies have been gradually introduced into the area of public administration with the purpose of decision support and even decision-making, which may be referred to as legal automation as an expression of e-government.

The handling of mass cases in areas such as social insurance and taxation is often put forward as an example of work in which the use of ICT is necessary to achieve a uniform and just application of administrative law. At the same time, the development of information systems for the purposes of public decision-making implies to a varying extent that vague criteria characterising natural legal language must be transformed into more precise (strict) criteria to form the basis of computer programs that will generate legal decisions wholly or partly automatically. More precisely, it concerns transformation of legal rules and associated legal information into program code that can be executed by computers.

Theoretical and empirical studies show that the transformation of legal rules into program code is not a trivial task from a legal point of view.[39] For example, in the field of social insurance, misinterpretations of statutes have occurred in the corresponding computer programs. Another problem is that of faulty programming methods,[40] leading to ambiguous results even if the outcome of the automatic data processing is not entirely wrong. An important point to make in this context is that the initial rule transformation will determine the outcome of almost all future cases, since in practice, the implemented interpretation of the legal rule(s) is made once and for all. Consequently, the value of the right to appeal an individual administrative decision may be questioned when the real decision-making lies in the design of the information system.

The transformation from traditional legislative information to instructions in program code may – depending on the character of the process – be categorised in terms of (a) an administrative action of no particular interest, (b) a single interpretation and application of legal rules (i.e., individual decision-making),[41] (c) the issuing of new rules (i.e., general administrative decision-making), or (d) a special kind of administrative decision. Sometimes, legal rules are so to speak programmed without any alterations during the system-development procedure. On the other hand, rules expressed in program code may turn out to be quite different as compared with corresponding legislation. It can therefore be argued that the transformation should rather be looked upon as the issuing of new rules. In such a situation, a number of questions arise, e.g., to what extent the computer program complies with the fundamental laws of Sweden.

---

[38] See, e.g., Magnusson Sjöberg, Cecilia, 'Presentation of the Nordic School of Proactive Law', *Scandinavian Studies in Law*, Volume 49, *A Proactive Approach*, pp. 13-19 (Stockholm 2006).

[39] See further Magnusson Sjöberg, *Rättsautomation: Särskilt om statsförvaltningens datorisering* [Legal Automation. In particular concerning the computerization of public-sector administration] (Stockholm: 1992) and Schartum, Dag Wiese, *Rettssikkerhet og systemutvikling i offentlig forvaltning* [The Rule of Law and System Devolopment in Publc Administration] (Oslo 1993). See also Helling, Erik, 'Logical Formulation of Legal Norms', in: *Festskrift till Peter Seipel* (Stockholm 2006) pp. 227-248.

[40] The Swedish Parliamentary Ombudsman has for instance paid attention to consequences of inaccurate correction routines within large-scale computer systems for money transfers in the area of taxation. See *JO om felaktiga skattekrav – synpunkter på några viktiga ADB-rutiner i skatteuppbörd och indrivningsverksamhet*, 1982: S 3.

[41] Mention should be made here to a case in which the Supreme Administrative Court (RÅ 2004 ref. 8) reached the conclusion that information published on a homepage by a public authority may be conceived of as an administrative decision that can be complained about. See further Ragnemalm, Hans, *Förvaltning i förvandling* [Public Administration in Change], *Förvaltningsrättslig tidskrift*, No. 4, 2005, pp. 445-457.

If, for example, a piece of program code differs so much in comparison with the corresponding conventional legal rule(s) that the computer program qualifies (because of its similarities to a conventional legal rule in the sense of being general and binding) as an act of legislation, it must be considered whether it fits into the following formal structure of law-making.

The power to enact laws in Sweden is regulated in the Instrument of Government (IG), Chapters 1 and 8. The legislative body is the Riksdag, sometimes the Government, and under certain circumstances after delegation of power, a public authority. Provisions concerning the relations between private subjects and the community with regard to obligations incumbent upon private subjects or that otherwise interfere with the personal or economic affairs of private subjects shall, according to Chapter 8, Article 3 IG, be laid down by law. This topic refers to the so-called 'obligatory law field'. Consequently, it may be argued that to carry out programming that includes the formulation of instructions falling into the category of Chapter 8, Article 3 IG cannot by considered a constitutional action on the part of public authorities.

Notwithstanding Chapter 8, Article 3 IG, as with the authorisation of the law, the Government may in some cases issue regulations by way of decrees (Ch. 8, Art. 7 IG). In such a context, the Riksdag may also authorise the Government to confer upon an administrative authority or a municipality the power of issuing regulations in the matter (Ch. 8, Art. 11 IG). This means that, should a public authority decide another, perhaps burdensome, condition during the system development, it would need an authorisation form the Government or the Riksdag.

Another part of this norm hierarchy concerns 'regulations regarding the enforcement of laws' (Ch. 8, Art. 13, para. 1.1 IG). This is a power that belongs to the Government and is directly founded on the Instrument of Government. Further, if the topic of legislation lies in the field formally expressed as 'regulations that are not under the fundamental laws to be issued by the Riksdag' (Ch. 8, Art. 13, para. 1.2 IG), the Government may, according to Chapter 8, Article 13, paragraph 3 delegate to a subordinate authority the power to issue regulations. This implies that a computer program establishing regulations regarding the enforcement of laws corresponds to the category of constitutionally regulated law-making. The same applies if the topic to be programmed falls within the field of regulations that do not have to be issued by the Riksdag.

All this implies that it is essential to analyse the transformation process – from law expressed in natural language into program code – in order to establish conformity with the constitutional framework on the right to issue acts and other provisions. A key issue is to find whether a new legal rule is at hand or whether it is an expression of an already existing (legal) rule. In the situation when new legal rules are expressed in computer programs, it must be possible to deduce authority from applicable constitutional documents and also to make the ICT-related rule formulation conform to the principles on how provisions are to be enacted.

6.6.4. Distribution of competence

In spite of the fact that local agencies are formally in charge of handling matters in the public sector, the outcome of an administrative matter is in reality to a large extent determined in central information systems, where taxes are calculated, registers linked together, etc. Local responsibility is thereby reduced to the input of data as the basis of central processing. This raises the question of the extent to which this impact of centralised ICT solutions complies with Chapter 11, Article 7 of the Instrument of Government (GI):

> [n]o public authority, including the Riksdag and the decision-making bodies of local authorities, may determine how an administrative authority shall decide in a particular case relating to the exercise of public authority vis-à-vis a private subject or a local authority, or relating to the application of law.

The conclusion that can be drawn from the remarks above on (a) rule transformation and (b) distribution of competence is that the introduction of ICT challenges the constitutional distinction between rule formulation, on the one hand, and rule application, on the other. In this context it is therefore relevant not merely to speak of technical convergence but also of legal convergence.

6.7. Conclusion

There is no doubt that the introduction and use of new technologies have challenged constitutional rights in Sweden. The impact of information and communication technologies on the fundamental laws gives rise to both substantive-law issues and methodological questions.

The legal framework of the Swedish principle of openness regulated in the Freedom of the Press Act illustrates this well. For example, there are in the context of rule application obvious uncertainties as to how to differentiate between a ready-made electronic recording, on the one hand, and a recording of compiled data, on the other.

The other type of technology-related challenge concerns how to best design applications complying with the legal demand of so-called 'good openness structure'. In this context, it is important to note that although a distinction may in principle be made between substantive law and legal methodology, these two aspects in practice depend on each other.

A key issue, not only with regard to preserving the principle of openness, proves to be secure management of electronic documents in a long-term perspective. Of particular relevance here is to find legally well-founded digital measures for storage as well as disposal of documents.

To conclude, theoretical studies and practical experiences of computerisation in Sweden show that a critical factor in enabling the rule of law to prevail is to (a) show early awareness of the legal implications of ICT, and (b) integrate legal aspects at early stages of system design and management. This is similar to saying that law needs to play a proactive role in the modern information society.

In terms of regulatory strategies, Swedish law-making bodies have over the years chosen technologically neutral amendments, if there have been any amendments at all of the constitutional rights. Despite the fact that the arguments in favour of technological neutrality are strong, it might be questioned whether the vagueness that follows from such regulation really satisfies the need for clarifications of what the constitutional rights stand for when faced with new technologies.

In conclusion, new technologies challenge not merely the constitutional rights per se but also the associated processes of their emergence and preservation. Therefore, it is important to apply a holistic approach in which legal, technical, and organisational infrastructures are shaped together.

References

Datainspektionen, *Personuppgifter i arbetslivet*, Datainspektionen informerar No. 7, 2001.

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

Helling, Erik, *Logical Formulation of Legal Norms*, in: Cecilia Magnusson Sjöberg and Peter Wahlgren eds., *Festskrift till Peter Seipel*, Stockholm: Norstedts Juridik, 2006, pp. 227-248.

Justitieombudsmannen, *JO om felaktiga skattekrav – synpunkter på några viktiga ADB-rutiner i skatteuppbörd och indrivningsverksamhet*, Justitieombudsmannen 1982: S 3.

Magnusson Sjöberg, Cecilia, *Critical Factors in Legal Document Management: A study of standardised markup languages*. The Corpus Legis Project. Stockholm: Jure, 1998.

Magnusson Sjöberg, Cecilia, 'Juridiska utmaningar på elmarknaden: IT-styrd tillsyn', *Juridisk Tidskrift* (JT) No. 2. 2004-05, pp. 334-351.

Magnusson Sjöberg, Cecilia, 'Presentation of the Nordic School of Proactive Law', *Scandinavian Studies in Law*, Volume 49, *A Proactive Approach*, pp. 13-19. Stockholm: Institute for Scandinavian Law, 2006.

Magnusson Sjöberg, Cecilia, *Rättsautomation: Särskilt om statsförvaltningens datorisering*. Stockholm: Norsteds juridik, 1992.

Magnusson Sjöberg, Cecilia and Anna Nordén, 'Managing Electronic Signatures: Current challenges', *Scandinavian Studies in Law* Volume 47, *IT Law*, pp. 79-95. Stockholm: Institute for Scandinavian Law, 2004.

Öman, Sören, and Lindblom, Hans-Olof, *Personuppgiftslagen: En kommentar* (Second ed.). Stockholm: Norstedts Juridik AB.
Petersson, Olof and Söderlind, Donald, *Förvaltningspolitik*. Second ed. Stockholm: Publica, 1993.
Ragnemalm, Hans, 'Förvaltning i förvandling', *Förvaltningsrättslig tidskrift* (FT) No. 4, 2005, pp. 445-457.
Riksarkivet, *Elektroniskt underskrivna handlingar*, Rapport 2006:1.
Schartum, Dag Wiese, *Rettssikkerhet og systemutvikling i offentlig forvaltning*. Oslo: Universitetsforlaget, 1993.
SOU 2001:28, *Yttrandefrihetsgrundlagen och nya medier. Yttrandefrihetsgrundlagen och Internet. Utvidgat grundlagsskydd och andra frågor om tryck- och yttrandefrihet. Betänkande från Mediegrundlagsutredningen*.
SOU 2002:18, *Personlig integritet i arbetslivet Betänkande från Integritetsutredningen*.
SOU 2004:6, *Översyn av personuppgiftslagen. Betänkande av personuppgiftslagsutredningen*.
SOU 2006:11, *Spel i en föränderlig värld, Betänkande av Lotteriutredningen*.
SOU 2006:96, *Ett nytt grundlagsskydd för tryck- och yttrandefriheten? Betänkande av Tryck- och yttrandefrihetsberedningen*.
Wennergren, Bertil, 'IT-styrd tillsyn i disharmoni med förvaltningsrättens regler', *Juridisk Tidskrift* (JT) No. 3, 2004-2005, pp. 783-786.
Westregård, Annamaria, *Integritetsfrågor i arbetslivet*, Lund: Juristförlaget, 2002.
Sanna Wolk ed., *Biobanksrätt*, Lund: Studentlitteratur, 2003.

Chapter 7. Constitutional Rights and New Technologies in the United States

Susan W. Brenner[1]

7.1. Introduction

This chapter deals with how the U.S. Constitution – as written and as applied by the U.S. Supreme Court – deals with digital rights, particularly constitutional rights involving privacy and free speech. As the chapter demonstrates, the protection currently given digital rights in these (and related) areas is exclusively the result of the Supreme Court's interpreting constitutional provisions that date back over two hundred years.

As the next section explains, the U.S. Constitution itself really does not establish rights that are enforceable against the government. The text of the U.S. Constitution, as such, is for the most part concerned with constructing a government; it defines the three constitutive branches of the federal government (executive, judicial and legislative), articulates the powers assigned to and limitations imposed upon each, and deals with related structural issues. The text of the Constitution does touch on individual rights in three respects: Article I § 10 prohibits states from impairing the obligation of contracts; Article I §§ 9 and 10 bar the adoption of ex post facto criminal laws by the federal and state governments; and the same sections of Article I prohibit the state and federal governments from enacting bills of attainder, a common law device that imposed legislative punishment upon particular individuals and thereby denied them recourse to the judicial system.[2]

This chapter focuses only on *federal* Constitutional guarantees. The U.S, system of government is a federal system, with power allocated between a central, federal government and the states. The system of government has been a federal system since 1781, which is when the requisite number of states ratified the Articles of Confederation, the original constitutive document.[3] Because the system created by the Articles of Confederation proved to be too decentralized, a Constitutional Convention was convened in 1787 to develop an improved, rather more centralized system of government.[4] It drafted the current Constitution, which went into effect in 1788, after being ratified by the requisite number of states.[5]

7.2. History and scope of digital constitutional rights

7.2.1. History

As noted above, the U.S. Constitution, as such, does not privacy or other enforceable rights. It is concerned, instead, with establishing the basic organizational structure of the U.S. government.

The privacy guarantees that are explicitly or inferentially derivable from the U.S. Constitution appear not in the text of the Constitution but in amendments that have been adopted over the more than two hundred years since it was ratified and went into effect. The next section describes the amendment process.

The language and interpretation of the amendments that support digital and other rights is examined below, in the sections that deal with specific rights. This is necessary because, as noted above, neither the Constitution nor its amendments create a general set of human rights. Instead, specific amendments establish particular guarantees, guarantees that have been interpreted by the U.S. Supreme Court in more or less expansive ways.

---

[1] Prof. Susan W. Brenner is NCR Distinguished Professor of law & Technology at University of Dayton School of Law, Dayton, Ohio, United States.
[2] R.D. Rotunda & J.E. Nowak, *Treatise on Constitutional Law* (3d ed.) (West Publishing, St. Paul, MN 2006) § 10.10.
[3] Rotunda & Nowak, op. cit. n. 2 at § 1.1.
[4] Rotunda & Nowak, op. cit. n. 2 at § 1.1.
[5] Rotunda & Nowak, op. cit. n. 2 at § 1.1.

Generally, the U.S. Supreme Court's approach to interpreting rights created by the various amendments became much more expansive in the twentieth century. This is attributable to the mid-twentieth century Justices' increasing willingness to engage in judicial activism, a tendency some applaud but others criticize. [6] This inclination has been especially evident in decisions that address "fundamental rights," a concept some find problematic. As one treatise notes, the concept of fundamental rights remains vague (...). All that can be said with certainty is that the Justices have selected a group of individual rights which do not have a specific textual basis in the Constitution or its amendments and deemed them to be 'fundamental.'"[7]

The most notable instances of the mid-twentieth century Supreme Court's willingness to identify "fundamental rights" implicating privacy interests are its decisions in *Roe v. Wade,* 410 U.S. 179 (1973) and in *Griswold v. Connecticut,* 381 U.S. 479 (1965). In *Roe,* the Court upheld a woman's right to an abortion, at least under certain circumstances; in *Griswold,* it struck down a Connecticut statute that prohibited the use of contraceptives by married persons. The twentieth-century Court used the concept of "fundamental rights" to recognize other rights, including the rights to marry and have children.[8] Most recently, it applied this principle to hold unconstitutional a Texas statute that criminalized consensual sodomy between two persons of the same sex.[9]

In these and the other instances in which the U.S. Supreme Court has applied the notion of "fundamental rights" derivable from but not explicitly articulated in the Constitution, the prevailing Justices relied primarily on the Ninth Amendment to the Constitution, and secondarily on the notion of substantive due process.[10] The Ninth Amendment, which was one of ten amendments added in 1791, states that the "enumeration in the Constitution, of certain rights, shall not be construed to deny (...) others retained by the people."[11] The mid-twentieth century Supreme Court cited this residual pool of rights as one basis for recognizing certain "fundamental rights."[12]

The other basis was the theory of substantive due process, under which the protections of the Fourteenth Amendment's due process clause guarantee not only procedural fairness but also "heightened protection against government interference with certain fundamental rights".[13] Early twentieth century Supreme Court Justices developed the concept of economic substantive due process and used it to strike down "progressive" social and economic legislation until later Justices abandoned the doctrine in the 1930s.[14] The mid-twentieth century Court used a variation – which is sometimes described as non-economic substantive due process – to recognize the "fundamental rights" noted above.[15]

By the end of the century, substantive due process had somewhat fallen into disrepute; in one opinion, for example, Justices Scalia and Thomas describe it as an "oxymoron" and criticize the notion that the Court can justifiably "pick and choose" among rights to decide which should be accorded substantive due process protection.[16] They, and others, argue that the repertoire of rights available to Americans should be limited to those specifically enumerated in the Constitution and its amendments.

Justices Scalia and Thomas were not the only critics of the "fundamental rights" jurisprudence. When they issues, the "fundamental rights" decisions came under criticism from scholars and others who believed the U.S. Supreme Court had impermissibly exceeded its constitutional authority by engaging in an expansive, textually-unfounded interpretation of the Constitution and

---

[6] Rotunda & Nowak, op. cit. n. 2 at § 23.5.
[7] Rotunda & Nowak, op. cit. n. 2 at § 15.7; R.M. Cover, 'The Origins of Judicial Activism in the Protection of Minorities, 91 *Yale Law Journal* (1982), 1287, 1288-1289.
[8] *Loving v. Virginia,* 388 U.S. 1 (1967) (right to marry); *Skinner v. Oklahoma,* 316 U.S. 535 (1942) (right to have children); *Meyer v. Nebraska,* 262 U.S. 390 (1923) (right to supervise education of children); *Rochin v. California,* 342 U.S. 165 (1952) (right to bodily integrity).
[9] *Lawrence v. Texas,* 539 U.S. 558 (2003).
[10] Rotunda & Nowak, op. cit. n. 2 at § 1.
[11] U.S. Constitution, amendment ix.
[12] Rotunda & Nowak, op. cit. n. 2 at § 1.
[13] *Washington v. Glucksberg,* 521 U.S. 702 (1997).
[14] S.G. Calabresi, 'The Tradition of the Written Constitution,' 57 *Alabama Law Review* (2006) 635, 640-642.
[15] G.P. Magarian, 'Substantive Due Process as a Source of Constitutional Protection for Nonpolitical Speech,' 90 *Minnesota Law Review* (2005) 247, 285.
[16] *United States v. Carlton,* 512 U.S. 26 (1994).

its amendments.[17] Indeed, some went so far as to describe the *Roe-Griswold* style of decision-making as "judicial imperialism."[18]

The rights-expanding, *Roe-Griswold* style of interpretation declined at the end of the twentieth century as more conservative Justices were appointed to the Court.[19] Some contend – quite credibly – that the late twentieth-century and early twenty-first century Supreme Court has been characterized by the opposite tendency, i.e., by an era of conservative judicial activism.[20] One result of this is that the recognition of new "fundamental rights" has been curtailed and there is an increasing emphasis on the rights explicitly articulated in the amendments to the Constitution. Those rights are examined below.

7.2.1. Scope

Except for the doctrine of substantive due process, which is derived in large part from the Fourteenth Amendment to the U.S. Constitution,[21] the constitutional protections discussed in this chapter all derive from the first ten amendments to the Constitution: the Bill of Rights. [22] The Bill of Rights Amendments apply only when there is state action. As the authors of a treatise on American constitutional law note: 'the Bill of Rights (...) has been viewed only to limit the freedom of the government when dealing with individuals'.[23] The same construction is given to the Fourteenth Amendment.[24] 'Only the Thirteenth Amendment, which abolishes the (...) slavery, is also directed to controlling the actions of private individuals.'[25]

This interpretation of these amendments has given rise to the 'state action doctrine.' The '"state action" issue arises only when the person or entity alleged to have violated the Constitution is not acting on behalf of the government. In such a case the person alleged to have violated the constitutional provision will argue that he is incapable of violating the Constitution because he is not part of the government, giving rise to the state action issue.' [26] The reference to 'state action' does not, of course, limit the application of these amendments to conducts undertaken by or on behalf of one of the U.S. states; instead, it encompasses action undertaken by or on behalf of one or more U.S. states and/or the federal government. [27]

In *Edmonson v. Leesville Concrete Co.., Inc.,* 500 U.S. 614 (1991), the U.S. Supreme Court explained that courts should consider two issues when deciding if a private person or entity acted on behalf of a government so as to trigger the state action principle: ' whether the claimed constitutional deprivation resulted from the exercise of a right or privilege having its source in state authority, and (...) whether the private party charged with the deprivation could be described in all fairness as a state actor'.[28] One factor the Court has found significant in resolving the first issue is whether the private party's conduct was authorized by state or federal legislation.[29] If it was, then state action will probably exist. The *Edmonson* Court also explained that 'in determining whether a particular action or course of conduct is governmental in character, it is relevant to examine the following: the extent to which the actor relies on governmental assistance and benefits, (...) whether the actor is performing a traditional governmental function, (...) and whether the injury caused is aggravated in a unique way by the incidents of governmental authority'. [30]

---

[17] D.A. Farber, 'The Originalism Debate," 49 *Ohio State Law Journal* (1989), 1085, 1086.
[18] S.G. Calabresi, 'The Originalist and Normative Case Against Judicial Activism," 103 *Michigan Law Review* (2005), 1081, 1083.
[19] D.C. Williams, 'Civic Constitutionalism, The Second Amendment, and the Right of Revolution,' 79 *Indiana Law Journal* (2004), 379, 383.
[20] R.W. Garnett, 'Personal Reflections on the Chief,' 10 *Texas Review of Law & Politics* (2006), 283, 287-288.
[21] '[S]ubstantive due process analysis applies interchangeably to both the states, via the Fourteenth Amendment's Due Process Clause, and to the federal government, via the Fifth Amendment's Due Process Clause.' V.C. Abreu, 'The Malleable Use of History in Substantive Due Process Jurisprudence,' 44 *Boston College Law Review* (2002) pp. 177, 181-182.
[22] Rotunda & Nowak, op. cit. n. 2 at § 14.3.
[23] Rotunda & Nowak, op. cit. n. 2 at § 16.1.
[24] Rotunda & Nowak, op. cit. n. 2 at § 16.1.
[25] Rotunda & Nowak, op. cit. n. 2 at § 16.1.
[26] Rotunda & Nowak, op. cit. n. 2 at § 16.1.
[27] Rotunda & Nowak, op. cit. n. 2 at § 16.1.
[28] *Edmonson v. Leesville Concrete Co.., Inc.,* 500 U.S. 614, 620 (1991).
[29] *Edmonson v. Leesville Concrete Co.., Inc.,* 500 U.S. 614, 621 (1991).
[30] *Edmonson v. Leesville Concrete Co.., Inc.,* 500 U.S. 614, 621-622 (1991).

