Constitutional Rights and Technologies in the Netherlands

Groothuis, M.M.; Koops, E.J.; Leenes R.E., Koops E.J.

Chapter 6
CONSTITUTIONAL RIGHTS AND NEW TECHNOLOGIES IN THE NETHERLANDS

Bert-Jaap Koops and Marga Groothuis*

6.1 INTRODUCTION

This chapter intends to give an overview of the legislation and case law on fundamental rights in relation to new technologies, in particular ICT, in the Netherlands. The Dutch Constitution [*Grondwet*, hereinafter: Gw] provides in Chapter 1 a list of fundamental rights.[1] In recent years, much attention has been paid to applying these fundamental rights in a digital environment such as the Internet. According to the Cabinet, the Dutch Constitution needs to be modified in order to adapt to the new circumstances of the information age. The Cabinet has announced several Bills of Amendment to the Constitution in order to reach this goal, although these have not yet been submitted to Parliament.

The information age does not only pose challenges to the legislator, but also to the judiciary. Several fundamental rights, as laid down in the Dutch Constitution, contain technology-specific terms: they refer to specific technologies or means of communication. Article 13, for example, protects the secrecy of letters, telephone, and telegraph. It is not clear from the wording of this provision whether it also applies to electronic mail. Similar questions arise with regard to the freedom of expression and other fundamental rights in Chapter 1.

A complication for the development of case law is that the Dutch Constitution contains a prohibition on constitutional review (Art. 120) and that there is no Constitutional Court. The Dutch Supreme Court [*Hoge Raad*] and other courts have,

* Bert-Jaap Koops is Professor in Regulation & Technology at TILT, the Tilburg Institute for Law, Technology, and Society, of Tilburg University, the Netherlands; Marga Groothuis is Assistant Professor at the Department for Constitutional and Administrative Law of Leiden University, the Netherlands.

[1] All references in this Chapter are to articles in the Constitution. An English translation of the Dutch Constitution, published by the Dutch Ministry of the Interior and Kingdom Relations, is available at <http://www.minbzk.nl/contents/pages/6156/grondwet_UK_6-02.pdf>. All citations of the Constitution are taken from this version, unless stated otherwise.

R.E. Leenes, B.J. Koops and P. De Hert (Eds.), Constitutional Rights and New Technologies

however, published some important cases relating to the protection of digital fundamental rights in recent years, which will be analysed below.

This chapter addresses five fundamental rights which are pillars for the rule of law and democracy in the information age: the freedom of expression, the right to respect for private life and data protection, the inviolability of the home, the inviolability of the body, and the secrecy of communications. Furthermore, it gives a brief overview of other developments which affect fundamental digital rights of citizens, such as electronic voting and a Bill for a new constitutional right on access to public information.

6.2 History of digital constitutional rights[2]

6.2.1 Characteristics of the Constitution

The Dutch Constitution, which dates from 1848 and which has been amended several times since, is considered 'sober'. Chapter 1 contains a catalogue of fundamental rights. The following seven chapters regulate the position of the Government,[3] Parliament, Council of State, Court of Audit and Ombudsman, the legislative process, the position of the judiciary, the position of decentralised bodies, and the procedure for amending the Constitution.

As indicated above, the Dutch Constitution contains a prohibition on constitutional review of Acts of Parliament by the judiciary (Art. 120).[4] A second distinguishing feature of Dutch constitutional law is the direct effect of clauses of international treaties and decisions of international relations (Art. 93 and 94): if these clauses and decisions are through their content 'binding on citizens', they have effect within the national legal order and can be directly invoked by citizens in courts. A third characteristic of the Constitution is the 'horizontal effect' of fundamental rights: these rights do not only apply in the relationship between the state and citizens (the 'vertical effect') but also – indirectly – in relationships between citizens. The concept of horizontal effect of fundamental rights has not been codified in the Constitution, but has been developed in case law: judges weigh the interest of respect for fundamental rights against other interests when interpreting rules of civil law. It should be noted that the scope of horizontal effect may differ depending on the nature of the fundamental right at issue.

The procedure for amending the Constitution is laid down in Articles 137-139. A Bill of Amendment can be proposed by the Government or by the Second Chamber of Parliament (Art. 82). For a Bill of Amendment to be adopted, two rounds of

[2] A good overview in English is provided by Leenknegt 2002.

[3] The Government is composed by the King (who has a largely ceremonial role) and the Ministers. The Cabinet (a term which will be used below) is composed by the Ministers and the deputy Ministers.

[4] Courts may, however, review the constitutionality of lower regulations, e.g., municipal rules.

votes are prescribed. In the first round, the approval by a (regular) majority of the members of the Second and the First Chamber of Parliament is required. In the second round, which starts after re-election of the Second Chamber, an approval by two thirds of the members of both Chambers is prescribed.

6.2.2 Digital constitutional rights

The political debate on digital constitutional rights in the Netherlands basically started in 1998, when the First Chamber of Parliament expressed its disagreement with a Bill to amend Article 13 of the Constitution, the provision on the right to secrecy of letters, telephone, and telegraph. The main reason for the First Chamber to disagree with the Bill was that in its view, it had been prepared under too much time-pressure without sufficient reflection.[5]

In reaction to the opposition in the First Chamber against the proposed amendment to Article 13, in 1999, the Cabinet decided to establish a Committee on Fundamental Rights in the Digital Age (hereinafter: CFRDA), a committee of experts in the field of constitutional law and information technology law.[6] The CFRDA was asked to write an advisory report on the protection of fundamental digital rights and more specifically on the question whether Amendments to the Constitution were necessary in reaction to the development of the information society. To help the CFRDA, a comparative study was commissioned to survey developments in six foreign countries, the results of which were used in drafting proposals for the Dutch situation.[7]

In 2000, the CFRDA offered its report 'Fundamental Rights in the Digital Age' to the Cabinet.[8] The Committee advised the Cabinet to draft four Bills of Amendments to the Constitution: amendments to the provisions on the freedom of expression (Art. 7), the right to respect for private life (Art. 10), the right to private correspondence (Art. 13), and a proposal for a new provision on the right to access public information.[9] According to the Committee, the Articles 7, 10, and 13 of the Constitution were, in their present form, too technology-specific, i.e., they applied to particular technologies and means of communication, such as the press [*drukpers*], letter [*brief*], telephone and telegraph [*telefoon* and *telegraaf*] and could not, or

---

[5] *Kamerstukken II* [Parliamentary Proceedings, Second Chamber] 1998/99, 25 443, No. 40, p. 1-8. See *below* 6.5.1 about this Bill of Amendment and the debate in the Second and First Chamber of Parliament.