7.3. Changes in the constitutional system

The U.S. constitutional system has not changed since the current Constitution went into effect in 1788. The Constitution has, however, been amended on a number of occasions since then.

To this point, the U.S. Constitution has not been amended to address privacy or other issues raised by evolving technologies. And it is very unlikely this will occur; American law has been loath to tinker with the foundational document, particularly in ways that could impact upon fundamental principles governing the allocation of rights and obligations between citizens and their government.

The drafters of the U.S. Constitution intentionally made it very difficult to amend the Constitution. Article V of the U.S. Constitution establishes two methods of constitutional amendment:[31] Two-thirds of both Houses of Congress (the Senate and the House of Representatives) can propose an amendment; or the legislatures of two-thirds of the U.S. states can call upon Congress to convene a Constitutional Convention for the purpose of considering an amendment.[32] Once an amendment has been proposed, it does not become part of the Constitution unless and until it has been ratified by at least three-quarters of the U.S. states.[33] Amendments have so far been proposed only by Congress; the second method has never been used. [34] The next section reviews the relatively few amendments that have been added to date, with particular emphasis upon those that are relevant to this discussion.

Because Americans are reluctant to amend the Constitution and because the process itself discourages amendments, American constitutional law relies upon the process of extrapolation: the Supreme Court's construing centuries-old constitutional provisions, when and as appropriate, in ways that exclude or bring the effects of new technologies within the guarantees the Constitution establishes.

7.4. Privacy-related rights

While the U.S. Constitution nowhere expressly establishes a general right to privacy,[35] certain of the amendments to the Constitution explicitly or inferentially confer specific privacy rights. Unlike the more problematic "fundamental rights" discussed above, these rights are derivable from specific language in one or more amendments. The guarantees that have been the most important in this regard are the First Amendment's protection of free speech and freedom of assembly, the Fourth Amendment's prohibition on unreasonable searches and the Fifth Amendment's privilege against self-incrimination.

As interpreted by the modern U.S. Supreme Court, these amendments protect privacy in different ways: The First Amendment protects the privacy of certain acts. More precisely, the Supreme Court has held that as a function of its protecting free speech and freedom of assembly, the First Amendment guarantees the rights to speak anonymously and to preserve the confidentiality of one's associations.[36]

The Fourth Amendment historically protected certain areas – those constitutionally deemed 'private' – from unauthorized governmental intrusions. The modern Supreme Court has extended this notion of privacy to encompass at least certain uses of technology, as is explained below.[37]

The Fifth Amendment's contribution is more limited. While the Supreme Court has said that the Fifth Amendment privilege against compelled self-incrimination protects 'personal privacy',[38] it has never applied the privilege when the government's acquisition of evidence 'did not involve

---

[31] U.S. Constitution, article v.
[32] Rotunda & Nowak, op. cit. n. 2 at § 10.10.
[33] U.S. Constitution, article v.
[34] Rotunda & Nowak, op. cit. n. 2 at § 15.7.
[35] K. Gormly, 'One Hundred Years of Privacy,' 1992 *Wisconsin Law Review* 1335, 1343 (as of 1890 'there existed no coherent notion of privacy at all in American law').
[36] *McIntyre* v. *Ohio Elections Commission*, 514 *U.S.* 334, 341-342 (1995); *NAACP* v. *State of Alabama ex rel. Patterson*, 357 *U.S.* 449, 462 (1958).
[37] *Katz* v. *United States*, 389 *U.S.* 347, 350 (1967).
[38] *Fisher* v. *United States*, 425 *U.S.* 391, 399 (1976).

compelled testimonial self-incrimination of some sort.'[39] The only role the Fifth Amendment currently plays in the U.S. skein of privacy, therefore, is to prevent the state from forcing citizens to divulge their guilty testimonial secrets.

The sections below examine how these amendments have been applied to protect privacy in the U.S.

7.4.1. Privacy and data protection

The sections immediately below explain how the Fourth Amendment – which is the most important guarantor of privacy for U.S. citizens – constrains official efforts at data-gathering. The first section traces the evolution and purpose of the amendment; the next several sections explain how it has been applied in several pertinent contexts.

Fourth Amendment: overview

The Fourth Amendment is predicated on a spatial conception of privacy.[40] It was originally intended to protect the sanctity of private property from intrusions by public officials; this concern with private property derives from English common law.[41]

Early English law punished those who invaded another's premises, and by the twelfth century housebreaking had become a serious crime in England.[42] By the sixteenth century English law had specific prohibitions criminalizing housebreaking, burglary and trespass.[43] These laws were only concerned with trespasses by private persons because official searches of private premises were almost unknown until the fifteenth century[44] In the latter half of the fifteenth century, the King began authorizing trade guilds to search private premises to enforce guild regulations.[45] About a century later, the Court of the Star Chamber, which was responsible for regulating printing, decreed that the wardens of the Stationers' Company could search 'any warehouse, shop, or any other place' where they believed the printing laws were being violated.[46] Other courts authorized searches directed at those suspected of libel, heresy and political dissent.[47] These court decrees resulted in the development of the general warrant, which was not based on any showing of individualized suspicion and which gave the bearers the discretion to search wherever they liked.[48] As arbitrary, general warrant-based searches became more common, English citizens began to object.[49]

In a series of decisions issued in the mid-eighteenth century, English courts held that homes were protected from arbitrary action by government officials.[50] Most of the decisions grew out of investigations into seditious libel: In a typical instance, officers who were ordered to find the author of a recently-published letter relied on a general warrant to search houses.[51] Those whose homes were searched sued the officers for trespass, and won.[52] The effect was to apply the same standard to public and private actors: Either could be held civilly liable as a trespasser for entering another's property 'without a lawful authority'.[53] The difference between the two was that a public actor could rely on a warrant, as well as on a property owner's consent, as authorization for an entry.[54]

---

[39] *Fisher* v. *United States*, 425 U.S. 391, 399 (1976).
[40] *Olmstead* v. *United States*, 277 U.S. 438, 463 (1928).
[41] *See, e.g.,* Boyd v. United States, 116 U.S. 616, 627 (1886).
[42] N. B. Lasson, *The History and Development of the Fourth Amendment to the United States Constitution* (Baltimore: Johns Hopkins Press, 1937) 79-105.
[43] Lasson, op. cit. n. 42 at 79-105.
[44] Lasson, op. cit. n. 42 at 36, 75.
[45] Lasson, op. cit. n. 42 at 24.
[46] Lasson, op. cit. n. 42 at 25.
[47] Lasson, op. cit. n. 42 at 25-27.
[48] Lasson, op. cit. n. 42 at 45.
[49] Lasson, op. cit. n. 42 at 30-45.
[50] *Money* v. *Leach*, 97 *Eng. Rep.* 1050 (K.B. 1765); *Entick* v. *Carrington,* 95 *Eng. Rep.* 807 (C.P. 1765); *Wilkes* v. *Wood,* 98 *Eng. Rep.* 489 (C.P. 1763); *Huckle* v. *Money*, 95 *Eng. Rep.* 768 (C.P. 1763).
[51] Lasson, op. cit. n. 42 at 43-45.
[52] Lasson, op. cit. n. 42 at 44-46.
[53] III W, Blackstone, *Commentaries on English Law* 209.
[54] A.R. Amar, 'The Bill of Rights As a Constitution,' 100 *Yale Law Journal* (1991) 1131, 1178-1179.

During this era, American colonists were waging their own war against writs of assistance, a version of the general warrant.[55] Their legal challenges to the writs failed, but the resentment the writs generated was a driving factor in the Revolution and, later, in the adoption of bills of rights by states and by the federal government.[56] The Fourth Amendment was therefore a product of the same concerns that resulted in the English law of trespass' being applied to public actors: 'to guard individuals against improper intrusion into their buildings where they had the exclusive right of possession.'[57] Like its English analogue, the Fourth Amendment was intended to preserve privacy by discouraging law enforcement trespasses.[58]

'Papers'

There were few Fourth Amendment cases in the nineteenth century. Perhaps the best known is *Boyd v. United States,* which involved the 'compulsory production of a man's private papers,' which the Supreme Court found to be the 'equivalent' of a search and seizure.[59] The Court struck down the practice in an opinion that cited the most famous English trespass case – *Entick* v. *Carrington* – and seemed to fuse the Fifth Amendment privilege against self-incrimination with the Fourth Amendment's prohibition on unreasonable searches.[60] The opinion quotes extensively from *Entick* for the proposition that an unauthorized official violation of the security and seclusion of one's 'papers' is a trespass.[61] Conceptually, however, *Boyd* is of little significance, because the twentieth-century Supreme Court has 'systematically rejected and cabined *Boyd's* holding.'[62]

Letters

The other notable nineteenth-century Supreme Court decision considered whether the Fourth Amendment applies to postal mail. *Ex parte Jackson*[63] was an appeal from a conviction for sending 'a circular concerning a lottery' through the U.S. Mail.[64] The *Jackson* Court held that Congress had the power to prohibit the mail's being used to deliver certain types of material as long as the prohibitions were enforced in accordance with the Fourth Amendment:

> [A] distinction is to be made between (...) what is intended to be kept free from inspection, such as letters, and sealed packages (...) and what is open to inspection, such as newspapers (...) and other printed matter (...). Letters and sealed packages (...) are as fully guarded from examination and inspection, except as to their outward form and weight, *as if they were retained by the parties forwarding them in their own domiciles*. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures *extends to their papers, thus closed against inspection, wherever they may be*. Whilst in the mail, they can only be opened and examined under like warrant, issued upon (...) oath or affirmation, particularly describing the thing to be seized, *as is required when papers are subjected to search in one's own household (...).* [A]ll regulations adopted as to mail matter (...) must be in subordination to the great principle embodied in the fourth amendment of the Constitution.[65]

The *Jackson* holding is still good law, and some suggest it should also apply to e-mail. That is, some contend that the Fourth Amendment protects the contents of e-mail but does not protect traffic data, which is analogous to addressing information found on the outside of letters and other

---

[55] Lasson, op. cit. n. 42 at 53.
[56] *Marshall* v. *Barlow's, Inc.,* 436 *U.S.* 307, 311 (1978).
[57] *Jones* v. *Gibson*, 1 *N.H.* 266, 1818 *WL* 488 *5 (N.H. 1818).
[58] *Humes* v. *Taber*, 1 *R.I.* 464, 1850 *WL* 1823 *6 (R.I. 1850); *Jones* v. *Gibson*, 1 *N.H.* 266, 1818 *WL* 488 *5 (N.H. 1818); *Patcher* v. *Sprague,* 2 *Johns* 462, 1807 *WL* 931 (N.Y. Sup. 1807).
[59] *Boyd* v. *United States*, 116 *U.S.* 616, 622 (1886).
[60] *Boyd* v. *United States*, 116 *U.S.* 616, 632-635 (1886).
[61] *Boyd* v. *United States*, 116 *U.S.* 616, 626-630 (1886).
[62] M.S. Pardo, 'Disentangling the Fourth Amendment and the Self-Incrimination Clause,' 90 *Iowa Law Review* (2005) 1857, 1858.
[63] *Ex parte Jackson,* 96 *U.S.* 727 (1877).
[64] *Ex parte Jackson,* 96 *U.S.* 727, 727 (1877).
[65] *Ex parte Jackson,* 96 *U.S.* 727, 728 (1877) (emphasis added).

postal mail.[66] Others say that to be protected under *Ex parte Jackson*, the contents of e-mail must be "sealed," i.e., must have been encrypted.[67] At this writing, these issues remain unresolved.

As the next section notes, e-mail can also be analyzed under *Katz,* the most recent case in which the Supreme Court applied the Fourth Amendment to telephonic wiretapping.

Wiretapping

In 1928, the Supreme Court decided *Olmstead v. United States,* 277 U.S. 438 (1928). The issue – which was one of first impression – was whether wiretapping violated the Fourth Amendment. Federal agents had installed taps on telephone lines leading from the homes of bootlegger Roy Olmstead and three of his associates; the government subsequently used information obtained by the wiretaps to convict all four of violating prohibition laws. Since the taps were connected to the phone lines as they ran toward the residences, there was no physical intrusion into the homes.

In an opinion by Chief Justice Taft, a majority of the Court held that the Fourth Amendment did not apply because there was no trespass: "The language of the amendment cannot be (...) expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house (...) any more than are the highways along which they are stretched."[68] Writing for the Court, Justice Taft distinguished telephone conversations from the letters at issue in *Ex parte Jackson*, basically on the grounds that letters are tangible property while conversations are not.

Justice Brandeis famously dissented, arguing that the Fourth Amendment must adapt to a changing world. He argued that the Fourth Amendment would lose all meaning if it were applied only to the physical trespasses it was originally intended to control:

> Subtler and more far-reaching means of invading privacy have become available to the government (...).The progress of science (...) is not likely to stop with wire tapping. Ways may (...) be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and (...) expose to a jury the most intimate occurrences of the home (...). Can it be that the Constitution affords no protection against such invasions of individual security?[69]

After *Olmstead*, wiretapping was constitutionally permissible; Congress considered banning it, but ultimately did nothing.[70]

In 1967, the Supreme Court reversed *Olmstead* and held that FBI agents violated the Fourth Amendment by installing an 'electronic listening and recording device' on the *outside* of a telephone booth to record calls being made by Charles Katz.[71] In so doing, the majority of the Court announced a new standard for applying the Fourth Amendment's privacy protections: '[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection (...). But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'[72]

In a concurring opinion, Justice Harlan articulated the standard that has been used to implement the *Katz* holding:

> [T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is (...) a place where he expects privacy (...). On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[73]

---

[66] S.E. Henderson, 'Nothing New Under the Sun? A Technologically-Rational Doctrine of Fourth Amendment Search,' 56 *Mercer Law Review* (2005) 507, 525-526.
[67] E.P. Lowe, 'Emailer Beware: The Fourth Amendment and Electronic Mail,' 2 *Oklahoma Journal of law & Technology* (2005) 28.
[68] *Olmstead v. United States,* 277 U.S. 438, 465 (1928).
[69] *Olmstead v. United States,* 277 U.S. 438, 473-74 (1928).
[70] *Nardone v. United States*, 302 U.S. 379, 382 (1937).
[71] *Katz v. United States*, 389 U.S. 347, 348 (1967).
[72] *Katz v. United States*, 389 U.S. 347, 351 (1967).
[73] *Katz v. United States*, 389 U.S. 347, 361 (1967).

Katz is still the standard the Supreme Court uses to determine when the conduct of law enforcement officers violates a reasonable expectation of privacy and therefore constitutes a 'search' under the Fourth Amendment. The *Katz* test applies to any invocation of Fourth Amendment privacy, regardless of whether the use of technology is involved. A later section examines a recent decision in which the Supreme Court applied *Katz* to law enforcement's use of thermal imaging technology to scan a home.

The focus here is primarily on the use of technology to obtain data (papers), either from a home or from some other constitutionally-protected area or activity. It is clear that under *Jackson* and *Katz* the *contents* of sealed postal mail are 'private' and therefore protected by the Fourth Amendment. It is, as noted above, not at all clear if the contents of unencrypted e-mail is private under the Fourth Amendment.

As it has evolved, the *Katz* standard has developed into an 'assumption of risk' analysis. This means that while someone who, say, chats on their cell phone while standing in an airport can claim they subjectively believed the contents of their conversation was private under the Fourth Amendment, they will lose because the Supreme Court will find that they made no effort to keep their conversation private. Or, as the *Katz* Court said, what one "knowingly" exposes to public view (or hearing) is not private, even though the exposure occurs in his or her own home.

Some therefore argue that when this principle is applied to the contents of e-mail or other electronic communication, the conclusion is that the contents are not private under the Fourth Amendment unless they were encrypted. [74] At this writing, the issue remains unresolved. No reported decision of a lower court addresses the issue, and it will no doubt be years before the U.S. Supreme Court addresses it.

There are at least two reasons why this issue has not yet been addressed by U.S. courts. One is practical: Americans tend not to encrypt their e-mails. The other reason is that in 1986 Congress adopted the Electronic Communications Privacy Act ['ECPA'] to provide statutory guarantees of privacy for electronic communications. [75] ECPA's provisions exceed the requirements imposed by *Katz* in certain respects.[76] The substance of these provisions is quite outside the scope of this discussion, but they are relevant to this extent: They have become the default standard governing the collection of the content and traffic data generated by electronic communications and, in so doing, have shifted the focus away from the Fourth Amendment. It is, however, more than likely that the focus will shift back to the Fourth Amendment as the ECPA provisions become outdated, due to continuing advances in technology.

Traffic data

Katz dealt only with the *contents* of a transmitted communication. In a subsequent decision, the Supreme Court dealt with the related issue of whether the addressing and transmittal information – the traffic data – generated by an electronic or telephonic communication is 'private' under the Fourth Amendment.

To understand the holding in that case, it is necessary to understand the Court's holding in an earlier case: *United States v. Miller,* 425 U.S. 435 (1976). Miller, indicted on tax charges, moved to suppress records concerning his bank account; federal agents had obtained the records by using a grand jury subpoena, rather than a warrant. (Only a search warrant can satisfy the Fourth Amendment; subpoenas are used when a search warrant is not constitutionally required.)

Miller invoked *Boyd*, claiming the agents had "improperly circumvented" his Fourth Amendment rights. The Supreme Court disagreed because it found the subpoenaed documents were not Miller's '"private papers." Unlike the claimant in *Boyd*, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks.'[77] This set the stage for the case that involved an early form of traffic data.

---

[74] E.P. Lowe, 'Emailer Beware: The Fourth Amendment and Electronic Mail,' 2 *Oklahoma Journal of law & Technology* (2005) 28.
[75] R. Simmons, 'From *Katz* to *Kyllo:* A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies,' 53 *Hastings Law Journal* (2002) 1303, 1340-1342.
[76] R. Winick, 'Searches and Seizures of Computers and Computer Data,' 8 *Harvard Journal of Law & Technology* (1994) 75, 78.
[77] *United States v. Miller,* 425 U.S. 435, 440 (1976).

Three years later, the Court decided *Smith v. Maryland,* 442 U.S. 735 (1979). The issue was 'whether the installation and use of a pen register' – which captures the numbers dialed on a telephone – is a 'search' under the Fourth Amendment. Police suspected Smith was the person who had robbed a woman and was making threatening and obscene phone calls to her. At the police's request, the telephone company 'installed a pen register at its central offices to record the numbers dialed from the telephone at [his] home (...). The police did not get a warrant or court order before having the pen register installed.'[78] The pen register showed that Smith was calling her home; the police used this evidence to obtain a warrant to search Smith's home, where they found further evidence incriminating him in the illegal calls.

Indicted, Smith moved to suppress 'all fruits derived from the pen register' on the grounds that its installation and use was a warrantless search in violation of the Fourth Amendment. [79] He lost below and appealed to the Supreme Court.

The *Smith* Court began its opinion by noting that the standard used to implement *Katz* is the two-pronged test Justice Harlan enunciated in his concurring opinion: (i) whether the individual has exhibited a subjective expectation of privacy in the thing, place or endeavor; and (ii) whether society is prepared to regard the individual's subjective expectation of privacy as reasonable. The Court found Smith met neither criterion:

> Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner (...) cannot claim that his 'property' was invaded or that police intruded into a 'constitutionally protected area.' Petitioner's claim (...) is that, notwithstanding the absence of a trespass, the State (...) infringed a 'legitimate expectation of privacy' (...). [A] pen register differs (...) from the listening device employed in *Katz,* for pen registers do not acquire the *contents* of communications (...). [80]

The Supreme Court then held that Smith did not have a cognizable Fourth Amendment expectation of privacy in the numbers he dialled from his telephone.

On that issue, the Court was not inclined to believe that Smith – or, indeed, anyone – actually expects the numbers they dial to be private. The Supreme Court explained that all those who use telephone services 'know' the telephone company keeps track of the numbers they dial for billing purposes, and therefore do not (or cannot) expect that the numbers are 'private' within the compass of the Fourth Amendment. The Supreme Court also held that even if Smith could show that he had such a subjective expectation, it is not one society would regard as reasonable: 'This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'[81] The Court cited *Miller* for the last statement.

Both the *Smith* and *Miller* decisions apply the *Katz* assumption of risk standard that was described in the previous section. The effect of these decisions is to take all third-party records – including the records kept by telephone companies, Internet Service providers, cell-phone service providers and other providers of electronic communications – outside the Fourth Amendment. Americans currently have no Fourth Amendment expectation of privacy in any data they knowingly 'share' with a third-party. This means law enforcement officers can obtain this information by request – and without a search warrant – if the third-party record holder is willing to surrender it to the officers.

The Electronic Communications Privacy Act of 1986, which was discussed in the previous section, does create certain procedural requirements law enforcement must satisfy to obtain certain types of third-party records from those who provide electronic communication services. The Act goes beyond the requirements of the Fourth Amendment, as interpreted by the *Smith* and *Miller* Courts, by imposing some not-very-onerous procedural obligations upon police officers who wish to obtain a customer's name, address, service and payment information. And it does something similar with regard to traffic data. In neither instance, however, are officers required to obtain a search warrant in compliance with the Fourth Amendment.

---

[78] *Smith v. Maryland,* 442 U.S. 735, 736 (1979).
[79] *Smith v. Maryland,* 442 U.S. 735, 736 (1979).
[80] *Smith v. Maryland,* 442 U.S. 735, 741 (1979).
[81] *Smith v. Maryland,* 442 U.S. 735, 743-744 (1979).