[6] *Staatsblad* [Dutch Official Journal] 1999, 101. The members of the CFDRA were H. Franken (President of the Committee), J. Arnbak, M.A.P. Bovens, J.P.H. Donner, A.M. Gerritsma, H.R.B.M. Kummeling, J.E.J. Prins, H.J. de Ru, I.Th.M. Snellen, and P. Vogelenzang.

[7] Koekkoek, et al. 2000.

[8] CFRDA 2000.

[9] Press report of the Ministry of the Interior and Kingdom Relations, 17 August 2001 <http://www.minbzk.nl/actueel?ActItmIdt=2743>. The (withdrawn) Bills were published in 2004 and are available at <http://www.minbzk.nl/actueel?ActItmIdt=12755>.

only by means of an extensive interpretation, be applied to modern means of communication, such as the Internet and e-mail. The new provisions proposed by the CFDRA were all formulated in a 'technology-neutral' form.

The reactions in the literature to the report of the CFRDA were diverse.[10] Although most authors agreed with the analysis of the CFRDA that amendments to the Constitution were necessary in order to protect fundamental rights in the new information age, there was also criticism on elements of the proposals of the Committee, in particular the proposals for the new Articles 10 and 13. A major theme in the debates on the proposals of the CFRDA was whether the proposed provisions of the Constitution were too abstract and should be formulated in a more concrete – and thus more technology-specific – way.[11]

In August 2001, the Cabinet announced that it had, in accordance with the advice of the CFRDA, drafted four Bills of Amendments to the Constitution, proposing changes to the provisions on the freedom of expression (Art. 7), the right to respect for private life (Art. 10), the right to private correspondence (Art. 13), and a proposal for a new provision on the right to access public information.[12] The essence of the Bills was that the amended provisions of the Constitution would be 'applicable in the digital era': they would apply in a digital environment such as the Internet as well as in a non-digital environment.

Before sending the Bills to Parliament, the Cabinet asked the advice of the Council of State (as the Constitution prescribes). In its advice, which was sent to the Cabinet in January 2002 but only published nearly three years later, the Council of State was negative about the proposals of the Cabinet.[13] Although the Council agreed with the Cabinet that amendments to the Constitution were necessary in order to adjust the Constitution to 'new developments in the modern society', it strongly advised the Cabinet not to submit the Bills to Parliament. The essence of the criticism of the Council of State was that it was not clear how the proposed amendments to the Constitution related to developments in international law, in particular the case law under the European Convention on Human Rights and fundamental freedoms.

In reaction to the negative advice of the Council of State, the Cabinet decided not to send the Bills to Parliament. In November 2004, it announced that it withdrew the Bills and would draft new Bills which would take into account recent

---

[10] Asscher 2000; Dommering 2000; Kuitenbrouwer 2000; De Meij 2000, pp. 1-18; Nouwt, et al. 2000; Winter 2001; Asscher 2002, pp. 67-74 and 100-104.

[11] For a general discussion of technology neutrality, including an analysis of the constitutional right to secrecy of communications, see Koops 2006.

[12] Press report of the Ministry of the Interior and Kingdom Relations, 17 August 2001 <http://www.minbzk.nl/actueel?ActItmIdt=2743>. The Bills were published in 2004 and are available at <http://www.minbzk.nl/actueel?ActItmIdt=12755>.

[13] Advisory reports of the Council of State, Nos.W01.01.0465/I, W01.01.0463/I and No.W01.01.0467/I, available at <http://www.minbzk.nl/actueel?ActItmIdt=12755>.

developments in international law.[14] In December 2005, the Cabinet re-affirmed, in reaction to questions from Parliament, its intention to submit the announced new Bills to Parliament.[15] In 2006, the Ministry of the Interior and Kingdom Relations commissioned a new comparative study on constitutional rights and new technologies, which was sent to Parliament in March 2007, and the Minister announced the aspiration to be able to present Bills to amend the Constitution in the course of 2007.[16] As of June 2007, no Bills have yet been published.

6.3 CHANGES IN THE CONSTITUTIONAL SYSTEM

A remarkable development in 2002 was the submission to Parliament of a Bill which proposes to modify Article 120 of the Constitution, the prohibition of constitutional review.[17] This Bill was initiated by a Member of the Second Chamber, Halsema, and adopted by this Chamber in October 2004. Ever since then, the Bill has been pending in the First Chamber.[18] Should this Bill become an Act, all courts in the Netherlands would be entitled to review the constitutionality of acts of parliament.[19]

The comparative study of 2000 concluded already that all countries studied have some form of 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 were not abolished.[20] The Netherlands are thus fairly isolated on the Western constitutional scene when it comes to the lack of constitutional review. Despite the recommendations of the CFRDA in 2000 and the 'National Convention' in 2006[21] to install constitutional review, this still has not been

[14] Letter of the Minister of the Interior and Kingdom Relations of 1 November 2004, Ref. No. 2004-0000018207, available at <http://www.minbzk.nl/contents/pages/10386/artikel7gwvrijheidvanmeningsuiting.pdf>.

[15] Letter of the Minister of the Interior and Kingdom Relations of 28 November 2005, *Kamerstukken II* 2005/06, 30 300 VII, nr. 35, p. 1-2. In this letter, the Cabinet referred to recent developments in international law, in particular the adoption of the *Declaration on human rights and the rule of law in the Information Society* by the Committee of Ministers of the Council of Europe on 11 May 2005, COM(2005)56 final, available via <http://www.coe.int>.

[16] *Kamerstukken II* 2006/07, 27 460, No. 5. The report – Koops, et al. 2007 – updates the 2000 comparative study of Koekkoek, et al. 2000; it also forms the basis of the present book.

[17] *Kamerstukken II* 2001/02, 28 331, Nos. 1-3.

[18] *Kamerstukken I* 2004/05, 28 331, No. B.