Tracking devices

In *United States v. Knotts,* 460 U.S. 276 (1983), the Supreme Court applied *Katz* to hold that police officers' warrantless monitoring of an electronic tracking device ("beeper") inside a container of chemicals did not violate the Fourth Amendment when it revealed no information that could not have been obtained through visual surveillance.'[82] Officers had used the beeper to help them follow the vehicle carrying the container along a series of public roads. The Supreme Court held there was no violation of the Fourth Amendment because the information provided by the beeper was nothing more than what the officers could have learned by following the vehicle carrying the container as it traveled to a private cabin:

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements (...). When Petschen travelled (...) he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction (...).
>
> (...) Knotts, as the owner of the cabin (...) to which Petschen drove, undoubtedly had the traditional expectation of privacy (...) insofar as the cabin was concerned (...). But no such expectation of privacy extended to the visual observation of Petschen's automobile arriving on his premises after leaving a public highway.[83]

The Supreme Court reached the opposite conclusion in *United States v. Karo*.468 U.S. 705 (1984). As in *Knotts,* federal agents installed a beeper in a container of chemicals and used it to follow the vehicle carrying the container to a residence. On two occasions, they used the signal from the beeper to determine that it (i) was still in Karo's house and (ii) had been moved to another residence.

The Court applied *Katz* to hold that these latter uses of the beeper violated the Fourth Amendment because they infringed upon the privacy of the home. The Court first noted that individuals have a cognizable Fourth Amendment expectation of privacy inside their homes; this expectation derives from *Katz* and from the common law antecedents of the Fourth Amendment discussed earlier. The Court explained that the agents had used to beeper to obtain information from inside a home that they could not have otherwise have obtained except by entering the residence; since they would need a search warrant to enter the residence without violating the Fourth Amendment, it followed that they needed a search warrant to monitor the beeper to obtain this information.

The *Knotts-Karo* holdings are being applied to the use of more sophisticated technologies, including Global Positioning System tracking devices. Most U.S. courts routinely find that the use of *any* type of tracking device does not violate the Fourth Amendment under the Supreme Court's holding in *Knotts,* but a few lower courts have noted the differences between the beeper involved in that case and today's more sophisticated technologies. No court has so far held that the use of GPS or other modern tracking devices violates the Fourth Amendment, but such a holding may be forthcoming. One federal district court considered the issue, but found it did not have to decide the matter because the agents in that case had obtained a court order, which satisfies the requirements of the Electronic Communications Privacy Act.[84]

Lower courts are beginning to grapple with an issue the *Knotts-Karo* Court did not address: Does the Fourth Amendment apply to the *installation* of a tracking device? The *Knotts-Karo* decisions deal only with the monitoring of such a device, not its installation. (The *Knotts* Court explicitly did not rule on this issue.) At least one lower federal court has held that the installation of such a device does implicate the Fourth Amendment.[85]

7.4.2. Inviolability of the home

The home has always been the most sacrosanct Fourth Amendment enclave, primarily because the Fourth Amendment derives from the English trespass cases discussed earlier. As the Supreme Court noted in *Payton v. New York,* 445 U.S. 573 (1980), 'physical entry of the home is

[82] *United States v. Knotts,* 460 U.S. 276, 281 (1983).
[83] *United States v. Knotts,* 460 U.S. 276, 281 (1983).
[84] *United States v. Berry,* 300 F.Supp.2d 366 (District of Maryland 2004).
[85] *United States v. Garcia,* 2006 WL 298604 (Western District of Wisconsin 2006).

the chief evil against which the (...) Fourth Amendment is directed.'[86] As the *Payton* Court also noted, 'the Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant.' [87]

The Court reached a similar conclusion in *Kyllo v. United States*, 533 U.S. 27 (2001), its most recent parsing of the *Katz* standard. The issue in *Kyllo* was whether 'the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a 'search' within the meaning of the Fourth Amendment.'[88] Federal agents who suspected Danny Kyllo was growing marijuana in his home used a thermal imager to detect heat signatures in his home and garage:

> The scan (...) was performed from (...) Agent Elliott's vehicle across the street from the (...) house (...). The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes (...). Agent Elliott concluded that petitioner was using halide lights to grow marijuana in his house (...).[89]

Agents used the information from the thermal detector to obtain a warrant to search Kyllo's home, where they found a marijuana-growing operation. Indicted, Kyllo moved to suppress the results of the thermal imaging on the grounds that the scan was a warrantless search conducted in violation of the Fourth Amendment.[90] He lost at the trial and appellate court levels; those courts found Kyllo had 'no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home.[91] They also found that even if he had such an expectation, it was not objectively reasonable because the thermal imager 'did not expose any intimate details of Kyllo's life,' only (...) "hot spots" on the roof and exterior wall'.[92]

The Supreme Court reversed, holding that the Fourth Amendment is to be construed 'in a manner which will conserve public interests as well as the interests and rights of individual citizens.' [93] Its holding provides some guidance as to how the *Katz* test is to be applied when the use of new technology is at issue: 'Where (...) the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.[94]

The *Kyllo* holding has been criticized on two grounds: One is that by explicitly referring to uses of technology to 'explore details of the home', it leaves the Fourth Amendment protection of commercial and other non-residential property uncertain. The other is its reference to technology that is 'not in general public use.' This implies that once technology migrates into general public use its utilization by law enforcement is not longer a 'search' under the Fourth Amendment, an interpretation that is quite consistent with the *Katz* assumption of risk principle.

Some, at least, interpret the Third Amendment to the U.S. Constitution as providing an additional guarantee of privacy in the home, a very specific guarantee.[95] The Third Amendment provides that '[n]o Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.' [96] Others disagree with this interpretation, arguing that the Third Amendment is more properly understood as a 'structural' protection against an 'overbearing military' presence.[97] The issue will no doubt remain unresolved, since the Third Amendment has never been 'litigated in front of the United States

[86] *Payton v. New York,* 445 U.S. 573, 589 (1980).
[87] *Payton v. New York,* 445 U.S. 573, 590(1980).
[88] *Kyllo v. United States*, 533 U.S. 27, 29 (2001).
[89] *Kyllo v. United States,* 533 U.S. 27, 30 (2001).
[90] *Kyllo v. United States,* 533 U.S. 27, 30 (2001).
[91] *Kyllo v. United States*, 533 U.S. 27, 30 (2001).
[92] *Kyllo v. United States,* 533 U.S. 27, 31 (2001).
[93] *Kyllo v. United States,* 533 U.S. 27, 31 (2001).
[94] *Kyllo v. United States*, 533 U.S. 27, 31 (2001).
[95] *Katz v. United States*, 389 U.S. 347, 350 (1967) (Stewart, J., concurring); *Griswold v. Connecticut,* 381 U.S. 479, 484 (1965); *Bell v. Maryland,* 378 U.S. 225, 254 (1964) (Douglas, J., for reversing and dismissing indictment).
[96] U.S. Constitution, amendment iii.
[97] A.R. Amar, 'The Bill of Rights As a Constitution,' 100 *Yale Law Journal* (1991) 1131, 1174-1175.

Supreme Court' since it was adopted in 1791.[98] And this is unlikely to change, since American military authorities do not seem inclined to quarter troops in private residences,

7.4.3. Inviolability of the body

The Fourth Amendment is the primary guarantor of the right to be free from state-sponsored infringements of bodily integrity. Law enforcement officers generally must obtain a search warrant (or the consent of the person)[99] to obtain samples of physical evidence, such as blood, hair and saliva, from someone.

In *Schmerber* v. *California*, 384 U.S. 757 (1966), the Supreme Court explained that a search warrant is required for 'intrusions into the human body,' though it also held that a warrant is not necessary when the situation involves the exigent circumstances exception to the warrant requirement. The Schmerber Court found that the officer in that case did not violate the Fourth Amendment when he obtained a blood sample without first getting a search warrant because he was confronted with a classic exigency: the destruction of evidence. The officer in Schmerber had probable cause to believe Schmerber had been operating a vehicle while intoxicated; if the officer had, therefore, gone to a magistrate, he would have been able to obtain a search warrant authorizing the elicitation of the blood sample. The Court found, however, that if the officer had taken time to do this valuable evidence would have been destroyed, since Schmerber's body was metabolizing the alcohol in his system.

Absent such an exigency, or consent, an officer must obtain a search warrant that authorizes the minor bodily intrusions involved in obtaining samples of blood, hair, saliva or other biological evidence. The Supreme Court has imposed a more demanding standard – a 'warrant-plus' standard – for more serious intrusions, such as surgery.

In *Winston v. Lee,* 470 U.S. 753 (1985), the state of Virginia sought to compel Lee to undergo surgery to remove a bullet lodged in his chest. Virginia prosecutors claimed they needed the bullet to convict Lee of conducting an unsuccessful armed robbery, one in which he was shot by his potential victim. The state court ordered Lee to undergo surgery and he appealed, citing the Fourth Amendment.

The Supreme Court found that a 'compelled surgical intrusion into an individual's body for evidence (...) implicates expectations of privacy and security of such magnitude' that it requires special treatment under the Fourth Amendment.[100] The Court explained that '[n]otwithstanding the existence of probable cause, a search for evidence of a crime may be unjustifiable if it endangers the life or health of the suspect.'[101] It also noted that compelling someone to undergo surgery profoundly implicates 'dignitary interests in personal privacy and bodily integrity.'[102] The Court explained that these interests must be "weighed against" the community's interest in 'accurately determining guilt or innocence.'[103]

The Supreme Court therefore held that whenever the state seeks to compel someone to undergo surgery in order to obtain evidence, the court cannot merely utilize the procedure involved in issuing a search warrant; that is, it cannot simply rely on the state's showing there is probable cause to believe the procedure will result in the discovery of evidence. Instead, the Supreme Court held, in this situation the court being asked to order the procedure must first determine if probable cause exists to believe the procedure will produce relevant evidence; if the court finds that probable cause exists, it must then balance (i) the need for the evidence against (ii) the risks to the individual's health and the intrusion on his/her dignity and bodily integrity.[104]

There is another, independent standard that governs law enforcement-initiated intrusions into someone's body. In *Rochin v. California,* 342 U.S. 165 (1952), the Supreme Court applied the non-economic substantive due process analysis discussed earlier in this chapter to hold that the forcible pumping of a suspect's stomach was unconstitutional. The *Rochin* Court found that the

---

[98] T. Ekeland, 'Suspending Habeas Corpus,' 74 *Fordham Law Review* (2005) 1475, 1475 n. 5.
[99] Consent is an exception to the warrant requirement. It acts as a waiver of the individual's Fourth Amendment right, and so eliminates the need for a warrant. *Schneckloth v. Bustamonte,* 412 U.S. 218 (1973).
[100] *Winston v. Lee,* 470 U.S. 753, 759 (1985).
[101] *Winston v. Lee,* 470 U.S. 753, 759 (1985).
[102] *Winston v. Lee,* 470 U.S. 753, 760 (1985).
[103] *Winston v. Lee,* 470 U.S. 753, 760 (1985).
[104] *Winston v. Lee,* 470 U.S. 753, 766-767 (1985).

use of force to conduct such an intrusive procedure was conduct that 'shocks the conscience' and that therefore was "'close to the rack and the screw' to be tolerated. Contemporary courts have retreated from the *Rochin* holding, in that they generally will not find minor bodily intrusions such as stomach-pumping and the extraction of blood and other samples unconstitutional if the procedures were undertaken without the use of violence and/or for valid medical reasons.[105]

Genetic testing

In *Norman-Bloodsaw v. Lawrence Berkeley Laboratory,* 135 F.3d 1260 (9th Cir. 1998), the Ninth Circuit Court of Appeals held that the district court erred in granting summary judgement for a public employer who had tested its employees for "sensitive medical information," such as syphilis, sickle cell trait and pregnancy. The Ninth Circuit issues of fact existed as to whether or not the employer's testing violated the employee's due process right to privacy or right to privacy under the Fourth Amendment which, as is discussed below, applies to state-sponsored bodily intrusions.

In remanding the matter to the district court for a further proceedings (such as a trial on the merits), the Ninth Circuit cited Supreme Court decisions that have upheld drug testing by public employers and public schools.[106] The Supreme Court has held that drug testing implicates the Fourth Amendment's protection of privacy because the method involved in testing (the taking of urine) impacts on individual privacy. The Court has so far upheld drug testing in the cases brought before it by applying a particular branch of Fourth Amendment analysis. This branch is known as the "special governmental needs" exception to the Fourth Amendment's warrant requirement.[107] "[W]here a Fourth Amendment intrusion serves special governmental needs, beyond the normal need for law enforcement, it is necessary to balance the individual's privacy expectations against the Government's interests to determine whether it is impractical to require a warrant or some level of individualized suspicion in the particular context."[108]

In the *Von Raab* case, for example, the Court found it was

> clear that the Customs Service's drug-testing program is not designed to serve the ordinary needs of law enforcement. Test results may not be used in a criminal prosecution of the employee without the employee's consent. The purposes of the program are to deter drug use among those eligible for promotion to sensitive positions within the Service and to prevent the promotion of drug users to those positions. These substantial interests (...) present a special need that may justify departure from the ordinary warrant and probable-cause requirements.[109]

In special governmental needs cases, the courts balance the individual's interest in privacy (which may be reduced by having assumed certain employment or, in the case of school children, having chosen to participate in athletic or other school activities) against the need for the testing. Basically, as long as the government can articulate a valid need for the testing, show that the testing is calculated to further that need and show that a neutral selection process (e.g., testing everyone who applies for promotion to a certain position or goes out for a school activity) is used in the testing, courts will uphold it.

The Supreme Court has refused, however, to sanction a state agency's routinely disclosing the results of drug testing to police for law enforcement purposes. In *Ferguson v. City of Charleston,* 532 U.S. 67 (2001), the Supreme Court held that a state hospital's practice of testing obstetrics patients for cocaine and then reporting positive test results to police violated the Fourth Amendment because the testing was being used for law enforcement, instead of for some "special need."

Courts have applied the special governmental needs principle to uphold statutes requiring convicted offenders to undergo genetic testing.[110] As one court noted, "we hold that [the testing]

---

[105] *Lindsey v. State,* 895 So.2d 1018, 1021-1022 (Alabama Court of Criminal Appeals 2004).
[106] *Vernonia School District v. Acton,* 515 U.S. 646 (1995); *National Treasury Employees Union v. Von Raab,* 489 U.S. 656 (1989); *Skinner v. Railway Labor Executives Assn.,* 489 U.S. 602 (1989).
[107] *Vernonia School District v. Acton,* 515 U.S. 646 (1995); *National Treasury Employees Union v. Von Raab,* 489 U.S. 656 (1989); *Skinner v. Railway Labor Executives Assn.,* 489 U.S. 602 (1989).
[108] *National Treasury Employees Union v. Von Raab,* 489 U.S. 656, 665 (1989).
[109] *National Treasury Employees Union v. Von Raab,* 489 U.S. 656, 666 (1989).
[110] *People v. Kelly,* 361 Ill. App.3d 515, 838 N.E.2d 236 (Illinois Court of Appeals 2005); *Gaines v. State*, 116 Nev. 359, 998 P.2d 166 (Nevada Supreme Court 2000).

does not violate the Fourth Amendment because the State's interest in solving crimes outweighs both the convict's diminished expectation of privacy and the minimally intrusive nature of the blood draw."[111]

7.5. Communication-related rights

The constitutional rights relating to communications are: (i) the Fourth Amendment, as discussed above; (ii) the Fifth Amendment, which is discussed in the section immediately below; and (iii) the First Amendment, which is discussed in the section following the discussion of the Fifth Amendment.

7.5.1. Secrecy of communications

The three constitutional provisions cited above – the First, Fourth and Fifth Amendments — each contribute to a general right on the part of Americans to expect that their communications will remain private, subject to certain conditions.[112]

One condition is that this right exists and is enforceable only with regard to actions by government agents.[113] Eavesdropping or other intrusions by private citizens must be vindicated, if at all, in private, civil suits against the offending party.[114]

Another condition, at least for the Fourth Amendment, is that the right applies only to American citizens or to aliens residing in the United States. The Supreme Court has refused to apply the Fourth Amendment to extra-territorial invasions of privacy directed at non-U.S. citizens.[115] This means the extra-territorial interception of non-U.S. citizens' communications or data by U.S. authorities does not violate the Fourth Amendment, even though it is conducted without a search warrant.[116] And the Supreme Court has also suggested that the Fifth Amendment has no application to extra-territorial activity by U.S. authorities that is directed at non-U.S. citizens.[117]

The Fourth Amendment's contribution to the privacy of communications is examined in detail in earlier sections of this chapter. This section, therefore, will focus only on the contributions the First and Fifth Amendments respectively make to this area of privacy.

First Amendment

As § 5.2 explains, the First Amendment guarantees the rights to freedom of speech and freedom of the press. It also guarantees the rights to freedom of religion and freedom of association.[118] The latter, as the Supreme Court explained in *Roberts v. U.S. Jaycees,* 468 U.S. 609 (1984), two distinct components: freedom of expressive association and freedom of intimate association.

> In one line of decisions, the Court has concluded that choices to enter into and maintain certain intimate human relationships must be secured against undue intrusion by the State because of the role of such relationships in safeguarding the individual freedom that is central to our constitutional scheme. In this respect, freedom of association receives protection as a fundamental element of personal liberty. In another set of decisions, the Court has recognized a right to associate for the purpose of engaging in those activities protected by the First Amendment – speech, assembly, petition for the redress of grievances, and the exercise of religion. The Constitution guarantees

---

[111] *Gaines v. State*, 116 Nev. 359, 998 P.2d 166 (Nev. 2000).
[112] J.P. Nehf, 'Recognizing the Societal Value in Information Privacy,' 78 *Washington Law Review* (2003) 1, 33.
[113] L.B. Pincus & C. Trotter, 'The Disparity Between Public and Private Employee Privacy Protections,' 33 *American Business Law Journal* (1995) 51, 54.
[114] *Vollmar v. Laura*, 2006 WL 1008995 (Michigan Court of Appeals 2006); *Ball v. Ehlig,* 2005 WL 1023650 (Pennsylvania Court of Common Pleas 2005).
[115] *United States v. Verdugo-Urquidez,* 494 U.S. 259 (1990).
[116] *United States v. Gorshkov,* 2001 WL 1024026 (Western District of Washington 2001).
[117] *United States v. Verdugo-Urquidez,* 494 U.S. 259 (1990); *Johnson v. Eisentrager,* 339 U.S. 763 (1950).
[118] U.S. Constitution, amendment i.

> freedom of association of this kind as an indispensable means of preserving other individual liberties.[119]

Others have further parsed the right to freedom of expressive association into (i) a right to freedom of expressive association and (ii) a right to freedom of political association.[120]

In *McIntyre v. Ohio Elections Commission,* 514 U.S. 334 (1995), the Supreme Court held that the First Amendment right to free speech encompasses the right to speak anonymously: '[T]he interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous (...) is an aspect of the freedom of speech protected by the First Amendment.'[121] *McIntyre* and subsequent cases involved the right to anonymity in political speech;[122] the Supreme Court applied the same right to religious speech in *Watchtower Bible and Tract Society of New York, Inc. v. Village of Stratton,* 536 U.S. 150 (2002). One scholar has pointed out, correctly, that the *McIntyre* decision and other decisions addressing the right to anonymous speech have all involved anonymous political, religious or literary speech; this scholar argues that the right to anonymous speech would not extend to commercial speech because the Supreme Court has generally treated commercial speech as warranting less protection than these other types of speech.[123]

Almost forty years before it decided *McIntyre,* the Supreme Court had held that the First Amendment right to freedom of association encompasses the right to anonymous or pseudonymous association. In *National Association for the Advancement of Colored People v. State of Alabama ex rel. Patterson,* 357 U.S. 449 (1958), the Court derived this right from the 'deterrent effect on the free enjoyment of the right to associate' that would result if one's associative activity could not remain anonymous or pseudonymous. The Supreme Court reached the same conclusion in two subsequent decisions, *Gibson v. Florida Legislative Investigation Commission,* 372 U.S. 539 (1963) and *Shelton v. Tucker,* 364 U.S. 479 (1960), both of which involved governmental efforts to obtain information about individuals' membership in certain groups.

The right to anonymity in one's speech and/or in one's associations has been raised in a few cases challenging the use of subpoenas, search warrants or national security letters to obtain identifying information from someone's Internet service provider. In *Freedman v. America Online, Inc.,* 412 F. Supp.2d 174 (District of Connecticut 2005), for example, the plaintiff brought a civil rights suit claiming that local police violated his First Amendment right to anonymous speech by using an unsigned search warrant to convince his Internet service provider to disclose his name, address and account information. The officers sought the information in order to identify the person who had sent an e-mail to candidates opposing the candidate Freedman supported in a local election. The district court denied the officers' motion for summary judgement on Freedman's First Amendment claim, holding that issues of fact exist as to whether the e-mail in question was valid First Amendment speech or was, as the officers argued, reasonably interpretable as a threat. Threats are not protected by the First Amendment.[124]

Another district court case raised the issue of whether the Federal Bureau of Investigation's use of National Security Letters [NSLs] to obtain subscriber and other information from Internet service providers violates the rights to anonymous speech and association guaranteed by the First Amendment. NSLs are, as the district court noted, ' a unique form of administrative subpoena cloaked in secrecy and pertaining to national security issues.'[125] The statute authorizing NSLs – 18 U.S. Code § 2709 – allows the FBI to obtain customer records by merely certifying that the information is relevant to a terrorism investigation; it also includes a provision

---

[119] *Roberts v. U.S. Jaycees,* 468 U.S. 609, 617-618 (1984).
[120] B. Richards, 'The Boundaries of Religious Speech in the Government Workplace,' 1 *University of Pennsylvania Journal of Labor and Employment Law* (1998) 745, 780.
[121] *McIntyre v. Ohio Elections Commission,* 514 U.S. 334, 342 (1995).
[122] *Buckley v. American Constitutional Law Foundation, Inc.* 525 U.S. 182 (1999).
[123] S.K. Sandeen, 'In For A Calf Is Not Always In For A Cow: An Analysis Of The Constitutional Right Of Anonymity As Applied To Anonymous E-Commerce,' 29 *Hastings Constitutional Law Quarterly* (2002) 527, 551-569.
[124] *Freedman v. America Online, Inc.,* 412 F. Supp.2d 174, 185-187 (District of Connecticut 2005).
[125] *Doe v. Ashcroft,* 334 F. Supp.2d 471, 475 (Southern District of New York 2004).

under which the recipient of an NSL can be barred from disclosing that fact to its customer or to any other person who is the object of the NSL.[126]

In *Doe v. Ashcroft,* 334 F. Supp.2d 471 (Southern District of New York 2004), the district court held that the NSL statute potentially infringed Internet service provider subscribers' First Amendment rights of anonymous speech and association because it did not permit sufficient judicial review to preserve those rights. This court found, among other things, that

> such First Amendment rights may be infringed by application of § 2709 in a given case. For example, the FBI theoretically could issue to a political campaign's computer systems operator a § 2709 NSL compelling production of the names of all persons who have email addresses through the campaign's computer systems. The FBI theoretically could also issue an NSL under § 2709 to discern the identity of someone whose anonymous online web log, or "blog," is critical of the Government. Such inquiries might be beyond the permissible scope of the FBI's power under § 2709 because the targeted information might not be relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, or because the inquiry might be conducted solely on the basis of activities protected by the First Amendment. These prospects only highlight the potential danger of the FBI's self-certification process and the absence of judicial oversight.[127]

The district court therefore declared the NSL statute unconstitutional and enjoined the Attorney General of the United States and the Federal Bureau of Investigation from enforcing NSLs.[128] The government appealed to the Second Circuit Court of Appeals. The Second Circuit vacated this decision and remanded the matter for further consideration, in light of an amendment to § 2709 which now allows Internet service providers to seek legal counsel as to whether they should comply with a request and provides for judicial review of the terms and conditions of nondisclosure imposed on the recipient of an NSL letter.[129] The Second Circuit remanded the matter because the plaintiff credibly argued that implementation of the amended statute would still violate First Amendment rights to anonymity in speech and association; it concluded that it would be better to have 'these novel First Amendment issues' resolved by the district court. [130]

In a different context, the Virginia Court of Appeals held that the state anti-spam statute did not violate the First Amendment right to anonymous speech. In *Jaynes v. Commonwealth,* 48 Va. App. 673, 634 S.E.2d 357 (Virginia Court of Appeals 2006), Jeremy Jaynes appealed his conviction for violating the Virginia unsolicited bulk email statute. The statute makes it a felony for someone to use 'a computer or computer network with the intent to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider of its subscribers'.[131] Jaynes argued, among other things, that the statute was ' overbroad because its language prohibits anonymous speech of a non-commercial nature and that the First Amendment protects such speech.' unconstitutionally overbroad under the First Amendment when it prohibits a substantial amount of protected speech, either absolutely or as compared to the unprotected conduct also encompassed by the statute.