[19] The constitutional review is, however, limited to the fundamental rights articulated in Arts. 1, 2(3-4), 3-9, 10(1), 11-17, 18(1), 19(3), 23(2-3, 5-7), as well as to a few other articles of the Constitution (54, 56, 99, 113(3), 114, 121, and 129(1)).

[20] Koekkoek, et al. 2000, p. 234.

[21] CFRDA 2000, p. 49 (note that one committee member, Donner, who later became Minister of Justice, dissented). Nationale Conventie ['National Convention', a Committee of Experts], *Hart voor de Publieke Zaak. Aanbevelingen van de Nationale Conventie voor de 21 eeuw* [Heart for Public Matters. Recommendations of the National Convention for the 21st Century], offered to the Cabinet in September 2006, at pp. 44-47, available at <http://www.onzedemocratie.nl>. See also Leenknegt 2002, p. 344.

made possible in the Netherlands. We agree with the CFRDA that introducing constitutional review is an important supplement to amending the Constitution in relation to new technologies, in particular if the fundamental rights are formulated in a more technology-neutral way. In that light, it is to be recommended that the Halsema Bill be adopted.

In February 2007, the new Cabinet decided to install an Advisory Committee [*Staatscommissie*], which was asked to investigate whether amendments to the Constitution are necessary with regard to three other issues:

1. the question whether a preamble should be added to the Constitution,
2. the transparency of the Constitution for citizens, and
3. the relationship between the constitutional rights laid down in the Constitution and the constitutional rights laid down in international treaties on human rights, such as the right to a fair trial and the right to life.[22]

At the time of writing, June 2007, it was not yet known when the Committee is expected to publish its findings and whether the Committee will also advice on issues related to digital constitutional rights.

6.4 PRIVACY-RELATED RIGHTS

6.4.1 **Privacy and data protection**

Privacy in the Netherlands is protected in the Constitution in several ways. There is a general right to privacy (Art. 10 para. 1) and four specific privacy-related rights: data protection (Art. 10 paras. 2-3), bodily integrity (Art. 11), inviolability of the home (Art. 12), and secrecy of communications (Art. 13). The latter two have been part of the Constitution since the first half of the 19th century; the former, including the general right to privacy, were introduced in 1983. In this section, we will discuss the general right to privacy and the right to data protection. The other rights are treated in the subsequent sections.

The right to privacy

Privacy in the Dutch Constitution was for a long time restricted to the inviolability of the home and the secrecy of letters. When a new Constitution was prepared in the 1960s, these two rights were at first still considered adequate to protect privacy. However, given the population growth and the developments in technology, an advisory committee recommended introducing a general right to privacy, not a defen-

[22] *Regeerakkoord* [Coalition Agreement], 7 February 2007, p. 34, available at <http://www.kabinetsformatie20062007.nl/>.

sive right against the government, but an instruction norm to the government to pass legislation to protect privacy both in horizontal and in vertical relationships. In the mid-1970s, however, privacy was considered an essential condition for human life and one of the core principles of the rule of law, and hence, a full-blown right to privacy was considered necessary.[23] As a result, Article 10 paragraph 1 Gw reads:

> 'Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament.'

'Privacy' is called 'personal sphere' [*persoonlijke levenssfeer*] in this provision. What exactly this means, is left to jurisprudence to decide. The parliamentary proceedings on this constitutional right give some insight into the meaning, but by and large, Dutch case law often does not go into Article 10 Gw but rather refers to Article 8 ECHR to determine the scope of the right to privacy. Apart from the parts of the personal sphere that are protected by other specific rights – personal data, home, body, communications – the right to privacy largely boils down to 'intimate life', i.e., intimate activities and intimate contacts.[24] A key factor mentioned by the legislator is 'the nature and extent of the intimacy of that which is observed or published'.[25] Outside of the intimate sphere, there is not much occasion to assume privacy; activities in public, for example, do not touch upon privacy, even though observation in public has occasionally been judged to infringe the personal sphere (but this related to intimate life, i.e., to see whether a woman was living together with someone). Criminal-investigation methods unrelated to personal data, home, body, or communication are sometimes judged to infringe privacy to a small extent (for which the general task description of the police in Article 2 Police Act [*Politiewet*] provides sufficient legal ground), but there is no material difference with methods that are not considered to infringe privacy at all, such as dumpster diving or looking into a car. As a result, as Peter Blok has argued, 'personal sphere' should be interpreted as by and large restricted to the home, body, communications, and intimate life.[26]

Article 10, paragraph 1 is generally accepted as an important constitutional right, which is often referred to in academic literature as a source of the right to privacy. At the same time, it is hardly ever debated, and it does not play – as a constitutional right – a significant role in academic or societal debates on privacy, for example when discussing the impact of new technologies. Instead, like in political debates and in case law, more often, Article 8 ECHR is invoked when privacy-related problems are discussed and when the acceptability of new, potentially privacy-threatening technologies is to be assessed. The legislator motivates privacy-infringing laws,

---

[23] See Blok 2002, Ch. 3, for an overview and background of the constitutional right to privacy.
[24] See Blok 2002, pp. 58-59.
[25] *Kamerstukken II* 1975/76, 13 872, No. 3, p. 41, quoted in Blok 2002, pp. 58-59.
[26] Blok 2002, pp. 43-65 and 72, with references to legislation and case law.

notably in criminal procedure and national security, by following the assessment scheme of Article 8 ECHR: does it infringe privacy, and if so, is it foreseen by law, does it serve one of the goals of Article 8, paragraph 2 ECHR, and is it necessary in a democratic society? The Dutch constitutional right to privacy thus currently has little added value, in practice, over Article 8 ECHR. It is likely that this is partly caused by the fact that the ECHR provision is more specific, with its assessment scheme. In our opinion, in order to keep the right to privacy vital and visible as an important right on the national level, it would be useful to strengthen Article 10, paragraph 1, and to give it more power in practice, by including crucial elements of Article 8 ECHR. Particularly important in this respect is specifying the grounds for limitation ('without prejudice to restrictions') by including the element of necessity for the purpose of specifically mentioned interests.

Article 10, paragraph 1 has not been discussed in the context of the debate on digital constitutional rights.[27] The CFRDA suggested a slightly different wording, but with exactly the same content, and the government did not propose any adaptation in its 2004 draft Bill to amend Article 10, which only covered the second and third paragraphs of Article 10.