The Virginia court began its analysis of this argument by explaining that a law is 'unconstitutionally overbroad under the First Amendment when it prohibits a substantial amount of protected speech, either absolutely or as compared to the unprotected conduct also encompassed by the statute.'[132] After analyzing the history and purpose of the statute, the court held that Jaynes' First Amendment argument was 'not relevant. The [statute] proscribes no speech. Rather, the statute proscribes intentional falsity as a machination to make massive, uncompensated use of the private property of an ISP. Therefore, the statute cannot be overbroad because no protected speech whatsoever falls within its purview.' [133]

---

[126] *Doe v. Ashcroft,* 334 F. Supp.2d 471, 475 (Southern District of New York 2004).
[127] *Doe v. Ashcroft,* 334 F. Supp.2d 471, 507 (Southern District of New York 2004).
[128] *Doe v. Ashcroft,* 334 F. Supp.2d 471, 525 (Southern District of New York 2004).
[129] *Doe v. Gonzales,* 449 F.3d 415, 419 (2d Cir. 2006).
[130] *Doe v. Gonzales,* 449 F.3d 415, 419 (2d Cir. 2006).
[131] Virginia Code § 18.2-152.3:1.
[132] Virginia Code § 18.2-152.3:1.
[133] Virginia Code § 18.2-152.3:1.

The Washington Court of Appeals reached a similar conclusion in *State v. Heckel,* 122 Wash. App. 60, 90 P.3d 189 (Washington Court of Appeals 2004). This court relied on the Supreme Court's holding in *Central Hudson Gas & Electric Corporation v. Public Service Commission of New York,* 447 U.S. 557 (1980): 'For commercial speech to come within [the First Amendment], it at least must concern lawful activity and not be misleading.' The Washington court found that the statute at issue in that case did not violate the First Amendment because it targeted only commercial speech that *was* misleading.

Fifth Amendment

As noted at the beginning of this chapter, the Fifth Amendment privilege against self-incrimination plays a very modest role in protecting online privacy. Although the nineteenth century Supreme Court found that the privilege played an integral role in protecting "the privacies of life",[134] the modern Court has reduced its role to barring the government from "compelling" someone to provide "testimony" that is "incriminating."[135] The three requirements – compelled incriminating testimony – derive from the language the amendment uses to establish the privilege against self-incrimination, e.g., that "[n]o person (...) shall be compelled in any criminal case to be a witness against himself".[136]

The Fifth Amendment privilege only comes into play when all three elements are present.[137] Compulsion usually takes the form of a subpoena – – usually a grand jury subpoena – enforceable by civil contempt sanctions.[138] The Supreme Court has held that the Fifth Amendment, as such, only encompasses the type of judicial compulsion represented by civil contempt sanctions; it, unlike the derived protections of *Miranda,* does not apply to police interrogation. [139]

As noted above, the compulsion must seek to extort "testimony" — oral, written or other communications (such as gestures) — from an individual[140] because the Fifth Amendment privilege does not encompass physical evidence *per se*.[141] So the Fifth Amendment privilege protects someone from being compelled to write incriminating testimony, but it does not protect them from providing samples of their handwriting, hair, blood or other physical evidence.[142]

The act of *producing* non-testimonial physical evidence (e.g., documents, guns, videotapes, videotapes, etc.) in response to government compulsion can itself be a testimonial act encompassed by the privilege. [143] To be 'testimonial,' the act of producing evidence must establish that the evidence exists, that it is within the control of the person being compelled to produce it and that the evidence produced is 'authentic,' i.e., is the evidence sought by the subpoena. [144] If the judicially compelled act of producing physical evidence is testimonial (and is incriminating), then the person being ordered to produce the evidence can invoke the Fifth Amendment privilege against self-incrimination and refuse to produce the evidence.

As noted above, the third requirement is that the compelled testimony be "incriminating". In parsing this requirement, the Supreme Court has held that the privilege "not only extends to answers that would in themselves support a conviction under a (...) criminal statute but likewise embraces those which would furnish a link in the chain of evidence needed to prosecute the claimant for a (...) crime."[145] In *Ohio v. Reiner,* 532 U.S. 17 (2001), the Supreme Court reiterated this standard and applied it to find that someone can invoke the Fifth Amendment privilege even

---

[134] *Boyd v. United States*, 116 U.S. 616, 630 (1886).
[135] *United States v. Braswell,* 465 U.S. 605, 611 n. 8 (1984); *Fisher v. United States,* 425 U.S. 391, 399 (1976).
[136] U.S. Constitution amendment v. *Andresen v. Maryland* 427 U.S. 463, 472 (1976).
[137] *Fisher v. United States,* 425 U.S. 391, 399 (1976).
[138] *United States v. Mandujano,* 425 U.S. 564, 571-572 (1976).
[139] *United States v. Mandujano,* 425 U.S. 564, 571-572 (1976).
[140] Corporations and other artificial entities are not protected by the privilege. *Braswell v. United States,* 487 U.S. 99, 105-108 (1988).
[141] *Schmerber v. California*, 384 U.S. 757, 763-764 (1966) ('[T]hd protection of the privilege reaches an accused's communications, whatever form they might take (...). but that compulsion which makes a suspect or accused the source of "real or physical evidence' does not violate it").
[142] *United States v. Dionisio,* 410 U.S. 1, 7 (1973); *Schmerber v. California*, 384 U.S. 757, 763-764 (1966).
[143] *Fisher v. United States,* 425 U.S. 391, 399 (1976).
[144] *Fisher v. United States,* 425 U.S. 391, 399 (1976).
[145] *Hoffman v. United States*, 341 U.S. 479, 486 (1951).

though they claim to be innocent of any crime because an 'innocent witness' truthful responses may provide the government with incriminating evidence from the speaker's own mouth.' (In the *Reiner* case a babysitter denied shaking a child who subsequently died, claiming the father must have been responsible for the injuries; the Court found that notwithstanding this denial of responsibility, the witness could claim the privilege because testifying might provide the prosecution with evidence – such as her access to the child – that could be used against her in a criminal proceeding.)

It is the requirement that all three elements be present which accounts for the limited role the Fifth Amendment plays in guaranteeing online privacy. Actually, the primary obstacles are the first two elements—the requirements that the government must be seeking to "compel" someone to provide 'testimony.'

'Testimony' is an act that 'must itself, explicitly or implicitly, relate a factual assertion or disclose information.'[146] Most of the constituent elements of cyberspace – e.g., websites, postings to newsgroups, conversations in chat rooms, e-mail, etc.—clearly qualify as 'testimony' under this definition because they involve the making of factual assertions and/or disclosing information. It is of no moment that the facts asserted or the information disclosed may be false; 'testimony' can be true or false. What is important in determining whether or not a component of cyberspace satisfies this test is whether it 'communicates' something factual. And while much of what appears in cyberspace takes the form of textual communication, this is not the only form in which information can be communicated and thereby qualify as 'testimony.'" It is, for example, possible to infer factual assertions from the graphical components of at least some websites; unlike the physiological processes which the Supreme Court have found to yield physical evidence instead of testimony,[147] the intellectual process involved in designing the non-textual aspects of a website can produce implicit testimonial communications.

The problem – insofar as someone's ability to invoke the privilege against self-incrimination is concerned – is that this testimony was not "compelled" by the government.

The Fifth Amendment provides no protection for communications that one makes voluntarily; voluntary 'testimony' given at any point in time waives the privilege.[148] Therefore, any comments that are posted online—in whatever form—will be outside the privilege because the person responsible was not 'compelled' to post them – was not, in other words, 'compelled' to testify. The Supreme Court has held that the rule governing voluntary statements also applies to documents; by preparing a document, one voluntarily gives the testimony it contains and cannot, therefore, claim the privilege as to its contents.[149] The Court has indicated that diaries may be governed by a different rule. [150]

This is true regardless of whether the comments are posted in 'public' areas such as websites or in 'private' conversations in a 'chat room.' Someone in a chat room conversing with an undercover officer is under no compulsion to have that conversation; indeed, she cannot be under any official compulsion because she is not aware she is 'speaking to' an agent of the state.[151] Compulsion is therefore quite lacking as to the content of communications posted online.

The area in which the Fifth Amendment can come into play involves the use of encryption. As explained earlier in this chapter, to have a Fourth Amendment expectation of privacy in the content of online communications such as e-mail, the correspondents must take steps designed to ensure that the content cannot be read by anyone other than the sender and the intended recipient(s). One way of doing this is to use encryption. If someone uses strong encryption to secure their e-mail or other online communications, the only way law enforcement can access the content of those files is with the key that can be used to decrypt the files.

---

[146] *Doe v. United States,* 487 U.S. 201, 210 (1988).

[147] *United States v. Dionisio,* 410 U.S. 1, 7 (1973) (suspect did not 'testify' by simply reading transcript; purpose was to obtain a sample that could be used to measure the physical properties of his voice); *Gilbert v. California,* 388 U.S. 263, 266-267 (1967) (requiring suspect to provide samples of his handwriting by copying letters and symbols as directed did not elicit 'testimony').

[148] *United States v. Mandujano*, 425 U.S. 564, 571-572 (1976).

[149] *United States v. Doe*, 465 U.S. 605, 610-611 (1984); *Fisher v. United States,* 425 U.S. 391, 409-410 (1976).

[150] *Fisher v. United States,* 425 U.S. 391, 401 n. 7 (1976).

[151] *Hoffa v. United States,* 385 U.S. 293, 303-304 (1966).

Can the owner of data or online communications be compelled to give up her encryption key? If law enforcement officers ask for the key, the owner can refuse to give it to them and will face no consequences unless some statutory scheme has been put in place that requires the surrender of encryption keys; no such scheme currently exists in the United States. Another alternative for law enforcement is to obtain a grand jury subpoena which directs the owner of the encryption key to produce the key to the grand jury; this *may* implicate the Fifth Amendment privilege against self-incrimination.

The subpoena establishes compulsion and it is reasonable to assume, if only for the purposes of analysis, that the contents of the encrypted files will incriminate their owner.[152] The critical question, therefore, is whether or not the subpoena compels the production of incriminating *testimony*.

Answering this question requires considering two different scenarios: In the first, the owner of the files has somehow committed the key to memory, so to 'produce' the key to the grand jury she would have to appear before the grand jury and tell them what the key is. In the second scenario, the owner of the files has recorded the key somewhere, in a diary, let us say; to 'produce' this key to the grand jury she would have to give the grand jury the entry in the diary.

If the owner of the files committed the key to memory, then she can claim the Fifth Amendment privilege and refuse to recite it before the grand jury as long as the contents of the files would incriminate her. Reciting the key to the grand jury constitutes a factual assertion: The owner is being asked 'what is the key needed to un-encrypt these files'; if she answers, she would be responding with a factual assertion in the form of 'The key needed to encrypt these files is (...).' Her response is a communication and therefore clearly constitutes testimony.[153] And while the key itself may not be incriminating, it becomes a link in the chain of evidence needed to prosecute her if the contents of the files are incriminating, since the government cannot access the contents of those files unless she 'testifies' as to the key.[154]

This, however, does not completely resolve the matter: While the privilege would protect the witness from being compelled to recite a memorized encryption key, the government could override her claim of the privilege by granting her immunity for the act of producing the key.[155] The decision to confer immunity is entirely within the government's discretion; if the government decides to give the witness immunity, she cannot refuse. She must then either give up the key or face sanctions for civil contempt (incarceration) until she does so. The immunity protects the witness from having the act of producing the key, or any evidence derived from that act, being used to prosecute her for a crime; it does not prevent a prosecution based on evidence independent of that act.[156]

Now assume the key was recorded as a diary entry. For the purpose of this analysis, it is irrelevant whether the entry was made in a paper diary or in a computer-generated diary. The form of the recordation is not important; what is important is that the key has been transformed from mere memory into a tangible record.

The key itself is not 'testimony'; it is now an artifact, not a communication.[157] But if the owner delivers the key to the grand jury, it can be used to 'produce' the contents of the encrypted files. (We are assuming the government has the files, but their content is inaccessible without the key.) The issue therefore is whether the owner's act of giving the entry containing the key to the grand jury is a testimonial act of production encompassed by the privilege against self-incrimination.[158] If the act of providing the key is 'testimony,' the owner can claim the privilege because the elements

---

[152] More precisely, it is reasonable to assume that the contents of the files will incriminate their owner in some already completed criminal activity. *United States v. Freed,* 401 U.S. 601, 606-607 (1971) (Fifth Amendment privilege cannot be claimed to insulate one from liability for criminal activity yet to be committed).

[153] *United States v. Hubbell,* 530 U.S. 27, 43 (2000); *United States v. Doe*, 487 U.S. 201, 210 n. 9 (1988).

[154] *See supra* text accompanying note 145.

[155] *United States v. Hubbell,* 530 U.S. 27, 43 (2000).

[156] *United States v. Hubbell,* 530 U.S. 27, 43 (2000).

[157] D.W. Wolfe, 'The Government's Right to Read, 49 *Emory Law Journal* (2000) 711, 737-738.

[158] We are assuming the government knows the witness has the key. If the government does not know this, then the act of handing over the recorded entry would itself be a testimonial act of production within the scope of the privilege. By giving the grand jury the key, the owner 'tells' the state something it did not already know, e.g., that she has the key needed to encrypt the files.

of compulsion and incrimination are present; if the act of providing the key is not testimonial, the owner cannot claim the privilege.

While the Supreme Court has not addressed this particular situation, it has observed that the act of producing the key to a strongbox containing incriminating documents is not 'testimony' within the scope of the Fifth Amendment privilege, but the act of reciting the combination to a wall safe containing such documents is.[159] The distinction the Court draws is whether the act in question requires an individual to express 'the contents of his own mind'.[160] Handing over a tangible key is a purely physical act like the other acts the Court has found not to be testimonial; but reciting a combination does require the person to use his or her mind to make a factual assertion, e.g., 'the combination to the safe is (...).' When the encryption key was recorded, it assumed tangible form and became an artifact like the key to a strongbox; since it has an independent, external existence, the owner of the files can give the key to the grand jury without having to communicate the contents of her own mind. Consequently, she apparently cannot claim the Fifth Amendment privilege as to the act of doing so.

The above analysis is based on scenarios in which a grand jury subpoenas an encryption key. What, if any, role does the Fifth Amendment play when law enforcement officers approach someone and ask her to surrender an encryption key? If she elects to comply—either by reciting a memorized key or handing over a recorded key – that would be a voluntary act outside the scope of the privilege against self-incrimination. She can, on the other hand, decline to provide the key without consequence because officers currently cannot compel someone to comply with their request.

Could they be given that ability? Could a statute be enacted that made it a crime to refuse to produce an encryption key to officers upon request? Such a statute could certainly be adopted, but its application would be unconstitutional if the holder of a key could invoke the Fifth Amendment privilege as the basis for refusing to produce the key; the key holder would be faced with the alternatives of giving up the key and thereby providing 'testimony' that incriminated her or refusing to give up it up and being held criminally liable for refusing to do so. This dilemma violates the Fifth Amendment. Enforcing the statute would, in other words, be unconstitutional (a) when the key holder had memorized the key and (b) when the government did not already know someone was the possessor of a key (in whatever form). Enforcing the statute in these instances would not, as noted above, violate the Fifth Amendment if the statute gave the key holder immunity for the act of producing the key. And even absent a grant of immunity, enforcing the statute would not violate the Fifth Amendment if the government knew the person possessed a key and if the key had been reduced to tangible, recorded form.

An effort to invoke the Fifth Amendment privilege against self-incrimination in response to subpoenas requesting encryption keys has appeared, so far, in only one U.S. case: *In re Amato,* 2005 WL 1429743 (District of Maine 2005). Amato was a chiropractor who moved to quash two subpoenas requiring the producing of various types of physical evidence, including 'passwords, password files (...) encryption codes or other information necessary to access" computer equipment federal agents had seized from his professional offices pursuant to a search warrant. Amato tried to invoke the arguments outlined above, arguing that the act of producing this evidence was (a) testimonial and (b) incriminating and therefore justified his invoking the Fifth Amendment privilege. The district court rejected his argument because it found that the subpoenas were addressed to Amato solely in his capacity as the custodian of corporate records. (He operated his practice as a corporation.) Since, as noted above, corporations do not have a privilege against self-incrimination under the Fifth Amendment, Amato could not invoke the privilege, as he could have done if the subpoenas had been directed to him in his personal capacity.

[159] *United States v. Hubbell,* 530 U.S. 27, 43 (2000); *United States v. Doe*, 487 U.S. 201, 210 n. 9 (1988).
[160] *United States v. Doe*, 487 U.S. 201, 210 n. 9 (1988).

7.5.2. Freedom of speech

The First Amendment to the U.S. Constitution provides, in pertinent part, that 'Congress shall make no law (...) abridging the freedom of speech, or of the press'. The Supreme Court has historically given these guarantees a liberal interpretation. As a result, there are very few restrictions that can be constitutionally placed upon speech (which includes 'symbolic or expressive conduct as well as (...) actual speech')[161] in the United States.

The Supreme Court has held that states can generally criminalize the use of 'fighting words' – 'those personally abusive epithets which, when addressed to the ordinary citizen, are (...) inherently likely to provoke violent reaction'.[162] The First Amendment 'guarantees of free speech and free press do not permit a State to forbid or proscribe advocacy of the use of force or of law violation except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action.'[163]

The First Amendment also lets states criminalize threats of violence, or what are commonly referred to as 'true threats.'[164] 'True threats' encompass 'statements where the speaker means to communicate a serious expression of an intent to commit an act of unlawful violence to a particular individual or group of individuals.'[165] 'The speaker need not actually intend to carry out the threat. Rather, a prohibition on true threats "protect[s] individuals from the fear of violence" and "from the disruption that fear engenders," in addition to protecting people "from the possibility that the threatened violence will occur."'[166]

The Supreme Court has held that a narrowly-defined class of obscene speech can be outlawed essentially because the Court considers that it has little if any social value. In *Miller v. California,* 413 U.S. 15 (1973), the Court held that states can constitutionally obscene material, i.e., material that depicts or describes 'sexual conduct.'[167] The *Miller* Court also held that state laws criminalizing obscene material 'must be limited to works which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way, and which, taken as a whole, do not have serious literary, artistic, political, or scientific value.'[168] In making that determination the trier of fact must apply 'contemporary community standards.'[169] Some have suggested that the Court's reliance on community standards has been undermined by cyberspace, which tends to erode parochial standards. The Supreme Court noted this criticism in *Ashcroft v. American Civil Liberties Union,* 535 U.S. 565 (2002), in which it analyzed the constitutionality of a statute that utilized a similar standard in prohibiting the dissemination of material that is 'harmful to minors.' It is likely that the Court will have to revisit its reliance on the *Miller* 'community standard' test at some point in the future.

The Supreme Court has held that child pornography the creation of which involves the use of 'real' children can be outlawed because of the physical and emotional injury its creation inflicts upon those children.[170] The Court has held that 'virtual' child pornography – computer-generated child pornography the creation of which did not involve the actual victimization of real children – is speech that is protected by the First Amendment and so cannot be outlawed.[171]

In 2003, Congress responded to the Supreme Court's striking down the old federal prohibition on child pornography by adopting a new virtual child pornography prohibition in the PROTECT Act, Public Law No. 108-21, §§ 102-601, 117 Stat. 650 (2003). Commentators generally agree that this new prohibition, which is functionally indistinguishable from its predecessor, is equally unconstitutional under the First Amendment.[172] In holding that another child pornography-related provision of the PROTECT Act was unconstitutional, the Eleventh Circuit Court of Appeals noted

---

[161] *Virginia v. Black,* 538 U.S. 343, 358 (2003).
[162] *Cohen v. California,* 403 U.S. 15, 20 (1971).
[163] *Brandenburg v. Ohio,* 395 U.S. 444, 447 (1969).
[164] *Virginia v. Black,* 538 U.S. 343, 359 (2003).
[165] *Virginia v. Black,* 538 U.S. 343, 359 (2003).
[166] *Virginia v. Black,* 538 U.S. 343, 359 (2003).
[167] *Miller v. California,* 413 U.S. 15, 23 (1973).
[168] *Miller v. California,* 413 U.S. 15, 23 (1973).
[169] *Miller v. California,* 413 U.S. 15, 23 (1973).
[170] *New York v. Ferber,* 458 U.S. 747 (1982).
[171] *Ashcroft v. Free Speech Coalition,* 535 U.S. 234 (2002).
[172] B. G. Slocum, 'Virtual Child Pornography,' 14 *Albany Law Journal of Science and Technology* (2004) pp. 637, 641-642.

that the provision criminalizing virtual child pornography may not withstand constitutional scrutiny.[173] So far, no reported decision has addressed the constitutionality of the new prohibition.

7.6. Other and new constitutional rights

A few civil rights suits have been filed in which the plaintiffs claim that problems with electronic voting machines violate their constitutional right to vote.[174] Essentially, the federal courts have refused to grant relief, finding that the plaintiffs only allege "incompetence" rather than actionable election fraud. [175] As one scholar has explained, federal courts "have been extremely reluctant to become involved in election disputes" because of "concerns over federalism and encroachment into predicaments reserved for the legislative branch".[176]

In 2006, the District of Columbia Court of Appeals used the non-economic substantive due process standard discussed earlier in this chapter to hold that terminally-ill patients had a constitutional right to access potentially life-saving experimental drugs.[177] More precisely, the D.C. Circuit held that

> a terminally ill, mentally competent adult patient's informed access to potentially life-saving investigational new drugs determined by the FDA after Phase I trials to be sufficiently safe for expanded human trials warrants protection under the Due Process Clause. The prerogative asserted by the FDA – to prevent a terminally ill patient from using potentially life-saving medication to which those in Phase II clinical trials have access – thus impinges upon an individual liberty deeply rooted in our Nation's history and tradition of self-preservation.[178]

One judge dissented, arguing that courts should be hesitant to create new constitutional rights and asserting that the plaintiff in the case was impermissibly trying to circumvent public debate and the legislative process by going through the courts.[179] On the whole, it seems unlikely that this constitutional right will receive general acceptance, if only because the courts tend to be parsimonious in using non-economic substantive due process to create new constitutional rights.

7.7 Conclusion

From the perspective of an American lawyer, anyway, the American system of constitutional rights appears to do a generally satisfactory job of protecting digital privacy. The broad protections the First Amendment provides to speech and other expressive conduct, as well as to the rights of association and religion, are certainly adequate, whether in the online or offline context. And the Supreme Court's use of non-economic substantive due process doctrines to guarantee personal privacy in areas not explicitly addressed by Constitutional amendments has

---

[173] *United States v. Williams,* 444 F.3d 1286, 1299 (11th Cir. 2006).
[174] *Bodine v. Elkhart County Election Board,* 788 F2d 1270 (7th Circuit Cout of Appeals 1986); *Ryan v. Board of Election Commissioners of DuPage County*, 1994 WL 505412 (District Court for the Northern District of Illinois 1994).
[175] *Bodine v. Elkhart County Election Board,* 788 F2d 1270 (7th Circuit Cout of Appeals 1986); *Ryan v. Board of Election Commissioners of DuPage County*, 1994 WL 505412 (District Court for the Northern District of Illinois 1994).
[176] C. W. Gramble, 'The Risks of Computerized Election Fraud: When Will Congress Rectify a 38-Year-Old Problem?,' 57 *Alabama Law Review* (2006) pp. 1123, 1152.
[177] *Abigail Alliance for Better Access to Developmental Drugs v. Von Eschenbach,* 445 F.3d 470, 487 (District of Columbia Court of Appeals 2006).
[178] *Abigail Alliance for Better Access to Developmental Drugs v. Von Eschenbach,* 445 F.3d 470, 487 (District of Columbia Court of Appeals 2006). 'The FDCA directs the Secretary [of the U.S. Department of Health and Human Services] to promulgate regulations for testing new drugs (...). Pursuant to this authority, the FDA has promulgated regulations that require three phases of government testing on humans before investigational new drugs can receive FDA approval and enter the commercial marketplace. In Phase I, new drugs are tested on 20 to 80 human subjects to determine "the side effects associated with increasing doses, and, if possible, to gain early evidence on effectiveness." 21 C.F.R. § 312.21(a). It takes approximately one year to conduct Phase I testing. FDA counsel acknowledged at oral argument that drugs that survive this phase have been deemed "sufficiently safe for substantial human testing, but [are] not yet proven to be safe and effective to the satisfaction of the FDA [to be commercially marketed]." (...) Phase II involves targeted, controlled clinical studies of up to several hundred human subjects "to evaluate the effectiveness of the [Phase I investigational new] drug ... and to determine the common short-term side effects and risks associated with the drug." 21 C.F.R. § 312.21(b).' 445 F.3d at 473.
[179] *Abigail Alliance for Better Access to Developmental Drugs v. Von Eschenbach,* 445 F.3d 470, 487-495 (District of Columbia Court of Appeals 2006).

so far proven adequate to extend the core protections of those amendments to areas that have become of evolving importance as the centuries pass. The Supreme Court may not move as quickly, or as extensively, in this regard as some citizens would like, but it tends to be conservative, both because of the predispositions of many of the Justices and because, as was noted earlier, the assumption is that the Court should generally defer to legislative rule-making in this context.

The most critical gap in constitutional privacy protections comes in the area of data privacy; more specifically, it exists in the area of third-party records. As was explained earlier, the Supreme Court has held that citizens 'assume the risk' – assume the loss of privacy – whenever they share information with third-parties, such as financial institutions, Internet service providers, utility companies, etc. On the one hand, this is a faithful, literal application of the spatially-based conception of privacy that existed when the Fourth Amendment was adopted; on the other hand, however, it is completely inconsistent with the realities of the modern world. As I have argued elsewhere, the Supreme Court can address this issue by adapting the Fourth Amendment conception of privacy to modern realities, i.e., by abandoning a strictly spatially-based conception and moving to a broader, transactional-based conception.[180]

The Court might also be advised to expand somewhat the Fifth Amendment's application to privacy, insofar as privacy involves data and what the Fourth Amendment refers to as 'papers.' As was noted earlier in this chapter, the nineteenth-century Supreme Court used a fusion of the Fourth and Fifth Amendment provisions to carve out a zone of privacy for personal 'papers.' The twentieth-century Supreme Court has so far consistently retreated from that approach, preferring to construe all voluntarily-created documents and data as being outside the protections of the Fifth Amendment. The effect of this is to deny citizens the ability to rely on the Fifth Amendment privilege against self-incrimination as the basis for refusing to surrender 'private' data to the government. This, in turn, creates what one might describe as a loophole: If the government knows of the existence and location of incriminating (un-encrypted) data and has probable cause to believe the data is relevant to the investigation of criminal activity, it can obtain a search warrant to locate and seize the data against the owner's wishes. If, on the other hand, the government cannot establish probable cause and does not know the location of incriminating (un-encrypted) data, it can have a grand jury issue a subpoena to the person who may have access to the data and thereby compel that individual to produce it. The net effect of parsing the Fourth and Fifth Amendments severally is, therefore, to effectively deny U.S. citizens any type of 'safe harbor' for recorded facts, thoughts and opinions. The Supreme Court could, if it were so inclined, utilize a version of the *Boyd* principle to address this effect and give citizens an increased ability to insulate certain types of evidence from the government.

References

V.C. Abreu, 'The Malleable Use of History in Substantive Due Process Jurisprudence,' 44 *Boston College Law Review* (2002) 177 et seq.

A.R. Amar, 'The Bill of Rights As a Constitution,' 100 *Yale Law Journal* (1991) 1131 et seq.

S.W. Brenner, 'The Fourth Amendment in an Era of Ubiquitous Technology,' 75 *Mississippi Law Journal* (2005) 1 et seq.

S.W. Brenner & L.L. Clarke, 'Fourth Amendment Protections for Shared Privacy Rights In Stored Transactional Data,' 14 *Journal of Law and Policy* (2006) 211 et seq.

S.G. Calabresi, 'The Originalist and Normative Case Against Judicial Activism," 103 *Michigan Law Review* (2005) 1081 et seq.

S.G. Calabresi, 'The Tradition of the Written Constitution,' 57 *Alabama Law Review* (2006) 635 et seq.

R.M. Cover, 'The Origins of Judicial Activism in the Protection of Minorities, 91 *Yale Law Journal* (1982) 1287 et seq.

[180] S. W. Brenner, 'The Fourth Amendment in an Era of Ubiquitous Technology,' 75 *Mississippi Law Journal* (2005) 1; S.W. Brenner & L.L. Clarke, 'Fourth Amendment Protections for Shared Privacy Rights In Stored Transactional Data,' 14 *Journal of Law and Policy* (2006) 211.

T. Ekeland, 'Suspending Habeas Corpus,' 74 *Fordham Law Review* (2005) 1475 et seq.
D.A. Farber, 'The Originalism Debate," 49 *Ohio State Law Journal* (1989) 1085 et seq.
R.W. Garnett, 'Personal Reflections on the Chief,' 10 *Texas Review of Law & Politics* (2006), 283 et seq.
K. Gormly, 'One Hundred Years of Privacy,' 1992 *Wisconsin Law Review* 1335 et seq.
C.W. Gramble, 'The Risks of Computerized Election Fraud: When Will Congress Rectify a 38-Year-Old Problem?,' 57 *Alabama Law Review* (2006) 1123 et seq.
S.E. Henderson, 'Nothing New Under the Sun? A Technologically-Rational Doctrine of Fourth Amendment Search,' 56 *Mercer Law Review* (2005) 507 et seq.
N.B. Lasson, *The History and Development of the Fourth Amendment to the United States Constitution* (Baltimore: Johns Hopkins Press, 1937), pp. 79-105.
E.P. Lowe, 'Emailer Beware: The Fourth Amendment and Electronic Mail,' 2 *Oklahoma Journal of law & Technology* (2005) 28 et seq.
G.P. Magarian, 'Substantive Due Process as a Source of Constitutional Protection for Nonpolitical Speech,' 90 *Minnesota Law Review* (2005) 247 et seq.
J.P. Nehf, 'Recognizing the Societal Value in Information Privacy,' 78 *Washington Law Review* (2003) 1 et seq.
M.S. Pardo, 'Disentangling the Fourth Amendment and the Self-Incrimination Clause,' 90 *Iowa Law Review* (2005) 1857 et seq.
L.B. Pincus & C. Trotter, 'The Disparity Between Public and Private Employee Privacy Protections,' 33 *American Business Law Journal* (1995) 51 et seq.
B. Richards, 'The Boundaries of Religious Speech in the Government Workplace,' 1 *University of Pennsylvania Journal of Labor and Employment Law* (1998) 745 et seq.
R.D. Rotunda & J.E. Nowak, *Treatise on Constitutional Law* (3d ed.) (West Publishing, St. Paul, MN 2006).
S.K. Sandeen, 'In For A Calf Is Not Always In For A Cow: An Analysis Of The Constitutional Right Of Anonymity As Applied To Anonymous E-Commerce,' 29 *Hastings Constitutional Law Quarterly* (2002) 527 et seq.
R. Simmons, 'From *Katz* to *Kyllo:* A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies,' 53 *Hastings Law Journal* (2002) 1303 et seq.
B.G. Slocum, 'Virtual Child Pornography*,'* 14 *Albany Law Journal of Science and Technology* (2004) pp. 637 et seq.
D.C. Williams, 'Civic Constitutionalism, The Second Amendment, and the Right of Revolution,' 79 *Indiana Law Journal* (2004), 379 et seq.
R. Winick, 'Searches and Seizures of Computers and Computer Data,' 8 *Harvard Journal of Law & Technology* (1994) 75 et seq.
D.W. Wolfe, 'The Government's Right to Read, 49 *Emory Law Journal* (2000) 711 et seq.

8. Conclusion

Paul de Hert,[1] Bert-Jaap Koops,[2] Ronald Leenes[3]

8.1. General

This report offers the result of a comparative study commissioned by the Dutch Ministry of the Interior and Kingdom Relations. It contains six country reports, covering Belgium, Canada, France, Germany, Sweden, and the US. Every chapter studies the changes in constitutional rights and human-rights policy related to developments in ICT and other new technologies. The main focus is on the constitutional rights to privacy and data protection, inviolability of the body, inviolability of the home, secrecy of communication, and freedom of expression. As mentioned in the introduction, this report is a sequel to an earlier study carried out in 1999-2000 under supervision of Alis Koekkoek of Tilburg University.[4] The present study contains the same countries as the Koekkoek report. The central question in this report is to identify which developments have taken place in Belgium, Canada, France, Germany, Sweden, and the US with respect to constitutional rights and new technologies, in particular since 2000.

The authors of this report are not the same as the authors that contributed to the Koekkoek report. Their contributions are thus fresh and in the way their analysis consolidates the findings in the Koekkoek report, they add to the solidness of the academic preparations for possible Dutch reforms. The current authors have not restricted themselves to a description of the constitutional developments after 2000, so that all chapters can be read as independent descriptions of the constitutional systems of the six countries in relation to new technologies. All chapters contain a state-of-the-art analysis, with examples taken from the most recent constitutional developments.

On the basis of these analyses, this chapter will indicate general trends, signal some striking similarities and differences between the countries, and give a few recommendations for the Dutch legislator that can be distilled from these developments.

8.2. General constitutional characteristics and developments

8.2.1. Little constitutional dynamics as a general trend

A first sub-question dealt with in all the reports is general and concerns the nature and main characteristics of the six constitutional systems and possible changes to the constitutional system, in particular since 2000, for instance with respect to constitutional review, horizontal effect, or the influence of international law. The chapters show that there are several constitutional systems with almost no change, and a few with some dynamics. The US is an example of a system with almost no change. Their 'rigid' constitution is very stable, and no significant amendments have been added or proposed. The Supreme Court has produced several relevant judgments that keep the interpretation of the Constitution up-to-date in light of technological developments. Belgium is an example of a country that used to be very static from a constitutional point of view, but has started to incorporate many changes. Its original 1831 Constitution has received several important revisions between 1970-1993 in order to transform

[1] Paul de Hert is Associate Professor in Law & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands, and Professor at Law, Science, Technology & Society (LSTS), Free University of Brussels, Belgium.
[2] Bert-Jaap Koops is Professor in Regulation & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands.
[3] Ronald Leenes is Associate Professor in Law & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands.
[4] A. Koekkoek, P. Zoontjens, et al., *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport* [Protection of fundamental rights in the digital age. A comparative study to the freedom of information and of communication and privacy in Sweden, Germany, France, Belgium, The United States of America and Canada], Tilburg, Katholieke Universiteit Brabant, 2000, 255 p.

the Unitarian state into a federal state with a plurality of legislative bodies with distinct competences, and governments. In addition, the Constitution was enriched with certain fundamental rights relevant to this report in 1993-1994 and in 2000. Moreover, the Court of Arbitration, operational in 1984 as an arbiter between the different legislative bodies, became a full Constitutional Court in 2004. Even in Belgium, however, technological developments have not been a primary trigger for constitutional amendments, and the fact that this country has been the most dynamic in constitutional change since 2000 among the countries surveyed in this report, indicates that new technologies have overall had little impact on constitutional changes over the past years.

The lack of profound constitutional changes in the countries surveyed has without doubt an institutional logic. Constitutions generally have a 'rigid' status and are not meant to be amended or altered swiftly. This seems to be even more the case in federal systems with a delicate power balance between different governments. The US, for example, where the Constitution is still in function more or less in its original form, is a case in point. The Canadian fundamental rights, as formulated in the Canadian Charter of Rights and Freedoms (Part I of the Constitution Act, 1982), are extremely difficult to amend, since the consent of the Parliament is needed together with the agreement of seven to ten provincial legislative assemblies representing more than 50 percent of the population.[5]

Another reason that none of the countries have undergone profound constitutional changes due to the emergence of new technologies, is that most constitutional rights, unlike Article 7 and 13 of the Dutch Constitution, are drafted in general terms broad enough to encompass new technologies. Freedom of expression and the right to secrecy of communications, for example, are usually worded in a technology-neutral way or, for instance in Sweden, with open endings like 'and other technical recordings' and 'or other confidential communications'. Many country reporters stress the importance of technology neutrality in constitutional protection, given the usually complex process of amending the Constitution. At the same time, as Magnusson Sjöberg warns, technology neutrality poses the risk of constitutional rights becoming very vague and thereby diluting constitutional protection. In that respect, open-ended formulations are to be preferred over overall abstract formulations.[6]

Still, the technology neutrality of most constitutional rights does not account wholly for the lack of dynamics. The chapters seem to suggest that developments in ICT and new technologies are often not looked at a from a constitutional or human-rights perspective, perhaps with the exception of general privacy issues. This seems to be especially the case for countries with older constitutions (Sweden, the US, and Belgium). These texts often tend to be smaller, more concise and less value-driven. The more pragmatic approach of Belgium contrasts heavily with the more principled approach of Germany and France, for instance in the area of biomedical technologies. It is not possible at this stage to assess these differences. One could also hold that the seemingly pragmatic approach in Belgium (with a Constitution that is very close to the Dutch) is inspired by the liberal value of freedom (e.g., to sell one's organs or to alter one's body) that dominated most nineteenth-century constitutions.

The impression nevertheless remains: technology seemingly produces little constitutional dynamics. This is not to say that the Constitution is entirely dormant. In France and Germany, for example, constitutional rights play a fairly active role in debates. In Germany, this is due to the presence of many (post-Wold War II) value-driven constitutional rights, whereas in France, this results from more procedural basic rules, such as the rule that the legislator is obliged to define the guarantees to the exercise of fundamental rights and liberties. Hesitations by the legislator to fulfil this role account for most of the constitutional case-law produced by the French Constitutional Council in the area of new technologies.

---

[5] See also H. Franken & A.K. Koekkoek, 'The Protection of Fundamental Rights in a Digital Age', in: International Academy of Comparative Law, Brussels, Bruylant, 2006, at 1162. These authors discuss national reports from Canada, Denmark, Japan and the Netherlands.

[6] On the pros and cons of technology neutrality and strategies to deal with the trade-off between sustainability of law and legal certainty, see Bert-Jaap Koops, 'Should ICT Regulation Be Technology-Neutral?', in: Koops et al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: T.M.C. Asser Press 2006, p. 77-108, available at http://papers.ssrn.com/abstract=918746.

8.2.2. The impact of international legal instruments

International human-rights treaties such as the European Convention of Human Rights (1950) and the UN International Covenant on Civil and Political Rights (1966) play an important role in the constitutional tradition of the European countries in this survey. In France, Germany, and Belgium, directly binding rights from international treaties, which are sometimes absent in the national constitutions, play a major role. The ECHR is more specific with regard to the possibilities for limitation, whereas the national constitutions tend to emphasise the existence of rights as such and usually do not go beyond the requirement that limitations have to have a legal basis.

Although not all of these European countries belong to the monist tradition (like the Netherlands), they are all eager to have cases decided in accordance with the case-law of the European Court of Human Rights. This situation stands in a striking contrast with the ethics of the US Supreme Court which, as a rule, does not refer to international treaties or case-law of foreign or international courts. Limitations to US constitutional rights do not resemble the European approach. The First Amendment with regard to freedom of expression omits every mention of the possibility to restrict this right, and the Fourth Amendment has its own particular requirements regarding limitations.

The open attitude in the European reporting countries also concerns acts and initiatives generated not by the Council of Europe, but by the European Union. Very often, ordinary legislation with regard to technological developments is enacted as a result of obligations created by regulations and directives (first pillar) or by decisions and framework decisions (third pillar). The position of the French Constitutional Council *not* to supervise national laws that implement European initiatives might be very problematic from a constitutional point of view with regard to third-pillar 'laws' enacted without co-decision power of the European Parliament and without effective judicial control by the European Court of Justice.[7] However that may be, the omnipresence of the European law-maker in areas affected by technological change likely also accounts for the lack of national constitutional activity discussed above.

8.2.3. Constitutional review

We have already observed that most reporting countries have constitutional rights with an open texture that apply in one way or another to the use of new technologies. In addition, all reporting countries have a system of constitutional review, ranging from unlimited variants, such as the US (all courts without limitation in time), to more limited variants, such as France (only the Constitutional Council before or six months after adoption of the text of the law). The chapters do not allow concluding on the eligibility of a particular form of constitutional review. From a theoretical perspective, one could argue that the continuous development of technology does not allow a court to decide on the constitutional nature of a given law in too short a period of time, but this argument is not supported in practice by the French chapter, which shows an active constitutional court unhampered by the requirement to demand constitutional review within six months of enactment of a law.

What the chapters do show, however, is the importance of having one form of constitutional review or other in the first place. The Koekkoek report already concluded that all countries have constitutional review, and that the wish to formulate the Dutch constitutional rights in a more technology-neutral way was pointless if the Dutch prohibition of constitutional review (Art. 120 Dutch Constitution) were not abolished.[8] Particularly now that Belgium has recently opted for a quite broad form of constitutional review, the Netherlands have become even more isolated on the Western constitutional scene. Despite the recommendation of the Committee for Constitutional rights in the digital era[9] to install constitutional review and a bill to modify Article 120 Dutch Constitution, constitutional review is still not possible in the Netherlands. Significantly

[7] See on this, P. De Hert, 'Division of Competencies Between National and European Levels with Regard to Justice & Home Affairs', in Apap, J. (ed.), *Justice and Home Affairs in the EU. Liberty and Security Issues after Enlargement*, Cheltenham (UK), Edward Elgar Publishing Limited, 2004, 55-102.
[8] Koekkoek et al. 2000, op. cit. n. 4, p. 234.
[9] See section 1.1.

enough, the latter bill has been pending in the First Chamber ever since October 2004.[10] If the Dutch Constitution is to be amended to update the constitutional rights in light of new technologies – which seems urgently needed for at least the technology-specific rights of Articles 7 and 13 –, constitutional review should also be introduced in the Dutch constitutional system. Otherwise, the constitutional rights at issue risk having less effect in actual practice.

Having said that, it should be noted that constitutional review does not solve all problems. It allows the courts to keep the Constitution alive and to keep a check on the legislative activities of the legislature, but it can also function as a restraint on constitutional vitality. The US chapter clearly spells out a reverse evolution with regard to judicial activism: most of the expanding interpretations of existing rights are set back by the present Court with its more conservative composition. Effective human-rights protection therefore cannot rely solely on the eagerness of judges to apply constitutional principles to the society of today. Judges also need to work on the basis of constitutional texts and principles that guide them through their work, and hence, constitutions should have truly guiding principles and should not become too abstract or too general.

8.2.4. Horizontal effect

Technology is not an instrument specifically for governments; citizens depend on the use of technology at least as much. None of the constitutions of the reporting countries, however, contain any clause relating to the horizontal effect of fundamental rights.[11] Constitutional law seems to be devised as an instrument to regulate vertical relations and to protect citizen against governmental power abuses. It is clear that similar power abuses can occur by private actors, including businesses, but this has not had a clear effect on constitutional protection at large. Most reporting countries address the issue of horizontal effect by assuming in one way or another that it is up to the legislator to convert fundamental-rights protection into specific legal norms that apply between citizens, for example in data-protection acts. On the basis of the chapters, it cannot be concluded whether the Netherlands should take specific action on this matter and open up constitutional protection in horizontal relations in a more direct way.