Data protection

Early debates on data protection did not include a constitutional perspective, until a proposal to include data protection in the Constitution appeared in 1975. It contained some of the emerging international data-protection principles, and attached these to the general right to privacy as an instruction norm to the government, in Article 10 paragraphs 2 and 3 Gw:

> '2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.
> 3. Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.'

These rights, part of the revised 1983 Constitution, largely entered into force in 1988, together with the main implementing law, the Person Registries Act [*Wet persoonsregistraties*]. Data protection as regulated in this Act was broader than the constitutional instruction norm, encompassing more data-protection principles, based on the international set of data principles as embodied in, for example, the 1981 Convention 108 of the Council of Europe. Following the European Directive 95/46/EC, the Person Registries Act was replaced in 2001 by the Personal Data Protec-

[27] The CFRDA cursorily considered the suggestion to replace Art. 10 para. 1 by a right to informational self-determination, comparable to the German constitutional right, but rejected this as having no added value. CFRDA 2000, p. 126.

tion Act [*Wet bescherming persoonsgegevens*]. This Act is being evaluated in 2006-2007.

The interpretation of and debate about data protection in the Netherlands is very much focused on these Acts, and seldom touches upon the constitutional safeguards of Article 10, paragraphs 2-3.[28] For the purposes of this chapter, we leave the general debate about the impact of new technologies for data protection aside, and restrict ourselves here to a constitutional perspective.

The CFRDA noted that, from a legal perspective, there is no strict need to adapt Article 10, paragraphs 2-3 in light of technological developments; after all, the legislator is free to determine more rules to protect people's personal sphere than are indicated by the constitutional instruction norm. However, they suggested that in Article 10, paragraph 2, 'storing and providing' would be replaced by the more general 'processing' of personal data, this being the core of Directive 95/46/EC. Moreover, they proposed extending the rights of Article 10 paragraph 3 with a right to take cognizance of the source of data and of the purpose of data processing, as well as with claims concerning deletion of personal data and complaints against data processing. No arguments were offered why exactly these issues should be included in the constitutional right to data protection.[29] Nevertheless, the proposal was adopted by the government and included in a draft Bill. The Council of State, however, offered fierce criticism of the proposal: there is no apparent urgent need here to amend the Constitution, it is undesirable to amend the Constitution to implement a European Directive, and it is not clear why the proposal would raise these four additional data-protection principles to a constitutional level, but not other principles as contained, for example, in Article 8 of the European Charter of Human Rights.[30] The Cabinet was convinced at least in part by the Council of State's objections and decided not to submit the Bill to parliament, but to draft a new Bill later on. As of June 2007, no new proposal has been published.

Two other fundamental issues relate to the essence of data protection: is it related to privacy, and should it in fact be protected at the constitutional level at all? The first issue has been raised in the literature. On the one hand, it is quite common in the Netherlands to speak of data protection as 'privacy protection',[31] and the data-protection legislation is in practice often referred to as 'the Privacy Act'.[32] Also, in the Dutch Constitution, data protection is tied along with the general right to privacy, thus suggesting a strong link between the two. On the other hand, there are significant differences between paragraph 1 and paragraphs 2-3 of Article 10: the former is a defensive right, the latter an instruction norm. Moreover, as Peter

[28] For example, the standard handbook Berkvens and Prins 2007, extensively discusses the Personal Data Protection Act, but merely mentions Art. 10 paras. 2-3 in passing.

[29] CFRDA 2000, pp. 130-132.

[30] Raad van State 2002a. The document contains the draft Bill and Explanatory Memorandum, and the Cabinet's reaction to the Council of State.

[31] E.g., Cuijpers (2007), p. 11, calls the data-protection principles 'privacy principles'.

[32] E.g., Kuitenbrouwer 1991, Ch. 9.

Blok has eloquently argued, data protection ultimately perhaps has less to do with privacy than with fair treatment, and personal data are also protected by data-protection principles if they are not privacy-sensitive at all. The current merger of the two rights blurs both of them and risks inflating their protectional value. Blok therefore proposed splitting up Article 10 into a right to privacy and a separate right to data protection.[33] He has been joined in that proposal by the Council of State, who also referred to the separation of privacy and data protection in the European Charter of Human Rights.[34] We consider Blok's argumentation sound and convincing and also recommend splitting. However, the Cabinet has earlier rejected this splitting proposal,[35] and it remains to be seen whether data protection will be separated from Article 10.

The second fundamental issue has also been raised by Blok. Principles for fair and correct data processing are important principles, but the same can be said of many principles. Not all principles need to be raised to the constitutional level, particularly since the Dutch Constitution is formally considered as 'sober', and not a 'table of contents of ordinary legislation'. Blok considers the instruction norms for data-protection legislation not essential enough to be included in the Constitution,[36] but this view has so far not been shared in the parliamentary discussions on digital constitutional rights.

A final, new issue worth mentioning is the discussion initiated by Vedder to include 'categorical privacy' within the ambit of data protection, i.e., data that relate not to individuals but to groups. With the increasing possibilities for data mining and group profiling, more and more data are being processed that are not linkable to individual persons, but which nevertheless contain information about people and may have a significant impact on people's lives when they are applied to individuals. The CFRDA did not find this issue sufficiently developed yet to warrant constitutional amendment; non-constitutional rules could suffice for the time being.[37]

6.4.2 **Inviolability of the home**[38]

Constitutional protection

The inviolability of the home was registered as early as the 1798 *Staatsregeling voor het Bataafsche Volk* [*State Regulation for the Batavian People*], and included in the Dutch Constitution of 1848. In 1983, the provision was placed in Article 12

---

[33] Blok 2002, pp. 66-70. Likewise, Ekker 2006, s. 8.5.

[34] See Raad van State 2002a.

[35] *Kamerstukken II* 2000/01, 27 460, No. 2, p. 44.

[36] Blok 2002, p. 71.

[37] CFRDA 2000, p. 128, referring to Vedder 1998. Cf., also Custers 2004.

[38] This section is partly based on Koops 2004, particularly Ch. 3 and Ch. 6. This book extensively surveys the consequences of new technologies for the constitutional protection of the home and of the body.

of the Dutch Constitution, with the addition of an identification and reporting obligation. As recently as 2002, the Article was adapted because of exceptions to the reporting obligation in connection with national security.[39] Nevertheless, the first paragraph principally still contains the same essence as in 1848:

> 'Entry into a home against the will of the occupant shall be permitted only in the cases laid down by or pursuant to Act of Parliament, by those designated for the purpose by or pursuant to Act of Parliament.'