8.3. Privacy

8.3.1. General

The right to privacy is not explicitly mentioned in the Canadian, US, France, German, and Swedish constitutions, but it is recognised as being a part of the constitutional heritage in all the reporting countries. Belgium has, like the Netherlands, a general privacy right, albeit of a more recent date. The 1994 insertion of this right in Article 22 of the Belgian Constitution is remarkable, but in line with our observation above that constitutions in Europe tend to be sparing in possibilities to limit rights: it copies the general wordings of the right as we know it from Article 8, paragraph 1 ECHR, but omits the limitation grounds of the Article 8, paragraph 2 ECHR. When Belgium adopted the amendment, it was asserted that the right and its limits should be understood along the lines of the ECHR and its case-law. It is unclear whether such a use of supranational constitutional law at the expense of national constitutional law is beneficial. The chapters often suggest that proportionality is at the heart of constitution-related privacy debates, and it can therefore be suggested to incorporate the criterion of proportionality in future constitutional amendments.

Privacy in general is expressed in different terms and is constructed differently in the reporting countries. In Germany, where neither privacy nor data protection are mentioned in the Constitution, its source is Article 2, paragraph 1 and Article 1 (human dignity). In France, the source of privacy is not human dignity but liberty. Besides an implicit recognition by the Council in 1997, privacy was more explicitly recognised in French constitutional law in 1995-1999 as a part

[10] *Kamerstukken I* [Dutch Parliamentary Series, First Chamber] 2004/05, 28 331, A.
[11] See also H. Franken & A.K. Koekkoek, *loc. cit.*, at 1155.

of the more generic right to individual liberty (Art. 66 Constitution) and rooted in Article 2 of the 1789 Declaration of Man and the Citizen: the right to liberty as an unalienable human right.

It is hard to assess the implications of these different expressions of the right to privacy and to put into question the formulation of the right to privacy as an independent right in the ECHR and in the Dutch and Belgian constitutions. It is neverthelss clear that the choice of Article 1 of the German Constitution (hereinafter: GG) as a source for the right to privacy is important for the strong position of the right to privacy in German constitutional law. The US chapter clearly demonstrates the weakness of privacy when it is not provided for explicitly in the constitution: privacy protection is built up and broken down by judges and can therefore fluctuate significantly.

The main constitutional provision in both Canada and the US where privacy is read into, is the provision protecting against unreasonable search and seizure. The chapters suggest that this right is formulated in terms that are perhaps too physical, but the cases quoted show that the wordings are (still?) open enough for the courts to apply them in a rapidly changing world. A crucial element in both rights is that they protect people, not places. This approach has significant advantages in a technology-driven world where traditional notions of place become blurred. In a world of Ambient Intelligence, 'place' becomes something centering on people rather than on physical objects or geographical locations, since the surroundings change along with the people acting in them.[12]

Courts in Canada and the US also use the criterion of 'reasonable expectations of privacy' to determine whether certain measures are unreasonable or not. Its application, especially in the US, seems rather tricky for privacy protection in a rapidly changing world where technology permeates everyday life. As technology develops, the 'reasonable expectation of privacy' develops along with it, generally to the detriment of privacy as technology of itself tends to decrease privacy expectations.[13] An example is the *Kyllo* case in the US, where the Supreme Court used the criterion of a device being 'in general use' to determine whether or not it infringed privacy;[14] as most technology applications tend to develop from limited, sectoral use to general, public use, the related privacy expectations at one point in time will become unreasonable. Hence, using 'reasonable expectations of privacy' to face developments in technology poses the risk of a slow but sure erosion of privacy. Although the criterion is not wholly absent in the case-law of the European Court of Human rights,[15] courts and legislatures should be cautious in applying it in the field of technology law.

8.3.2. Data protection

Recently, the role of data protection proper has received constitutional recognition in the EU Charter of fundamental rights of the European Union.[16] In the Charter, a separate right to data protection has been recognised apart from a right to a private life for the individual. The right to have personal data protected is, however, not explicitly mentioned in most constitutions of the reporting states, with the exception of Sweden and the Netherlands. Nevertheless, it is recognised as part of the constitutional heritage in all the reporting countries, and the incorporation in the EU Charter may be a sign of growing recognition for data protection as a constitutional right. Whether it will further develop as an autonomous right independent from privacy[17] remains to be seen: the chapters show that in most countries, data protection is (still) largely discussed in the context of privacy.

In Germany, the right to informational self-determination is a stand-alone right next to privacy. In France and Canada, the data-protection laws have a quasi-constitutional status. The French Data Protection Act is of a general nature. In Canada, the 1983 Privacy Act was designed to protect personal data in the federal public sector, whereas the 2000 Personal Information

[12] See also *infra*, section 8.3.3.
[13] See Bert-Jaap Koops & Ronald Leenes, '"Code" and the Slow Erosion of Privacy', *Michigan Telecommunications & Technology Law Review 12* (2005) 1, pp. 115-188, http://www.mttlr.org/voltwelve/koops&leenes.pdf.
[14] See section 7.4.2.
[15] ECHR, *Halford v. United Kingdom,* judgement of 25 June 1997, § 42. See also, generally, Sjaak Nouwt, Berend R. de Vries, et al. (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, 2005.
[16] See http://europa.eu.int/comm/justice_home/unit/charte/en/charter02.html.
[17] As recommended by some scholars, e.g., P. Blok, *Het recht op privacy*, Den Haag: Boom Juridische uitgevers 2002.

Protection and Electronic Documents Act was enacted to protect personal information in the private sector; only the first has quasi-constitutional value (it will trump other laws unless the other act addresses the privacy issues), the latter has the status of ordinary legislation. The 1995 EC Data-Protection Directive largely determines data protection in the European reporting countries.[18] Whereas Canada has responded to this initiative by enacting similar legislation, the US has refrained from adopting general ordinary data-protection legislation. In US law, however, some basic principles of data protection familiar to the Canadian and European regulations are absent. As soon as one gives data away or shares them, legal protection stops. The purpose-limitation principle, i.e., the principle that data should be collected and processed according to a predefined goal or purpose, has not found firm ground in the US tradition.

All chapters show the overall importance of data-protection principles as yardsticks to measure new developments. Constitutionalization of these principles, in the line of the EU Charter, is therefore to be recommended. In that respect, it is worth mentioning that the protection of the EU Charter is more specific and more inclusive than the protection of Article 10, paragraph 3 of the Dutch Constitution. The latter does not, for instance, mention the role of the Data Protection Authority. Generally, one senses a reluctance of courts in many countries to apply data protection principles to their fullest extent. This is partly compensated by the activities of the national Data Protection Authorities.[19] In the line of the EU Charter, it can therefore be recommend to give these institutes constitutional recognition. Also, the pivotal role of the purpose-limitation principle in many debates, e.g., the debate about privacy versus security, also suggests that this principle should be part of the constitutional codification of data protection.

Culture seems to be a factor of importance with regard to data protection. Although Sweden was the first state (after the German Land Hessen) to enact a national data-protection act (1973) and although Chapter 2, Article 3 of the Instrument of Government recognises that 'every citizen shall be protected against any violation of integrity by automatic processing', Swedish constitutionalism is dominated by the notion of transparency and access to government information. Sweden therefore struggles with the main principles of the 1995 EC Data-Protection Directive and is now proposing a more US-like data-protection regulation that does not focus on prevention, but on data abuse. Given the strong influence of culture that the Swedish example chose, it can be recommended to the Dutch legislator that, when looking for inspiration for constitutional reform, he should be primarily oriented towards countries that largely share the Dutch human-rights tradition and cultural values. This is not to say that the Swedish development should be neglected: it can be questioned whether the European data-protection system, with its focus on *a priori* regulation of data collection and processing, can be upheld much longer in a world where data processing occurs in so many ways, to such an extent, and for so many purposes as it does today. Shifting the focus of legal protection to *a posteriori* regulation of data abuse might turn out to be a better strategy to protect individuals in the long run.

In all reporting countries, specific issues have determined the constitutional privacy and data-protection agenda. These overlap only partially, except with regard to the issue of balancing privacy and security, which has triggered significant debates and legislative activity in all countries. As a consequence of the September 11 attacks, many countries have adopted anti-terrorist laws, often but not always technology-related, that infringe on privacy or data-protection principles. The chapters show some resistance by the constitutional courts against overintrusive government powers, for instance in Germany, where the Constitutional Court has tied video surveillance in public places to the requirement that there are objective indications of dangerousness of the place to be monitored. Also, some cases have taken into account the proportionality criterion in dealing with proposed measures. In general, however, constitutional rights have not functioned to substantially limit or block legislative proposals to extend government powers to enhance security.

[18] See also H. Franken & A.K. Koekkoek, *loc. cit.*, at 1160.

[19] In France, for example, the Data Protection Act is acknowledged as law which guarantees a constitutional right, but the control of it by the Constitutional Council is weak. The Council only formally controls whether other laws respect the data-protection guarantees and principles established by the Data protection Act. In reality, control is therefore realised by the CNIL.

Besides 'security versus privacy', the following themes have been mentioned in the chapters: video surveillance (France, Germany, Belgium), the use of camera's on highways (France), electronic surveillance or the e-bracelet (France), biometrics (France), the processing of location data (France), the impact of antiterrorism laws on other states (Canada), privacy competences of provinces in federal states (Canada, Belgium), access to government information versus data protection (Sweden), workplace privacy (Sweden), and genetic testing (Belgium, US).

8.3.3. Inviolability of the home

The inviolability of the home is covered explicitly in most constitutions, as such in the European constitutions except the French, and via the protection against unreasonable searches in the Canadian and US systems. Although these provisions have not triggered much debate in the reporting countries with regard to technological developments, two observations can be made.

The first regards the source of these provisions. Whereas French constitutional law considers the right to have the home protected as a component of individual liberty (Art. 66), most other systems identify privacy as a basic value underlying the protection of the home. This view certainly corroborates the observation that if there is an inner and outer sphere of privacy, then the home belongs to the most inner sphere (in the German term: Kernbereich) of privacy. It is not unproblematic, however. Indeed, the right to have the home protected is much older in legal history than the right to privacy, which was only recognised as such in twentieth-century constitutions. In the nineteenth century, it was therefore held that the right to property was at the core of the values underlying the protection of the house. It is unclear from a digital-rights perspective whether the right to inviolability of the home should be conceived as an independent right based on a plurality of values (liberty, property, privacy, etc.) or as privacy specific right protecting not bricks but people, but this issue certainly merits a debate.

Second, linked to the foregoing, it appears that the current conception and wordings of the right to inviolability of the home is not technology-proof. The chapters identify problems with regular video surveillance in public places (the issues of homes is often addressed in this context), with satellite video surveillance, with RFID, with data relating to living conditions in houses (such as water and electricity bills), and with heat surveillance and other forms of scanning the home from the outside. Related to the latter, Article 13, paragraph 1 GG – 'The home is inviolable' – has been complemented with a paragraph to allow the use of wiretaps, bugs, and similar equipment in homes for fighting organised crime 'provided that alternative methods of investigating the matter would be disproportionately difficult or unproductive'. Similar issues in other countries have given rise to case-law. The Belgian Constitutional Court made it clear in 2004 that police competences to use bugs in houses needed to fulfil all the requirements of regular physical searches. In *Plant*, the Canadian Court accepted an inquiry of the police, who suspected drug cultivation, to the electric-utility company to have data on the use of electric power, because there was no trust relation between the owner and the company. The protection of the home in Section 8 Canadian Charter did not apply, because the electric reader did not reveal data on lifestyle but gave only primitive data. In *Kyllo*, the US Supreme Court saw a Fourth Amendment violation in the warrantless use of heat scans that monitored homes from the outside with devices not in general use. In *Teslin*, the Canadian court reached an opposite conclusion, arguing there was no reasonable expectation in heat that could be registered from outside homes; this technology did not reveal intimate details of lifestyle. This judgement seemingly contradicts the *Kyllo* findings but the Canadian Court left the door open to find a reasonable expection of privacy in relation to more sophisticated technology. An issue not yet addressed in case-law is to what extent the inviolability of the home protects against hacking into or searching, by means of a network connection, personal computers located in the home.

Both observations give rise to two questions that should be answered by constitutional legislators. First, are the spatial dimensions of terms such as 'home', 'search', and 'illegal trespassing' technology-proof given the new means of monitoring the home from the outside in increasingly intrusive ways?[20] Second, what exactly is being protected by the inviolability of the

[20] Cf., Bert-Jaap Koops, Hanneke van Schooten and Merel Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004, 221 p.

home: the place or the people? Property, liberty, or privacy, or a combination of all these? It is important to take a stance on this, with a view to longer-term developments like domotics, which make homes 'intelligent' and therefore more revealing of intimate life to outside snoopers, and Ambient Intelligence, where a personalised environment follows individuals as they move around, rather than that individuals have a fixed geographical basis for a private sphere in the form of their physical home. In the long run, the notion of 'home' may need to be adapted itself to denote the personalised sphere around an individual rather than a fixed, brick-and-mortar place.

8.3.4. Inviolability of the body

The body is explicitly protected, like in the Netherlands, in Canada, Sweden, and Germany. The Belgian Constitution was amended in 2000 with a provision on the rights of children that includes protection of the body of the child. Other notions protecting the body are human dignity (France, Belgium), the right to life (Belgium), privacy (US, Belgium), and the privilege against self-incrimination (US)[21]. Canadian and German constitutional case-law suggest a high level of protection accorded to the body and to data related to the body. Canadian courts apply the rule that the closer something can be tied to the individual, the higher the expectation of privacy and the protection of the body. Thus, a handbag receives more protection than a school locker or a gym bag.

The right to have the body protected has not triggered many technology-related debates. Most debates, for example, about taking DNA samples, electronic monitoring of detainees, and using biometrics, have been conducted in the context of the general right to privacy and to ordinary data-protection legislation.

The notion of protection of the body is, however, particularly relevant for biomedical issues. Here, German and French law seem to be more principled and less pragmatic in their approach than the US, Sweden, and Belgium. The former systems let the notion of human dignity play a central role in these issues. In Germany, this right is rooted in the Constitution, whereas in France, it is recognised as a 'Principe sentinelle (…) garants de principes constitutionnels' and has been firmly incorporated in the Civil Code since 1994 (*Bioethics Act*). Although it is not easy to determine whether the more principled approach of some systems or the more pragmatic approach of other systems is to be preferred, it is beyond doubt that, when endeavouring to involve constitutional rights in a more active way in biomedical developments, recognising human dignity can complement the right to protection of the body. It should, however, be noted that human dignity can be interpreted in a more or in a less liberal way. The current German interpretation, for example, prevents liberal abortion laws and gives heightened constitutional protection to the embryo, in contrast to the current European human rights framework.[22]

8.4. Communication-related rights

8.4.1. Secrecy of communications

The right to secrecy of communications is explicitly recognised at the constitutional level in Germany and Sweden. Contrary to the Netherlands, where letters, the telephone, and the telegraph are protected (Art. 13 Dutch Constitution), these countries use a sufficiently technology-neutral formulation: 'the privacy of correspondence, posts, *and telecommunications*' (Germany) and 'mail *or other confidential correspondence*, (…) telephone conversations *or other confidential communications*' (Sweden) (emphasis added). In Belgium and France, the secrecy of communications is not regulated at the constitutional level but by lower legislation; Belgium only has a constitutional protection of mail (letters). In Canada and the US, the secrecy of

[21] This may also be the case in Europe, where the European Court of Human Rights found the administering by the police of an emetic (vomitive) to the applicant, who was suspected of having swallowed drugs, a violation not only of the right to be protected against inhuman or degrading treatment (Art. 3 ECHR) but also a violation of the privilege against self-incrimination (Art. 6 para. 1 ECHR). See ECHR 11 July 2006 (*Jalloh* v. *Germany*).

[22] See also, in general, comparing a utilitarian, a human-rights, and a human-dignity approach to addressing biomedical-ethical issues and warning against a too principled 'dignitarian' approach, Han Somsen, *Regulering van humane genetica in het neo-eugenetische tijdperk*, inaugural lecture Tilburg, Nijmegen: Wolf Legal Publishers 2006.

communications has been read into the constitutional protection against unreasonable search and seizure. In Canada, e-mail falls within the scope of this protection, albeit to a lower degree than letters, but in the US, constitutional protection of e-mail is still undecided. This is similar to France, where the protection of e-mail in ordinary legislation, as interpreted by the Constitutional Council, depends on the circumstances. In these countries, encryption of e-mail is likely a sufficient condition to invoke legal protection, but it is not a necessary condition: depending on other circumstances, unencrypted e-mail can also be considered secret (compare the *Weir* case in Canada).

As with the inviolability of the home, it is relevant to consider the exact nature of what is being protected: the communication itself, the place where the communication takes place, or the medium over which the communication is transported?[23] The US approach, similar to the Canadian approach, that the Fourth Amendment protects 'people, not places' was established in the *Katz* decision on wiretapping. This remark referred, however, primarily to the place where the interception occurred: a public phone booth, arguing that people can have a reasonable expection of privacy even in a public space. This gives little guidance as to the core of the protection, but it is presumably closer related to protecting the sender or recipient of a communication and the communication itself than to protecting the medium transporting the message.

The German approach differs in this respect. The German Constitution protects the confidentiality of individual communications that depend on a third party for transmission; it principally covers all forms of mediated communication for the period of the transport. It is, hence, the channel that is protected rather than the communications as such. The French protection in ordinary legislation seems to be based on the same approach of transport protection. This 'channel' approach has advantages in that it provides more legal certainty what kind of communications are protected, namely all communications transported across media that are protected as such, like the telephone. In the 'communication' approach, the medium is neither a sufficient nor a necessary condition: protection has to be determined on a case-by-case basis, by looking at all relevant aspects of the communication itself. A channel approach is, however, more difficult to maintain as media converge. This is visible in Germany, where only individual communications are protected and not mass communications (such as broadcasts): this distinction is blurred now that communications infrastructures converge (e.g., narrowcasting on TV infrastructures, broadcasting on the Internet, and types of communication on the Internet, such as blogging or communicating in large-scale but 'closed' communities like Hyves, that are not easy to call individual or mass).

On the basis of the chapters, it can therefore not be recommended to choose either a 'communication' approach or a 'channel' approach, but it is advisable that constitutional legislators at least make an explicit and argued choice in this matter, to provide as much legal certainty as possible in this complex area.

Traffic data and data retention

A relevant issue – and a debated one in the Dutch context – is to what extent the constitutional protection of secrecy of communications covers traffic data (such as number, time, and – with mobile communications – location of a call). Generally, the reporting countries make a distinction between the content of communication and traffic data and find the latter less privacy-sensitive than the former. In Germany, traffic data fall within the scope of secrecy of communications (Art. 10 GG), but in other European countries such as Belgium and France, the protection of traffic data tends to be seen as part of the general right to privacy or data protection rather than as part

[23] This is an as yet unresolved issue in the Dutch debate on adapting Art. 13 Dutch Constitution. The Committee on Constitutional rights in the digital era and the late-1990s bill to adapt Art. 13 opted for protecting communication as such, and therefore included face-to-face communication in its protection. Academic literature, on the other hand, particularly by several scholars of the Institute for Information Law of the University of Amsterdam, advocated a 'channel' approach to protect the medium of telecommunications. See, for example, Lodewijk Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2002. For a discussion of these varying approaches, see Bert-Jaap Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002, at 277-286.

of the secrecy of communications.[24] In Canada and the US, traffic data are treated – like the content of communications – in the context of unreasonable search and seizure, but with different outcomes: whereas the US denies constitutional, Fourth Amendment, protection to traffic data outright, Canada assigns some constitutional, Section 8, protection to traffic data, albeit to a lower extent than communication content. It is relevant to note that the latter distinction, made in the Lawful Access Initiative, is controversial in Canada, where scholars argue that traffic data can be just as privacy-sensitive as the content of communications.[25]

Given these varying constitutional approaches, it is hard to recommend how exactly traffic data should be protected at the constitutional level; perhaps it is ultimately a matter of choice to be made in light of the national interpretation of rights to secrecy of communications, privacy, data protection, and protection from unreasonable search and seizure. It should also be noted that, however varying the constitutional approaches may be, the material protection for traffic data does not necessarily differ that much in practice, since it is usually provided by ordinary legislation; the US ECPA, for example, offers more protection than the Fourth Amendment *Katz* standard.

A topical issue is data retention: the requirement for telecommunications providers to store traffic data for a certain period, as a measure to combat serious crime and terrorism. Significantly enough, this measure is only taken in Europe, with the 2006 Data Retention Directive;[26] it does not feature in the US anti-terrorism PATRIOT Act, and there are no proposals considering data retention in the US or in Canada. In Europe, France and Belgium had enacted data-retention legislation before the EC Directive. In France, the application Decree bringing into force this part of the Daily Safety Act was published in 2006, and ultimately approved by the CNIL as being constitutionally acceptable, given the limitations in the law of purpose-specification and duration. In Belgium, the implementing decree for Article 126 Electronic Communication Act is still in preparation. Germany and Sweden will have to draft implementation laws. From a constitutional perspective, it is relevant to note that a motion was rejected by the German Parliament to request the government to challenge the directive at the European Court of Justice,[27] but that several groups and individuals have announced to challenge the future German transposition law before the Constitutional Court.[28]

8.4.2. Freedom of expression

The freedom of expression is an important constitutional rights in all reporting countries. The scope of the right differs, however. In France, Sweden, and the US, the right focuses on the *expression* or *communication* of thoughts and opinions. Canada has a more encompassing right, covering also the freedom to *hold* thoughts and beliefs; Belgium is similar in that it creates the freedom of expression along with the freedom of worship (Art. 19 Belgian Constitution). Germany also stipulates a constitutional right to *gather* information, to stimulate the forming of thoughts and opinions.

Despite the overall importance of the freedom of expression and the largely similar culture in the reporting countries to favour openness and public debate over censorship, each country distinguishes certain types of speech that are excluded from protection. Several of these are shared by most countries, such as – in the US terminology – 'true threats', defamation, and child pornography (in all reporting countries), and hate speech (in all except the US). Other categories are more specific for certain countries, such as political speech (banned in Canada in the 20-hour

[24] Contrary to the European Court of Human Rights, which treats traffic data as part of the right to respect for 'correspondence' in Art. 8 ECHR. See, e.g., ECtHR 2 August 1984 (*Malone* v. *United Kingdom*) and ECtHR 25 September 2001 (*P.G. & J.H.* v. *United Kingdom*).

[25] This has also been argued by scholars in the Dutch context, opposing the position taken by the Committee on Constitutional rights in the digital era in this matter. See, for example, A.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen: Wolf Legal Publishers 2006, and the annotation by Egbert Dommering under ECtHR 25 September 2001 (*P.G. & J.H.* v. *United Kingdom*), *Nederlandse Jurisprudentie* 2003, No. 670, available at http://www.ivir.nl/publicaties/dommering/ehrm25sep2001.html.