Paragraphs 2 and 3 contain further requirements in case of infringements. Government officials entering a dwelling on the basis of paragraph 1 must first identify themselves and state the goal of their entry, except when stipulated otherwise by law (Art. 12 para. 2). Moreover, the occupant must be notified in writing expeditiously after the entry, except when for law-enforcement or national-security reasons it is important to postpone or, only in national-security cases, to cancel the notification (Art. 12 para. 3).

The term 'enter' (*binnentreden*, literally: stepping inside) is particularly relevant in this context. The Supreme Court of the Netherlands stipulates in the so-called 'arm ruling' that a person is in violation of the home when she puts her arm into a building to pull someone out to arrest him. To 'step inside' is therefore not only a case of entering a home by putting one's foot into a building, but also of entering by using other parts of the body. This means, however, that it still concerns physically using a limb to enter the home: 'the emphasis should be on protection against unlawful entry of a home by external parties, *irrespective of which part of the body is used by the external party* to violate the home' [emphasis added].[40] However, in literature, there is a plea for a wider interpretation. Tak, for example, speaks of a violation 'as soon as an act is undertaken with the purpose of violating the inviolability of the home', but he gives as an example, breaking a window from the outside, which is still a physical and visible violation of the home.[41]

Despite the apparent physical formulation of the right to inviolability of the home, the CFRDA spent few thoughts on Article 12. Restricting themselves to direct eavesdropping, with directional microphones (from the outside) or with bugs (placed in the house after stealth entry), the CFRDA noted that it is odd if protection of the home depends on the *way* a conversation within a home is being intercepted (with bugging being a violation of Art. 12 because of the entry, and directional microphones not being a violation of Art. 12). However, they did not consider any amendment necessary, since conversations in the home are more protected through (the proposed new) Article 13 on secrecy of communications (see below 6.5.1).[42]

---

[39] See Act of 7 February 2002, concerning changes in the Dutch Constitution of the provisions concerning entering of homes to the revision of Art. 12 DC, *Staatsblad* 2002, 144.

[40] Hoge Raad [Dutch Supreme Court] 7 February 1956, *Nederlandse Jurisprudentie* 1956, 147.

[41] Tak 1973, pp. 77-78.

[42] CFRDA 2000, p. 206-207.

The CFRDA therefore did not consider other ways of monitoring a dwelling from the outside. The Cabinet, in its reaction to the CFRDA report,[43] did not pay any attention to the inviolability of the home, and left a parliamentary question on an 'electronic right to inviolability of the home' unanswered.[44]

The physical focus has been challenged in the literature. Koops, Van Schooten, and Prinsen have argued that there is little difference for a person's privacy of home life if this is violated by a body part entering the home or by obtaining information from outside. Furthermore, physical entry can usually be seen, whereas violations using modern technologies such as directional microphones, thermal-imaging sensors, and minuscule cameras are much less noticeable, and a citizen can do little to prevent them from being used. Therefore, it is no longer sufficient for citizens to take responsibility to protect their own privacy by closing the curtains if they want to prevent someone from seeing what they are doing in their home. Just as people behave differently at home if an investigating officer and an investigating judge are looking around, they also would feel restricted and inhibited if they knew that the police were observing their behaviour inside the home or that they were potentially being watched secretly. This infringes the essence of the inviolability of the home. Therefore, an 'electronic' right to inviolability of the home is necessary. Koops, et al. propose to remove the term 'entering' from Article 12 paragraph 1, and reformulating the right in terms of: 'The home is inviolable', 'Everyone has the right to inviolability of the home', or 'Everyone is inviolable in her home'. The essence of the inviolability of the home, in their opinion, is the right to be uninhibited in one's home, meaning that, in principle, neither the inside of the home nor the behaviour within it may be infringed or monitored.[45]

Article 12 provides two additional stipulations in paragraphs 2 and 3. By its nature, the requirement of prior identification (para. 2) particularly concerns the physical entry of the home. In contrast, an electronic infringement of the inviolability of the home has a natural claim to secrecy: electronic observation for purposes of criminal proceedings is less worthwhile if the occupant knows that she is being observed. This is why the present paragraph 2 could remain restricted to cases of entry.[46] The reporting obligation in paragraph 3, however, would be important in respect of other types of infringements besides entry. In the case of covert observation from the outside, notification is even more important because the citizen is by definition unaware that an infringement has been made on the inviolability of her home. The third paragraph should therefore apply to all types of infringement of the inviolability of the home as formulated in the first paragraph.[47]

---

[43] *Kamerstukken II* 2000/01, 27 460, No. 1.
[44] Id., No. 2, p. 58.
[45] Koops, et al. 2004, s. 11.1.
[46] Koops, et al. 2004, s. 11.1. In the same vein, CFRDA 2000, p. 207.
[47] Koops, et al. 2004, s. 11.1.

The home in relation to criminal investigation

Since the right to inviolability of the home has a very broad exception ground in the Constitution ('only in the cases laid down by or pursuant to Act of Parliament'), it is relevant to look at the protection of the home in lower legislation. For the purposes of this chapter, we leave aside the General Entry Act, which lays down requirements for any kind of government entry in a dwelling,[48] and focus on the provisions relating to the home in the Dutch Code of Criminal Procedure [*Wetboek van Strafvordering*, hereinafter: DCCP]. These have a similar emphasis of physical infringement of the home, in the context of search and seizure (see, in particular, Arts. 96c, 97, and 110 DCCP). It is not very clear to what extent the home is protected against judicial inspection from the outside. The legislator has only given thought to this in the context of the direct interception of confidential communications (*direct afluisteren*, the Dutch equivalent of the US 'oral interception'): eavesdropping from outside is equivalent to entering a home to install monitoring equipment.[49] However, violation of the home is considered less serious when activities inside the home are observed from the outside, with or without technically-aided means: observation of behaviour inside the home without physical entry is only considered as equivalent to entering the home, if the observation takes place permanently.[50] Less stringent conditions apply for 'non-permanent' observation than for searching premises: it just takes an order from the public prosecutor and suspicion of any crime.

The literature has pointed out one significant gap in protection of the home in the context of criminal procedure: the authorization procedure for network searches. Article 125j DCCP authorises the judiciary when searching a place, to search elsewhere in a computer system that is legitimately accessible from the place that is being searched. A home computer can nowadays easily be connected to computers elsewhere, for example, through wireless Internet connections and access to hotspots. At present, a search can be carried out in other places than inside the home under far less stringent conditions than those applying to a search of the home: a search can also be carried out in every place (with the exception of a home) by the (assistant) public prosecutor (Art. 96c DCCP), and a vehicle can even be searched by any investigating officer (Art. 96b DCCP). When a car is searched and a laptop is found with a wireless Internet connection via a mobile hotspot to a home computer, the investigating officer can, through a network search of the pc, search the home without the authorisation of an investigating judge. This means that the home computer is less protected by law, and this in an age where computers are increasingly containing more data about the personal lives of the occupants. This gap in legal protection can be closed by, for example, including a provision in Article 125j DCCP

[48] *Algemene wet op het binnentreden*, Act of 22 June 1994, *Staatsblad* 1994, 572.
[49] See Art. 126l DCCP and *Kamerstukken II* 1996/97, 25 403, No. 3, p. 79.
[50] *Kamerstukken II* 1996/97, 25,403, No. 3, pp. 70-71.

stating that the investigating judge's authorisation is required if a network search from a non-dwelling covers a computer elsewhere in a home.[51]

In this context, it is also relevant to note the suggestion that in the long term, the concept of 'dwelling' may need to be re-interpreted. Through technological and societal developments, the function of the house is changing: it includes more 'outside' activities like work (through teleworking and domotics), while at the same time, the place where you can be completely yourself may no longer be restricted to the dwelling, if in a world of Ambient Intelligence people may feel equally 'at home' in other places. This calls for a longer-term reflection on the right to inviolability of the 'home'.[52]

6.4.3 **Inviolability of the body**[53]

Constitutional protection

The right to inviolability of the body, or bodily integrity, was introduced in the Dutch Constitution relatively recently, in1983, and only after many debates about the need for a specific right. This does not mean that it was considered irrelevant as a fundamental right, but rather that it was considered as part of the general right to privacy under Article 10. As the government argued, separating a part of privacy in a specific constitutional right is only useful if this provision offers additional protection, and this was not envisioned for bodily integrity; moreover, separating bodily integrity from the right to privacy risks watering down the notion of privacy.[54] However, forced by a resolution of parliament, the government introduced a proposal for a specific right to bodily integrity after all.[55] This resulted in Article 11 Gw, which has not changed since 1983:

> 'Everyone shall have the right to inviolability of his body,[56] without prejudice to restrictions laid down by or pursuant to Act of Parliament.'

This entails a right to resist acts aimed at infringing the integrity of one's body. The body appears to be seen in a physical sense; the constitutional right does not protect

---

[51] Koops, et al. 2004, s. 11.1. As an aside, besides identifying threats to legal protection, they note here that technology can also help to protect the home. For example, infrared cameras can be used to detect heat sources like the human body, and hence, in a search for a suspect, the whole house does not have to be searched but only those parts of the home in which heat sources are observed.

[52] Koops, et al. 2004, s. 11.1.

[53] Like the previous section, this section builds on Koops, et al. 2004, in particular Ch. 7 and Ch. 10.

[54] *Kamerstukken II* 1978/79, 15 463, No. 2, pp. 7-9.

[55] *Kamerstukken II* 1979/80, 16 086, No. 2.

[56] The regular translation (English translation of the Dutch Constitution, published by the Dutch Ministry of the Interior and Kingdom Relations, available at <http://www.minbzk.nl/contents/pages/6156/grondwet_UK_6-02.pdf>) uses the term 'person' instead of 'body', but in our opinion, the Dutch phrase *onaantastbaarheid van zijn lichaam* is better translated as 'inviolability of the body'.

mental integrity unless the mental infringement is the result of an act that physically affects the body.[57]

The grounds for restriction of infringement are extensively formulated: these must be determined by Act of Parliament or by a regulation that has a basis in an Act of Parliament. There is no mention of conditions under which an infringement is allowed. In this respect, this fundamental right does not provide any advantage over the general right to privacy under Article 10, which contains the same restriction clause.

Primarily, Article 11 is a right to be invoked by a citizen against the government; there is no duty of care for the government to actively encourage the protection of bodily integrity. In addition to being a defensive right – a right to protect the inviolability of the body against others – it is also a right to self-determination; the right to determine what to do with one's body. In that respect, informed consent is important: bodily integrity is not at issue if the person concerned gives permission for an act infringing her bodily integrity.

The right to inviolability of the body can be interpreted as a right to resist external influences on the body, covering acts that have some physical influence on the body, even if it is only a question of some cells or molecules being moved. It may exclude, however, acts that treat the body only in a reactive way without affecting it at all, like merely registering radiation from the body. In this respect, if a suspect's photograph is taken, it only infringes her bodily integrity if the camera uses a flash or if she were forced to pose in a certain position.[58]

There has been little discussion about the impact of new technologies on the constitutional right to bodily integrity. The CFRDA cursorily went into telesurgery as a topical issue, but found no reason to suggest adaptation of Article 11.[59] The Cabinet, in its reaction to the CFRDA report, likewise left Article 11 undiscussed, except when they noticed in passing that information relating to the body, including hereditary genetic information, is not covered by bodily integrity but by the right to data protection.[60]

In the literature, however, one problem has been noted in light of new technologies. Article 11 does not include a notification obligation as other fundamental privacy rights do.[61] This is not surprising, because as of old, infringements of bodily

[57] *Kamerstukken II* 1978/79, 15 463, No. 4, p. 2.

[58] For this interpretation, see Koops, et al. 2004, s. 7.4. They argue for a wider interpretation of bodily integrity to also cover mere registration of the body or of radiation from the body, since otherwise, new technical possibilities to covertly scan bodies could have a chilling effect on the self-determinational aspect of bodily integrity; Koops, et al. 2004, s. 10.1.

[59] CFRDA 2000, pp. 204-205. This conclusion is basically shared by Koops, et al. 2004, s. 10.1.