[26] European Directive 2006/24/EC of 15 March 2006 on data retention.

[27] http://dip.bundestag.de/btd/16/016/1601622.pdf.

[28] http://www.edri.org/edrigram/number4.10/dataretentionde. Outside the scope of this survey, but relevant to note in this respect, is the case brought before the Irish High Court against the Irish government by Digital Rights Ireland, challenging the Irish data-retention law and the EC Directive as unconstitutional. See http://www.digitalrights.ie/category/data-retention/.

period preceding the closing of polls, given the vastness and time zones of the country), court proceedings (which in certain cases cannot be published in Canada), and commercial speech (which has a lower standard of protection in the US). For virtual child pornography, it is noteworthy that a US law banning this was struck down as unconstutional; the constitutionality of a subsequent, more strictly formulated but functionally equivalent, criminalisation has so far not been decided in court. In the other reporting countries, several of which have also criminalised virtual child porn in the wake of the Council of Europe's Convention on Cybercrime, the constitutionality of these prohibitions does not seem to be an issue.

Particularly relevant in the context of this report is the freedom of media that express or transmit opinions. Article 25 of the Belgian Constitution is restricted to freedom of the press, which tends to be associated with the printing press, and courts are reluctant to interpret this to cover new media. The US First Amendment also only mentions freedom of the press, but this is interpreted much more broadly than in Belgium, and there is no debate that the right is formulated in too technology-specific a way. The German Constitution, in Article 5, mentions the freedom of the press and the freedom of reporting by means of broadcasts and films, thus distinguishing the press from audiovisual media. Given a similar distinction in French ordinary legislation, the Internet has triggered a restructuring of French media law, which now has a general category of 'electronic public communications', which is divided in two sub-categories: 'audiovisual communications' (subject to the Freedom of Communications Act), and 'on-line public communications' (subject to the Trust in the Digital Economy Act). Canada and Sweden have no problems with new technologies, since they use open-ended formulations: 'and other forms of communication' (Canada), 'and certain like transmissions, (…) and other technical recordings' (Sweden). Nevertheless, given the fact that Swedish constitutional protection of freedom of speech is spread across two constitutional laws, the Freedom of the Press Act and the Fundamental Law on Freedom of Expression, an inquiry is on-going to merge these laws.

The Internet raises several questions with respect to the freedom of expression. A primary topic is the categorisation of bloggers. On the one hand, they serve a purpose very similar to journalists in the printed press, by fostering the collection and spreading of information, ideas, and opinions, and therefore may well, in the longer term, turn out to be equally valuable for the public debate as traditional media, or perhaps even more valuable. On the other hand, on the Internet, everyone can start a blog and call herself a journalist. The reporting countries are tentatively coming to terms with defining bloggers. In Belgium, the criterion of 'everyone who directly contributes (…) information aimed at the public via a medium' has been formulated to trigger applicability of the Act on the protection of journalistic sources, thus in principle covering bloggers as well. In Canada, courts tend to apply a broad definition of journalism as well in relation to new media.[29] In Sweden, a more material criterion is used, namely that information be 'of importance to the public debate' in order to be protected by the freedom of expression;[30] this allows courts to assess bloggers – and other expressers of opinions on new media – on a case-by-base basis in light of the rationale of the constitutional protection. With converging media, this seems a more sustainable approach than a media-centered type of protection.

Other interesting Internet-related issues with respect to the freedom of expression are the distinction between static and interactive websites (in Sweden, only static websites fall within the scope of the Fundamental Law on Freedom of Expression), the liability for hyperlinks that link to prohibited speech (Germany: no liability because the hyperlinker aimed at faciliting people to form an opinion; France: liability because the hyperlinker had explicit knowledge of or advertised the linked content), the liabiliity of ISPs (e.g., in France and Canada), and filtering systems (e.g., in Canada). Also noteworthy are the activities in France and Belgium for the protection of minors on the Internet.

On the basis of the reports, it can be recommended that the freedom of expression – possibly strengthened by the freedom to gather information and to hold beliefs and opinions – is formulated in a sufficiently media-neutral way. An enumeration of media with an open-ended formulation – like the Canadian 'and other forms of communication' – seems particularly apt to strike a balance between legal certainty (for media that should be protected in any case) and

[29] Jason Young, communication at the 1 December 2006 workshop.
[30] Cecilia Magnusson Sjöberg, communication at the 1 December 2006 workshop.

technology neutrality (for media that may also need to be protected, perhaps through future technological developments). Given the increasing convergence of media and the rise of new ways of expression, such as blogging, that blur tradiational concepts like 'journalist', it is also useful to consider including, besides or instead of the mentioning of media, a material criterion, such as 'of importance to the public debate', that judges can use to decide whether in a concrete case a communication serves the values underlying the freedom of expression.

8.5. Other and new constitutional rights

The chapters have also mentioned several other constitutional rights as being affected by new technologies. Apart from the right to anonymity, which all reporters touched upon as it closely relates to both privacy and freedom of expression, and which we therefore treat separately in this section, no general conclusions can be drawn from the chapters, since the reporters were asked to focus on the privacy-related and communications-related rights and to go into other rights only as far as time and expertise were available.

8.5.1. Right to anonymity

Although anonymity is a topic of debate in all reporting countries, none of the countries knows a general right, constitutional or otherwise, to anonymity. It is, however, often a subsidiary or a derivative of constitutional rights. There exists, to some extent, a constitution-related right to anonymity in the context of privacy (in France), data protection (in the form of the right to informational self-determination, in Germany), the secrecy of communications (in Germany), free speech (in Canada and the US), and the right to individual liberty (which, in France, includes the freedom to come and go anonymously). This right is far from absolute: numerous exceptions are made, such as a legal obligation for bloggers to inform the hosting provider of his identity (France), a ban on equipment that obstructs caller-identification in telecommunications (Belgium), and a prohibition of anonymous political advertising (Canada). Also, discussions about revealing the identity of unknown or pseudonymous Internet users alledgedly infringing copyright or committing a content-related crime online, can be witnessed in all countries, often allowing the lifting of anonymity of the purported offender. A conclusion that can be tentatively drawn from this overview is that anonymity tends to be protected in most countries as a not unimportant value, also at the constitutional level, but that infringements of anonymity are generally easily accepted. It is therefore not possible, on the basis of the chapters, to conclude that a 'right' to anonymity exists; rather, it plays a role as a value in the context of several other constitutional rights.

8.5.2. Various

Various constitutional rights and issues are mentioned in the chapters as being potentially affected by new technologies. We give a brief overview here.

The freedom of assembly is possibly relevant for on-line demonstrations or virtual sit-ins, although a lower court in Germany declined applicability. Equal treatment (Art. 10-11 Belgian Constitution) was an issue in Belgium when the Official Journal (*Belgisch Staatsblad*) was transformed into an on-line publication, impacting the accessibility of the journal in an unconstitutional way. Computer games raise questions about the applicability of personality rights, such as portrait rights, and the freedom of art; a German lower court held that a computer game could claim the constitutional right to freedom of art, but the appeal court found that even so, a celebrity's consent was needed to use his name in the game. In the United States, a right to experimental, potentially life-saving, medication was invoked even if the drugs had not passed all tests for FDA approval. In France, the right to be forgotten is mentioned for underage offenders.

In the criminal-law context, the criminal legality principle (no crime without prior law, Art. 12 Belgian Constitution) is relevant in that it requires precise law-making, so that citizens can foresee what is punishable and how they can be investigated. In the Belgian Computer Crime Act, the formulation of 'any other technological means' was used in an attempt to make the description technology-neutral. This meets the legality principle on the face of it, since all

'technical' crimes are covered, but at the same time, foreseeability is not guaranteed with such an open ending. Also in the criminal context, in the US, the privilege against self-incrimination (Fifth Amendment) is relevant in relation to technology, for instance in the context of a power to compel citizens to hand over encryption keys. Brenner argues that such a power would violate the Fifth Amendment unless the key (or password) was reduced to tangible, recorded form. Saliently enough, such a power, which has not been enacted in the US, does exist in France and Belgium, but in these countries, the power to force suspects to decrypt has so far not been challenged as infringing the privilege against self-incrimination.[31]

In the context of electronic government, various issues spring to attention. Notable first of all is the right to access public information, which is a constitutional right in both Belgium and Sweden. Both use the term 'document'. In Belgium, this has been interpreted broadly to cover all kinds of documents regardless of the storage medium, whereas in Sweden, the term 'recording', used alongside 'written or pictorial matter' in the definition of 'document', refers to electronic documents. 'Recordings' in Sweden can be ready-made (such as e-mail messages) or compilations (like merged data bases); compilations only fall within the scope of the right to access public information if the government can make them accessible 'using routine means'. In Sweden, also the storage and deletion of official electronic documents has been called attention to in the context of the right to access public information.

Another relevant rights in the context of e-government is the right to vote. In Belgium, the law was adapted in 1998 to allow voting machines, without debate; in the US, a few civil-law suits arguing that flawed voting machines violated their right to vote were denied. E-voting has been discussed and briefly experimented with in France as an alternative to distance-voting.

Finally, a fundamental issue is raised in the Swedish chapter outside the field of human rights. The power to enact laws is constitutionally attributed to the legislator (the Riksdag, and sometimes the Government or by delegation another public authority). The increasing use of computer-assisted and computer-executed legal decisions, notably in the field of administrative law, raises the question whether and to what extent the programs used for these decisions, in which rules are embedded, should be seen as enacted laws. After all, the legal rules of law proper are not trivially translatable into technical, computer-logical rules, and hence, programming constitutes a degree of autonomous rule-making. This requires a check on the conformity of the resulting program rules with the legal rules and on the constitutional authority underlying the technical rule-making process. Related to this is the issue in Sweden of the distribution of competence between local and central authorities: if administrative decisions are largely the result of centralised information systems, the constitutional task of local governments to take indivdidual administrative decisions is at risk.

8.5.3. Conclusion

Although no general conclusions can be drawn from this brief overview, two observations can be made on the basis of the mentioning in the chapters of other rights. First, the challenges that new technologies pose to constitutional law are wide-ranging and go deeper than merely the occurrence of technology-specific formulations in constitutional provisions. The issues mentioned range from traditional, age-old constitutional rights like the freedom of assembly and the right to vote to more recent or new rights, such as the right to access government information and the right to be forgotten. What is more, they also relate to constitutional issues outside the field of human rights, such as the division of power within the government.

Second, despite the wide range of issues touched upon, the issues signaled by and large relate to developments in the near rather than the distant future, and they tend to involve ICT rather than other new technologies. This may well be caused by the background of the reporters, all of whom have a track record in the field of ICT law in particular, but it could also be an indication that biotechnology and genetics, nanotechnology, and the convergence of nano, bio, information, and cognitive sciences (NBIC) have as yet caused little discussions in relation to constitutional rights. The long-term impact of these developments on fundamental issues, for

[31] The privilege against self-incrimination is not always recognised at the constitutional level in European countries, but it is at the core of the constitutional right to a fair trial as interpreted by the European Court of Human Rights, since its first acknowledgement in ECtHR 25 February 1993 (*Funke v. France*).

example, whether cyborgs and robotics necessitate a rethinking of the concept of the bearer of constitutional ('human') rights, or the effect of NBIC on legal notions based on the concept of free will, has to our knowledge not been discussed in any detail in literature or in constitutional-policy debates.

8.6. Conclusion

New technologies challenge constitutional rights. This is particularly visible in the Dutch context, where the technology-specific formulation of several constitutional rights necessitates an adaptation of the Constitution. In the countries covered in this report, however, the text of the Constitution itself is hardly at issue. In some countries, a few adaptations have been made to bring the formulation up-to-date in light of new technologies, but no such adaptation has occurred since 2000, and no need is currently felt to adapt the Constitution – with the possible exception of the Belgian freedom of the 'press'. Generally, constitutional rights are sufficiently technology-neutral, because they are abstractly worded or use open endings (notably in Sweden), use guiding principles like a general right to personality (Germany), or are kept up-to-date by constitutional or other courts who can interpret the rights by deviating from a literal reading (US, Canada). Constitutional review is also, in varying forms, a primary feature of all constitutional systems covered in this report that explains the lack of need to modify the constitution itself.

Besides a lack of constitutional amendments, a general trend is perceptible of low constitutional dynamics. Some countries, notably Belgium, have seen a relatively vibrant constitutional activity in the past few years, with a full-blown Constitutional Court as a result, but in most countries, constitutional rights do not seem to play a key role in debates over new technologies, at least, on the face of it. A second look at many of the issues covered in this report shows that constitutional values related to privacy and freedom of communication do feed technology-related policy, legislation, and case-law, but often without reference to specific constitutional rights. In other words, constitutional values are important for technology policy and law, but in an indirect way: they often play a role in an implicit way, and through other, non-constitutional legislation that embeds and implements constitutional rights.

This is hopeful, because new technologies pose challenges, if not to Constitutions as such, to all areas of the law. In shaping the law and legal policy to face future, technology-related developments, constitutional values are urgently needed to help guide society through a process that will certainly bring radical changes, particularly since it is hard to foresee which changes exactly will be brought about by new technologies. Constitutional rights are core values that define what human beings and society are and should be. Therefore, even if constitutional rights are far from dormant, legislatures and policy-makers would do well to more explicitly refer to constitutional rights in their activities, and to create an environment in which constitutional rights can flourish and guide society along.

For the Netherlands, this means not only that several constitutional rights that are currently worded in a technology-specific way should be adapted, but equally or perhaps even more importantly, that a form of constitutional review should be created that allows constitutional rights to mature and work in practice.

References

Lodewijk Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving*, Amsterdam: Otto Cramwinckel 2002.

H. Franken & A.K. Koekkoek, 'The Protection of Fundamental Rights in a Digital Age', in: International Academy of Comparative Law, Brussels, Bruylant, 2006, pp. 1147-1164.

P. De Hert, 'Division of Competencies Between National and European Levels with Regard to Justice & Home Affairs', in APAP, J. (ed.), *Justice and Home Affairs in the EU. Liberty and Security Issues after Enlargement*, Cheltenham (UK), Edward Elgar Publishing Limited, 2004, 55-102.

A. Koekkoek, P. Zoontjens, et al., *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport* [Protection of fundamental rights in the digital age. A comparative study to the freedom of information and of communication and privacy in Sweden, Germany, France, Belgium, The United States of America and Canada], Tilburg, Katholieke Universiteit Brabant, 2000, 255 p.

Bert-Jaap Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy*, Deventer: Kluwer 2002, 335 p.

Bert-Jaap Koops, 'Should ICT Regulation Be Technology-Neutral?', in: Koops et al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: T.M.C. Asser Press 2006, p. 77-108, available at http://papers.ssrn.com/abstract=918746.

Bert-Jaap Koops, Hanneke van Schooten and Merel Prinsen, *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken*, Den Haag: Sdu 2004, 221 p.

Bert-Jaap Koops & Ronald Leenes, '"Code" and the Slow Erosion of Privacy', *Michigan Telecommunications & Technology Law Review 12* (2005) 1, pp. 115-188, http://www.mttlr.org/voltwelve/koops&leenes.pdf.

Sjaak Nouwt, Berend R. de Vries, et al. (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, T.M.C. Asser Press, 2005.

A.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen: Wolf Legal Publishers 2006.

Han Somsen, *Regulering van humane genetica in het neo-eugenetische tijdperk*, oratie Tilburg, Nijmegen: Wolf Legal Publishers 2006.

Nederlandstalige samenvatting

Grondrechten en nieuwe technologieën. Een rechtsvergelijkende studie van België, Canada, Duitsland, Frankrijk, de VS en Zweden

prof.dr. B.J. Koops, dr. R.E. Leenes & prof.dr. P. de Hert
TILT – Tilburg Institute for Law, Technology, and Society

1. Inleiding

Deze studie, geschreven in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, beschrijft ontwikkelingen in grondrechten & nieuwe technologieën in zes landen: België, Canada, Duitsland, Frankrijk, de Verenigde Staten en Zweden. Het is een vervolg op het rapport-Koekkoek uit 2000 over grondrechten in het digitale tijdperk.[1] De studie bestaat uit zes landenrapporten geschreven door deskundigen uit de desbetreffende landen en een inleiding en conclusie geschreven door TILT, Universiteit van Tilburg. Elk rapport bestudeert ontwikkelingen sinds 2000 inzake grondrechten in verband met informatie- en communicatietechnologie (ICT) en andere nieuwe technologieën, zoals biotechnologie. De aandacht is vooral gericht op de privacygerelateerde grondrechten (vgl. art. 10-13 Gw: bescherming van de persoonlijke levenssfeer en persoonsgegevens, onschendbaarheid van het lichaam en van de woning, het communicatiegeheim) en het recht op vrije meningsuiting (vgl. art. 7 Gw).

2. Algemene grondwettelijke aspecten

De constitutionele systemen in de betrokken landen hebben nauwelijks veranderingen ondergaan. De enige uitzondering is België, waar in 2004 een constitutioneel hof ontstond dat wetten aan de Grondwet kan toetsen. Voor het overige zijn er weinig veranderingen waarneembaar, in systeem noch in formulering van grondrechten. Grondwetten zijn van nature rigide en stabiel, zeker in federale systemen met een delicate bevoegdheidsverdeling tussen de diverse overheden, zoals in de VS en Canada. Een andere reden is dat de meeste grondrechten zo algemeen of technologie-neutraal zijn omschreven dat zij eenvoudig kunnen worden toegepast op nieuwe technologieën. Tegelijkertijd brengt dat wel het gevaar met zich mee dat de grondrechten vaag zijn, waardoor de rechtsbescherming dreigt te verwateren. Daarom zijn niet-limitatieve opsommingen, zoals die bijvoorbeeld in Zweden worden gebruikt, te verkiezen boven al te abstracte omschrijvingen. Maar technologie-neutraliteit is niet de enige reden voor gebrek aan dynamiek: uit de studie blijkt dat ontwikkelingen in ICT en andere technologieën vaak niet worden bekeken vanuit een grondrechtelijk perspectief. Technologie lijkt weinig constitutionele dynamiek voort te brengen.

Door de voorname rol die het Europees Verdrag voor de Rechten van de Mens (EVRM) speelt vanwege de directe werking, geldt de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM) als leidraad voor de Europese landen. Deze bijna continue wisselwerking met het supranationale niveau contrasteert met de Amerikaanse situatie, waar het Supreme Court (VS) nooit verwijst naar internationale verdragen of rechtspraak van buitenlandse of internationale rechtbanken.

De studie toont aan dat de rechtsbescherming gebaat is bij één of andere vorm van constitutionele toetsing. De mogelijkheid van grondwettelijke toetsing is belangrijk, zeker bij abstract geformuleerde grondrechten, om de bescherming die nationale grondrechten bieden ook daadwerkelijk in de praktijk tot stand te brengen en vitaal te kunnen houden. Alle onderzochte landen kennen een bepaalde, meer of minder vergaande vorm, van toetsingsrecht. Nu ook in

[1] A. Koekkoek, P. Zoontjens, et al., *Bescherming van grondrechten in het digitale tijdperk. Een rechtsvergelijkend onderzoek naar informatie- en communicatievrijheid en privacy in Zweden, Duitsland, Frankrijk, België, de Verenigde Staten en Canada. Eindrapport,* Tilburg, Katholieke Universiteit Brabant, 2000, 255 p.

België een constitutioneel hof is ingevoerd, staat Nederland met zijn verbod op toetsing aan de nationale grondrechten (art. 120 Gw) internationaal geïsoleerd.

Technologie is geen instrument specifiek voor overheden: burgers maken minstens evenveel gebruik van technologie. Geen van de onderzochte grondwettelijke systemen bevat echter een duidelijk ankerpunt met betrekking tot het horizontale effect van grondrechten. De meeste landen behandelen de kwestie van horizontale werking door op één of andere manier te veronderstellen dat de wetgever ook een zorgplicht heeft voor rechtsbescherming in relaties tussen burgers onderling, zoals bij de bescherming van persoonsgegevens; de reikwijdte van die zorgplicht kan verschillen per grondrecht. Op basis van deze studie kan geen aanbeveling worden gedaan voor Nederland om horizontale werking op een directere wijze dan momenteel te regelen.

3 Privacy

3.1. Bescherming van de persoonlijke levenssfeer

Het recht op privacy wordt behalve in België niet expliciet vermeld in de grondwet in de onderzochte landen, maar het wordt wel overal erkend als een deel van het constitutionele erfgoed. België heeft, zoals Nederland, een algemeen privacygrondrecht, maar zonder beperkingsgronden: de grenzen van het recht moeten op Europees niveau bepaald worden, via artikel 8 lid 2 EVRM.

Privacy wordt in het algemeen uitgedrukt in verschillende termen en wordt in de onderzochte landen op uiteenlopende wijze geconstitueerd. In Duitsland, waar de Grondwet privacy noch persoonsgegevensbescherming vermeldt, wordt de basis gevormd door de menselijke waardigheid en het algemene persoonlijkheidsrecht. In Frankrijk is de bron van privacy niet menselijke waardigheid maar het grondrecht op vrijheid. Ondanks deze verschillen is wel duidelijk dat een stevige grondwettelijke basis voor privacy belangrijk is: in de VS, waar het recht op privacy alleen op constitutionele rechtspraak berust, fluctueert de privacybescherming al naar gelang de keuzes van de rechters. In de meeste landen staat de proportionaliteit van overheidsmaatregelen vaak centraal bij grondwet-gerelateerde debatten over privacy; daarom valt het te overwegen ook het criterium van proportionaliteit in grondwettelijke privacybepalingen op te nemen.

De belangrijkste grondwettelijke bepaling in Canada en de VS inzake privacy is de bescherming tegen onredelijke doorzoeking en inbeslagneming. Hoewel dit recht behoorlijk fysiek is geformuleerd, bieden de bepalingen nog steeds ruimte voor de rechtspraak om deze in een veranderende en digitaliserende wereld toe te passen. Een essentieel element in beide rechtssystemen is dat zij mensen beschermen en niet plaatsen. Deze benadering heeft belangrijke voordelen in een technologiegestuurde wereld waar het traditionele begrip van plaats vervaagt. Wanneer de omgeving steeds slimmer wordt (*Ambient Intelligence*), zal het begrip 'plaats' zich meer op mensen dan op fysieke voorwerpen of geografische plaatsen richten, aangezien de omgeving zich aanpast aan de mensen die erin rondwandelen.