[60] *Kamerstukken II* 2000/01, 27 460, No. 1, p. 27.

[61] See Art. 10 para. 3 and Art. 12 para. 3. Art. 13 (secrecy of communications) does not contain a notification obligation yet, but this does occur in all proposals to update this provision: CFRDA 2000, p. 167; *Kamerstukken II* 2000/01, 27,460, No. 1, pp. 28-29.

integrity are physical acts that are immediately recognisable to those involved. Increasingly, however, technological developments enable the police to covertly scan the bodies of suspects or citizens, so that an infringement may occur without their knowledge that an infringement has taken place. Therefore, Koops, et al., have argued for an obligation of notification to be added to the fundamental right concerning bodily integrity, in cases in which the infringement is not by its nature known to those involved.[62]

These authors have also pointed out two longer-term issues concerning the right to bodily integrity in light of new technologies. First, as more and more technology is built-in in the human body (from cochlear implants and pacemakers to bionic limbs and chip neuro-implants), people may tend to consider this built-in technology to be an inseparable part of their body.[63] This means that bodily integrity could also extend to built-in technology. But where exactly does this technology end if an implanted wireless chip is connected to a computer or to an intelligent network? A reflection is needed on the scope of bodily integrity if people were to physiologically experience external data processors as a fundamental part of their being: how far does the right to bodily integrity extend outside the body?[64]

Second, another long-term question is how to apply the right to bodily integrity in the case of man-machine combinations or cyborgs, or even to robots with (near) human characteristics.[65]

Will fundamental rights need to differentiate between humans, cyborgs, and robotic androids, and, if so, at what point in the development of man-machine combinations does man stop being human, thus losing a claim to human rights? If no differentiation takes place, however, can the fundamental right to bodily integrity be upheld at all if man-machine combinations are inextricably connected to external body networks? In this light, developments in the field of man-machine combinations should be carefully monitored, and social and political debates should be held concerning such fundamental questions.[66]

The body in relation to criminal investigation

Like with the inviolability of the home, the right to bodily integrity in the Constitution gives little guidance as to the actual legal protection, given its wide exception

---

[62] Koops, et al. 2004, s. 10.1.

[63] Cf., would-be cyborg Kevin Warwick: 'The biggest surprise for me during the experiment was that I very quickly regarded the implant as being "part of my body", a feeling shared with most people who have a cochlea implant or a heart pacemaker. In my case though, there was a computer linked to my implant and because the computer was making things happen I very quickly became attached to it as well.' Warwick 2002a.

[64] Koops, et al. 2004, s. 11.2.

[65] Cf., Van Balen, et al. 2006, p. 62n, who sensibly note that avatars in virtual games cannot claim human rights.

[66] Cf., Van Balen, et al. 2006, p. 62n.

grounds. A brief look at the Code of Criminal Procedure offers some more insight into the extent of protection.

A basic distinction is made between searching clothing and searching the body. The first is less impinging than the second, and hence, searching clothing is allowed in more cases than searching the body and by a larger number of officials (see, for example, Art. 55b and 56 DCPP and Art. 8 paras. 3-4 Police Act 1993 [*Politiewet 1993*]). A body search is generally only allowed in the event of serious charges [*ernstige bezwaren*], i.e., when it is likely that the person is guilty of a punishable act. A second, major distinction concerns a search *of* the body versus a search *in* the body. The former means a search of the surface of the bare skin and openings and orifices of the upper part of the body; the latter a search of openings and orifices of the lower part of the body and searches using technology like x-rays or echoscopes to search the inside of the body. There are stricter conditions for searching inside the body (see Arts. 56 and 195 DCCP). Altogether, from the legal system and statements by the legislator, a ranking order can be made of investigating methods as to the seriousness of the infringement. Taking a photograph of suspects is a slight infringement, frisking a more serious infringement, taking a sample of internal body tissue is an even more serious infringement, and a psychological test using a polygraph (lie detector) or truth serum is considered to be the most serious infringement possible.[67]

It has been observed that due to developments in technology, the subsidiarity requirement, which states that a lesser infringement to a fundamental right is preferable to a more serious one, may lead to different conclusions in the future. As technology progressively provides more opportunities to scan clothing and the body from the outside, physical infringement of the body will be less necessary. Moreover, the distinction between searching *of* the body and searching *in* the body will blur or change. For example, many people will find a scanner that sees through clothing to show naked skin[68] a lot more disturbing than an x-ray scanner which shows just a skeleton, with or without drugs hidden in the stomach. As a result, the present hierarchy of seriousness of investigation powers may need to be reviewed.[69] More futuristic questions have also been raised, for example, under what conditions the police should be allowed, if at all, to intercept brain-to-brain or brain-to-computer communications;[70] and how a network search should be valued if networks are interconnected with cyborgs.[71]

---

[67] See, for example, the enumeration in the appeal to the Procurator General in HR 2 July 1990, *Nederlandse Jurisprudentie* 1990, 751.

[68] Cf., 'Plane passengers shocked by their x-ray scans', *Sunday Times* 7 November 2004.

[69] Koops, et al. 2004, s. 11.2.

[70] '[T]hought communication is the biggest – yet most likely – step of all. It is certainly the direction in which I want my own research to head in the future (...). [In 2050, cyborgs'] brains are linked, by radio, directly with the global computer network. They can tap into it, call on its intellectual power, its memory, merely by thinking to it. In return, the global network can call on its cyborg nodes for information or to carry out a task.' Warwick 2002b, pp. 294-295.

[71] Koops, et al. 2004, s. 11.2.

6.5 COMMUNICATION-RELATED RIGHTS

6.5.1 Secrecy of communications

Constitutional protection

The right to secrecy of communications entered the Dutch Constitution in 1848, as the right to inviolability of the secrecy of letters entrusted to public mail-transport agencies, which could only be infringed with a court order. It was felt that letters should be just as inviolable as the home. It basically protects against government taking knowledge of the contents of sealed letters; in the periphery of the right, it also implies some protection against telling to third parties the content that was lawfully taken knowledge of, for example, the text of postcards.[72]

Although in the 19th and 20th centuries, several debates took place to broaden the constitutional right with the secrecy of telegraphy and telephony, it was not until 1983 that these 'new' media were included in the Constitution.[73] A distinction was made with the secrecy of letters, in that the right to secrecy of telegraphy and telephony could be infringed by lower authorities than a judge. As a result, since 1983, Article 13 Gw stipulates a twofold right to secrecy of certain forms of telecommunications:

> '1. The privacy of correspondence [*briefgeheim*] shall not be violated except in the cases laid down by Act of Parliament, by order of the courts.
> 2. The privacy of the telephone and telegraph [*telefoon- en telegraafgeheim*] shall not be violated except in the cases laid down by Act of Parliament, by or with the authorisation of those designated for the purpose by Act of Parliament.'