De rechtspraak in Canada en de VS gebruikt het criterium van een redelijke privacyverwachting om te bepalen of maatregelen al dan niet toelaatbaar zijn. Dit gebruik lijkt, vooral in de VS, nadelig uit te pakken voor de bescherming van privacy naarmate technologie meer en meer in de samenleving doordringt. De redelijke privacyverwachting ontwikkelt zich met de technologie mee, meestal in negatieve zin omdat technologie over het algemeen meer mogelijkheden biedt om door te dringen in de persoonlijke levenssfeer. Tekenend is de zaak-*Kyllo* in de VS, waarin het Supreme Court het criterium hanteerde of een privacybeperkend technisch hulpmiddel 'in algemeen gebruik' was om te bepalen of de privacy al dan niet werd geschonden door de politie; zodra het hulpmiddel breed in de maatschappij wordt gebruikt – wat bij de meeste technologietoepassingen vroeg of laat gebeurt – hebben burgers geen redelijke privacyverwachting meer en mag de politie het zonder meer gebruiken. Dit schept een risico dat privacy langzaam maar zeker wordt uitgehold door de enkele ontwikkeling van technologie. Daarom is terughoudendheid gepast bij toepassing van het criterium van redelijke privacyverwachting in het kader van technologiegerelateerde vraagstukken.

In de context van post-11 september-terrorismebestrijding staat de afweging tussen privacy en veiligheid veelal centraal in debatten en wetgeving van de onderzochte landen. De constitutionele hoven bieden daar een zekere weerstand tegen al te vergaande onderzoeksbevoegdheden van de staat, door de proportionaliteit van de maatregelen te beoordelen. In de praktijk hebben grondrechten echter niet vaak paal en perk gesteld aan ingrijpende antiterrorismemaatregelen.

3.2. Bescherming van persoonsgegevens

De bescherming van persoonsgegevens is recent grondwettelijk verankerd in het Handvest van de Grondrechten van de EU naast het recht op privacy. Ondanks het feit dat de meeste onderzochte landen geen expliciet grondwettelijk recht kennen, kan men wel stellen dat het recht op bescherming van persoonsgegevens deel uitmaakt van het grondwettelijk erfgoed van de onderzochte staten, met uitzondering van de VS; de opname ervan in het Handvest wijst ook op een groeiende erkenning ervan als grondrecht. Onduidelijk is of dit recht zich verder los van privacy zal ontwikkelen – in de meeste landen wordt het vooralsnog vooral in samenhang met privacy beschouwd.

Vanwege technologische ontwikkelingen die verwerking van persoonsgegevens faciliteren, is constitutionalisering van de beginselen van persoonsgegevensbescherming sterk aan te bevelen. Het EU-Handvest gaat daarin verder dan de Nederlandse Grondwet, door constitutionalisering enerzijds van de toezichthouders (voor Nederland het CBP), en anderzijds van het beginsel van doelbinding, aangezien dit beginsel cruciaal is in debatten over bijvoorbeeld 'privacy versus veiligheid'.

Cultuur is een belangrijke factor bij de bescherming van de persoonsgegevens. In Zweden wordt het grondwettelijke toneel gedomineerd door de uitgangspunten van rechtstreekse toegang tot overheidsgegevens en transparantie, wat problemen oplevert bij de implementatie van de EG-richtlijn bescherming persoonsgegevens. De Zweedse wetgever werkt daarom meer in de richting van de Verenigde Staten, waar het zwaartepunt van gegevensbescherming eerder ligt bij het reguleren van misbruik van gegevens dan bij preventie. In de huidige informatiesamenleving, waarin gegevensverzameling op zo'n grote schaal en voor zoveel verschillende doeleinden plaatsvindt, is op lange termijn deze verschuiving naar a posteriori-toezicht op misbruik van gegevens te overwegen, ook voor landen met andere culturele tradities.

3.3. Onschendbaarheid van de woning

In de meeste Europese landen wordt het huisrecht expliciet erkend in de Grondwet, behalve in Frankrijk. In de VS en Canada wordt de onschendbaarheid van de woning gegarandeerd via de bescherming tegen onredelijke doorzoekingen. Bij dit grondrecht spelen twee relevante probleemvelden in het licht van technologische ontwikkelingen.

Ten eerste de achtergrond van het grondrecht. In Frankrijk wordt de onschendbaarheid van de woning gezien als onderdeel van het recht op persoonlijke vrijheid; de meeste andere rechtssystemen baseren het huisrecht op de privacy. In de 19de eeuw werd de woning vooral beschermd omwille van het recht op eigendom. Vanuit het perspectief van digitale grondrechten is een relevante vraag of de onschendbaarheid van de woning eerder moet worden opgevat als een recht dat gebaseerd is op een samenstel van waarden (vrijheid, eigendom, privacy) of eerder als een specifiek privacyrecht.

Dat is vooral van belang in het licht van het tweede probleemveld: de huidige omschrijving en inhoud van het huisrecht lijkt in veel landen niet technologiebestendig. Door allerlei nieuwe mogelijkheden, zoals cameratoezicht in publieke ruimten, satellietcamera's, RFID, on-line gegevensuitwisseling met nutsdiensten (elektriciteit, water) en het scannen van huizen van buitenaf (bijvoorbeeld om warmtestraling op te vangen) ontstaan opsporingstechnieken die meer dan voorheen het huisrecht bedreigen. Sommige landen hebben in dat licht een grondwetswijziging doorgevoerd (Duitsland), terwijl andere (België, Canada, VS) in rechtspraak de onschendbaarheid van de woning trachten aan te passen aan de nieuwe technologische mogelijkheden. Een probleem dat nog niet voorwerp van rechtspraak is geweest, is de vraag of

het huisrecht ook bescherming biedt tegen hacking of netwerkzoekingen van computers die zich binnen de woning bevinden.

Deze probleemvelden doen twee vragen rijzen voor de grondwetgever. Ten eerste: is de ruimtelijke dimensie van noties als 'woning', 'huiszoeking' en 'binnentreden' bestand tegen nieuwe manieren om van buitenaf op een zeer indringende manier de woning binnenin te observeren? Ten tweede: wat wordt eigenlijk beschermd, de plaats of de persoon? Eigendom, vrijheid, privacy, of een combinatie daarvan? Op lange termijn, door ontwikkeling van domotica ('slimme' woningen) en Ambient Intelligence, zouden de concepten 'woning' en 'huisrecht' heroverwogen moeten worden, waarbij eerder de directe privé-ruimte rond een individu wordt beschermd, waar deze zich ook bevindt, dan een vaste plaats met vier muren.

3.4. Recht op lichamelijke integriteit

De lichamelijke integriteit wordt expliciet beschermd in de Canadese, Zweedse en Duitse grondwetten. In 2000 werd de Belgische grondwet gewijzigd om de lichamelijke integriteit van het kind te beschermen. Andere bepalingen die de lichamelijke integriteit beschermen betreffen menselijke waardigheid (België, Frankrijk), het recht op leven (België), privacy (België, VS) en het nemo-teneturbeginsel (VS). Canada en Duitslang waarborgen via rechtspraak een hoog beschermingsniveau voor de lichamelijke integriteit en gegevens over het lichaam.

Het recht op lichamelijke integriteit heeft in relatie tot technologie nog niet veel vragen opgeroepen. De meeste debatten worden gevoerd in de algemene context van het recht op privacy en de bescherming van persoonsgegevens. Het recht op lichamelijke integriteit is echter wel relevant bij biomedische kwesties. Daar waar het Duitse en Franse rechtssysteem principieel zijn en de menselijke waardigheid centraal stellen, is de aanpak in de VS, Zweden en België eerder pragmatisch. Hoewel niet evident is welke aanpak de voorkeur verdient, is wel duidelijk dat grondrechtelijke erkenning van de menselijke waardigheid de grondwettelijke bescherming van de lichamelijke integriteit kan aanvullen bij biotechnologische ontwikkelingen. Daarbij moet wel aangetekend worden dat het begrip 'menselijke waardigheid' meer of minder liberaal kan worden uitgelegd. In Duitsland wordt bijvoorbeeld het embryo beschermd en abortus beperkt door de grondwet, in tegenstelling tot het hedendaagse Europese mensenrechtenkader.

4. Communicatiegrondrechten

4.1. Vertrouwelijkheid van communicatie

De Duitse en Zweedse grondwet kennen – in tegenstelling tot het Nederlandse brief-, telefoon- en telegraafgeheim (art. 13 Gw) – een voldoende technologieneutraal (tele)communicatiegeheim; Zweden gebruikt daarbij een niet-limitatieve opsomming: '… en andere vertrouwelijke communicatie'. In België en Frankrijk is het communicatiegeheim alleen in lagere wetgeving geregeld, behoudens het briefgeheim in de Belgische grondwet. In Canada en de VS volgt het communicatiegeheim uit de bescherming tegen onredelijke doorzoeking en inbeslagneming. E-mail valt in Canada onder deze bescherming, zij het in mindere mate dan traditionele post. In de VS en Frankrijk hangt de bescherming van e-mail af van de omstandigheden. Versleuteling van berichten is hierbij een voldoende, maar niet noodzakelijke, voorwaarde voor bescherming.

Een belangrijke vraag is wat in dit licht bescherming geniet: de communicatie zelf, de locatie waar de communicatie plaatsvindt, of het medium waarlangs het communicatietransport plaatsvindt. In de VS wordt het Vierde Amendement op basis van de zaak-*Katz* (een aftapzaak) geacht bescherming te bieden aan personen, niet aan plaatsen; hetzelfde geldt voor Canada. Dit criterium komt dichter in de buurt bij bescherming van de communicatie zelf dan bij bescherming van het communicatiemedium. Duitsland en Frankrijk hebben juist gekozen voor grondwettelijke bescherming van middellijke communicatie via derden, waarbij communicatie gedurende het transport over een bepaald medium is beschermd. Het voordeel van deze benadering is rechtszekerheid: alle communicatie via het beschermde kanaal valt eronder, zodat geen casuïstische beoordeling nodig is van alle factoren rond de communicatie om te weten of een bericht wordt beschermd. Mediaconvergentie bemoeilijkt echter deze benadering, nu over allerlei

media zowel individuele communicatie als publieke communicatie (omroep) wordt getransporteerd. Op basis van deze studie valt geen duidelijke voorkeur uit te spreken voor mediumbescherming of communicatiebescherming. Wel is aan te bevelen dat de grondwetgever een duidelijke, gemotiveerde keuze maken tussen beide regimes, waarbij rechtszekerheid voorop staat.

Verkeersgegevens en dataretentie

Een relevant vraagstuk is of de communicatiebescherming zich uitstrekt over verkeersgegevens (zoals aansluitnummer, tijd, duur en locatie bij mobiele communicatie). Alle landen maken onderscheid tussen de inhoud van communicatie en de verkeersgegevens, en zij beschouwen verkeersgegevens als minder privacygevoelig. Alleen in Duitsland vallen verkeersgegevens onder het ruime grondwettelijke telecommunicatiegeheim; in andere Europese landen worden zij doorgaans beschermd door het algemene privacyrecht of de bescherming van persoonsgegevens. In Canada en de VS worden verkeersgegevens beschouwd in de context van onredelijke doorzoeking en inbeslagneming; in de VS worden zij hierdoor niet beschermd, in Canada wel, zij het minder dan de inhoud van communicatie. De houdbaarheid van dit onderscheid tussen inhoud en verkeersgegevens is omstreden in Canada, waar deskundigen betogen dat verkeersgegevens net zo privacygevoelig kunnen zijn als de inhoud van communicatie. De verschillen in constitutionele benaderingen maken overigens voor de feitelijke bescherming van verkeersgegevens niet per se uit, omdat lagere wetgeving hierbij veelal maatgevend is.

Verkeersgegevens zijn actueel nu aanbieders van telecommunicatie op basis van de Europese dataretentierichtlijn (2006/24/EG) een bewaarplicht voor dergelijke gegevens krijgen. Opvallend is dat in de Amerikaanse en Canadese wetgeving en debatten rond terrorismebestrijding dataretentie niet aan de orde is. In Europa bestond dataretentiewetgeving reeds in Frankrijk; de toezichthouder voor bescherming van persoonsgegevens achtte deze wetgeving verenigbaar met de grondwet vanwege de duidelijke doelbinding en de beperkte duur van de bewaring. België is gevorderd met de implementatie van de richtlijn, Duitsland en Zweden nog niet. Vanuit grondrechtelijk perspectief is vermeldenswaard dat een Duitse parlementaire motie om de regering te bewegen de grondwettelijkheid van de richtlijn aan te vechten bij het Europese Hof van Justitie geen meerderheid haalde, maar dat verschillende organisaties en individuen reeds hebben aangekondigd de komende Duitse implementatiewetgeving aan te vechten bij het Duitse constitutionele hof.

Op basis van de studie kan geen voorkeur worden uitgesproken voor het onderbrengen van verkeersgegevens bij het communicatiegeheim of bij het algemene recht op privacy of de bescherming van persoonsgegevens. Duidelijk is wel dat verkeersgegevens als een belangrijke categorie gegevens worden beschouwd die grondwettelijke bescherming genieten. In dat licht is aan te bevelen terughoudend te zijn bij dataretentieverplichtingen.

4.2. Vrijheid van meningsuiting

De vrijheid van meningsuiting is een belangrijk grondrecht in alle landen, zij het met verschillende invullingen. De *uiting* van gedachten en meningen staat centraal in Frankrijk, Zweden en de VS, terwijl in Canada ook het *koesteren* van gedachten en overtuigingen is inbegrepen. België plaatst de vrijheid van meningsuiting naast de vrijheid van godsdienstbeoefening. Duitsland kent verder een *garingsrecht* voor informatie om gedachten- en meningsvorming te bevorderen.

Hoewel in alle onderzochte landen openheid en publiek debat prevaleren boven censuur, worden wel bepaalde vormen van meningsuiting uitgesloten van bescherming, zoals bedreigingen, laster, kinderporno, en racisme. Er zijn ook meer specifieke beperkingen, in Canada bijvoorbeeld voor politieke uitingen tijdens verkiezingen (vanwege de vele tijdzones) en voor sommige rechterlijke uitspraken, en in de VS voor reclame-uitingen. Interessant is dat een verbod op virtuele kinderporno in de VS ongrondwettig werd verklaard door het Supreme Court vanwege schending van de vrije meningsuiting; een opvolgend, strikter geformuleerd verbod van gelijke strekking is nog niet aangevochten. De grondwettelijkheid van een verbod op virtuele kinderporno lijkt geen punt van discussie in de Europese landen.

Een relevant aandachtspunt is welke media ter openbaring of verspreiding van uitingen bescherming genieten. Het Belgische grondrecht is gericht op de traditionele drukpers; de rechtspraak is terughoudend om dit te verruimen met nieuwe media. Het grondrecht in de VS ziet eveneens op persvrijheid, maar dit begrip wordt ruim opgevat en er is geen discussie over de technologiespecifieke formulering. Frankrijk heeft de wetgeving aangepast om een onderverdeling te maken van soorten elektronische publieke communicatie: 'audiovisuele' communicatie en 'on-line publieke' communicatie vallen onder verschillende reguleringsregimes. Canada en Zweden kunnen technische ontwikkelingen makkelijker opvangen doordat zij een niet-limitatieve opsomming van media hanteren bij het recht op vrije meningsuiting.

Internetontwikkelingen leveren nieuwe vragen op rond de vrijheid van meningsuiting, bijvoorbeeld voor de positie van bloggers. Deze hebben een met traditionele journalisten vergelijkbare functie in de garing, analyse en openbaarmaking van informatie, gedachten en overtuigingen en kunnen hierdoor op termijn een even essentiële functie vervullen in het publieke debat als de klassieke pers. Daartegenover staat dat iedereen een weblog kan beginnen en zichzelf journalist kan noemen. De onderzochte landen proberen inmiddels voorzichtig de positie van bloggers te bepalen. In België en Canada worden ruime definities gehanteerd van journalistiek, waardoor ook bloggers hieronder kunnen vallen. Zweden hanteert echter een meer materieel criterium, namelijk dat de geüite informatie van belang moet zijn voor het publieke debat om grondwettelijke bescherming te kunnen genieten. Dit betekent dat rechtspraak blogs en andere nieuwe media-uitingen individueel moet beoordelen in het licht van de strekking van het grondrecht, wat de rechtszekerheid niet ten goede komt. In het licht van mediaconvergentie is een dergelijke materiële benadering echter wel duurzamer dan een media-specifieke benadering van vrije meningsuiting.

De conclusie die voortvloeit uit dit overzicht is dat het recht op vrije meningsuiting – mogelijk ondersteund door een garingsrecht en een recht meningen te koesteren – voldoende media-neutraal moet worden geformuleerd, bijvoorbeeld door een niet-limitatieve opsomming van media ('… en andere vormen van communicatie'). Vanwege mediaconvergentie en nieuwe vormen van meningsuiting, zoals bloggen, die traditionele begrippen als 'journalist' doen vervagen, valt ook te overwegen om, naast of in plaats van het opsommen van media, een materieel criterium te hanteren, zoals 'in het belang van het publieke debat', dat rechters in concrete gevallen kunnen gebruiken om te bepalen of een uiting de belangen dient die het recht op vrije meningsuiting beoogt te beschermen.

5. Andere grondrechten

Deze studie is met name gericht op de privacy- en communicatiegerelateerde grondrechten. De landenrapporteurs hebben daarnaast als aanvulling aandacht besteed aan andere grondrechtelijke thema's. Een belangrijk onderwerp van discussie in de onderzochte landen is anonimiteit. Hoewel er nergens een grondrecht of ander algemeen recht op anonimiteit bestaat, wordt het in veel landen wel beschouwd als hulpmiddel of afgeleide van andere grondrechten, zoals privacy, persoonsgegevensbescherming, communicatiegeheim, vrije meningsuiting en, in Frankrijk, het individuele vrijheidsrecht. In de meeste landen wordt anonimiteit in dat licht beschermd als een niet-onbelangrijke waarde, ook op grondrechtelijk niveau, maar beperkingen van anonimiteit worden over het algemeen makkelijk geaccepteerd. Op basis hiervan kan niet worden geconcludeerd dat er een 'recht op anonimiteit' bestaat in de onderzochte landen, maar wel dat het een rol speelt als waarde binnen de context van diverse grondrechten.

Naast anonimiteit zijn de nodige andere grondwettelijke thema's aangestipt in de studie. Daarbij valt op dat de discussie breder is en niet alleen de precieze – al dan niet technologiespecifieke – formulering van grondrechten in de grondwet betreft. De implicaties van technologie strekken van traditionele rechten als het recht tot betoging en het kiesrecht tot nieuwe rechten als de toegang tot overheidsinformatie. Bovendien gaat de discussie niet alleen over grondrechten, maar ook over constitutionele thema's als de scheiding van machten. Wat verder opvalt bij de discussies is dat deze vooral technologische ontwikkelingen op de korte termijn betreffen, vaak op het vlak van ICT. Andere nieuwe technologieën en langetermijnontwikkelingen, zoals de convergentie van nano-, bio-, informatie- en

cognitietechnologie (NBIC), lijken in de onderzochte landen vooralsnog geen onderwerp van debat te zijn geweest.

6. Conclusie

Nieuwe technologieën vormen een uitdaging voor de grondrechten. Dat is zeker zichtbaar in de Nederlandse context, waar de technologiespecifieke formulering van diverse grondrechten tot aanpassing van de Grondwet noopt. In de landen die onderzocht zijn in deze studie, speelt de tekst van de grondwet echter nauwelijks een rol. Voorzover aanpassing van formuleringen nodig was, gebeurde dit al voor 2000, en momenteel vindt er geen discussie plaats over aanpassing. De grondrechten zijn meestal voldoende technologie-neutraal geformuleerd – in abstracte termen of met niet-limitatieve opsommingen –, men kan uit de voeten met richtinggevende beginselen zoals het algemene persoonlijkheidsrecht in Duitsland, en de grondwet wordt geactualiseerd en levend gehouden door de rechtspraak van constitutionele en andere rechters. Het toetsingsrecht is, in verschillende verschijningsvormen, eveneens een centraal element in de onderzochte constitutionele systemen, waardoor er geen noodzaak is tot aanpassing van de grondwet zelf.

Naast een afwezigheid van grondwetsaanpassingen valt ook een tendens op te merken van geringe constitutionele dynamiek. In de meeste landen speelt de grondwet op het eerste gezicht als zodanig maar een kleine rol in debatten over nieuwe technologie. Bij nadere beschouwing blijkt echter dat constitutionele waarden gerelateerd aan privacy en communicatievrijheid wel degelijk een belangrijke rol spelen bij technologiegerelateerd beleid, wetgeving en rechtspraak, maar zonder specifieke verwijzing naar de grondwet.

Dat is een hoopvolle constatering, nu technologie op allerlei terreinen het recht en de wetgeving uitdaagt, waarbij het moeilijk te voorzien is in welke richtingen de maatschappij zal veranderen door nieuwe technologieën. Grondrechten zijn kernwaarden die aanduiden wat mens en maatschappij zijn en zouden moeten zijn, en zij vormen daarom een belangrijk ankerpunt voor de wetgever om technologiegerelateerde maatschappelijke veranderingen in goede banen te leiden. De wetgever en beleidsmakers hebben daarom ook een verantwoordelijkheid om niet alleen grondrechten in acht te nemen bij hun activiteiten, maar ook om een klimaat te scheppen waarin grondrechten kunnen opbloeien en richting kunnen geven aan de maatschappij.

Voor Nederland betekent dit dat de Grondwet op diverse punten aangepast zou moeten worden, onder andere bij de technologiespecifieke formuleringen, om de grondrechten bij de tijd te brengen en duurzaam te maken in het licht van technologische ontwikkelingen. Daarnaast toont deze studie aan dat enige vorm van toetsingsrecht van wezenlijk belang is om grondrechten te doen rijpen en in de praktijk tot leven te brengen; daarom is ook een bezinning op het toetsingverbod van art. 120 Gw dringend gewenst.

Appendix. Participants to the Workshop

Workshop Constitutional Rights and New Technologies, The Hague, 1 December 2006

Lydia Bremmer	Dutch Ministry of Internal Affairs and Kingdom Relations
Henk-Martijn Breunese	Dutch Ministry of Internal Affairs and Kingdom Relations
Fanny Coudert	Catholic University of Leuven
Paul De Hert	Tilburg University
Harke Heida	Dutch Ministry of Internal Affairs and Kingdom Relations
Heleen Janssen	Dutch Ministry of Internal Affairs and Kingdom Relations
Els Kindt	Catholic University of Leuven
Bert-Jaap Koops	Tilburg University
Ronald Leenes	Tilburg University
Cecilia Magnusson Sjöberg	Stockholm University
Anselm Rodenhausen	University of Münster
Jon Schilder	Dutch Ministry of Internal Affairs and Kingdom Relations
Thomas Veling	Dutch Ministry of Internal Affairs and Kingdom Relations
Jason Young	Deeth Williams Wall, Toronto