The media-specificity of this formulation has led, since the mid-1990s, to rather fierce debates in literature and parliament to construct a more technology-neutral right. Following the dissertation of Hofman, who argued for a generic right to the secrecy of communications (telecommunications as well as oral communication),[74] a Bill was submitted to parliament in 1997 to amend Article 13 into a 'right to confidential communications'.[75] This was extensively discussed by the Second Chamber, which took a skeptical stance on using the vague concept of 'confidential communications' and disagreed with the proposal to allow infringements by lower authorities than a judge. Ultimately, an amendment was adopted that reformulated

---

[72] Van Dorst 1982 calls this the secrecy of communications in a broad sense, as opposed to the core right of the secrecy of communications in a restricted sense.

[73] For a historical overview of the discussions, see Hofman 1995, pp. 105-128 and Koops 2002, pp. 22-33.

[74] Hofman 1995, pp. 464-465.

[75] *Kamerstukken II* 1996/97, 25 443, Nos. 1-2.

the provision as the right to 'secrecy of letters, telephone and telegraph, and of comparable communication technologies', which could be infringed only by order of a judge. Moreover, it also included a right to secrecy of traffic data,[76] infringeable by any authority designated by law, as well as a duty of notification.[77]

The First Chamber, however, disagreed with the result of the Second Chamber decision, and found that the Bill had been handled under too great time-pressure without sufficient reflection. As a result, a Committee was installed to study constitutional digital rights at large (the CFRDA, see above 6.2), and the Bill to amend Article 13 was withdrawn.[78]

The CFRDA came up with a Hofmanish proposal for a 'right to communicate confidentially', infringeable by order of a judge (or a Minister in national-security cases) and with a duty of notification.[79] The Cabinet supported this proposal,[80] and a Bill with the same formulation was submitted to the Council of State for advice. The Council of State, however, considered that the very broad and vague concept of 'confidential communications' would lead to legal uncertainty and that the restriction ground was inadequately formulated; hence, it advised not to submit the Bill to Parliament.[81]

Further action was postponed pending the Declaration by the Committee of Ministers of the Council of Europe on *Human rights and the rule of law in the information society*.[82] The government subsequently intended to draft a new Bill to be circulated for advice before May 2007;[83] no such draft has been published as of June 2007.

Although the discussion on this constitutional right is far from resolved, some remarks can be made about crucial elements of a future revision, based on the discussion to date. Some elements are undisputed: the need to formulate it in a more technology-neutral way (although the level of 'technology neutrality' is disputed),[84] the inclusion of e-mail,[85] requiring a judge (or in cases of national security: a minister)

---

[76] Traffic data are data relating to communications, but not to their contents; for example, who communicated when and where with whom.

[77] *Kamerstukken I* 1998/99, 25 443, No. 232.

[78] Id., No. 40d.

[79] CFRDA 2000, pp. 135-169; see, in particular, p. 162.

[80] *Kamerstukken I* 2000/01, 27 460, No. 1.

[81] Raad van State 2002b.

[82] See *above* n. 15.

[83] *Kamerstukken II* 2005/06, 30 550 VII, No. 1, p. 63.

[84] See Letter of the Minister of the Interior and Kingdom Relations of 28 November 2005, *Kamerstukken II* 2005/06, 30 300 VII, nr. 35, pp. 1-2.

[85] In the parliamentary debate over the 1997 Bill, the government first took the position that e-mail only fell within the scope of the secrecy of communications if it was encrypted; some time later, however, the government changed its mind and included e-mail outright, and this seems to be the general point of view in the Netherlands to date.

to authorise infringements, and the creation of a duty of notification. Other elements, however, are more controversial. We mention three key issues.

The first is *what* exactly is to be protected by the constitutional right: the communication itself, communications as far as they have been entrusted to a third party for transport, or the medium over which the communication is transported? This is an as yet unresolved issue in the Dutch debate on adapting Article 13 Dutch Constitution.[86] The CFRDA and the late-1990s bill to adapt Article 13 opted for a 'communications' approach, in which communication as such is protected, and which therefore includes face-to-face communication in its protection. This has the advantage of apparent simplicity and legal certainty, since all communications are protected. The downside, however, is that two different kinds of communications are brought together which, at least historically, are not altogether comparable. The constitutional right to secrecy of letters as of old protected the citizen against the government from reading letters that had been entrusted to them in their role as transporter of mail; the protection of face-to-face communications rested as of old in the general notion of privacy, and was protected by the inviolability of the home (and by the self-protecting option of whispering). Arguing from that perspective, a 'channel' approach that emphasises protection of the medium of telecommunications has been advocated in academic literature, for example by scholars of the Institute for Information Law of the University of Amsterdam.[87]

The question what is being protected also relates to a second problem: defining the exact *duration* of the protection. This has been an issue in the parliamentary debate, with rather contradictory views: the 1990s Bill and the CFRDA opted for an extensive duration of protection: this included the period when communications are received by the recipient but not yet opened,[88] or even when communications are stored confidentially by the sender or receiver.[89] The Cabinet, however, restricted the duration to the transport stage,[90] although they did not define clearly whether the transport stage ends as soon as the receiver can access the communication, or when the carrier no longer has access to the communication (which is a significant difference in the case of e-mail and voice mail).[91] Whichever approach – 'communication' or 'transport' – is ultimately chosen, the legislator will have to provide a clear criterion to judge the duration of the protection.

A third issue, highly debated 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 – the location of a call. With the exception

---

[86] For a discussion of these varying approaches, see Koops 2002, pp. 277-286.

[87] See, for example, Asscher 1999, pp. 107-132, in particular the preference for the 'transport' scenario, pp. 131-132.

[88] CFRDA 2000, p. 155.

[89] *Kamerstukken II* 1997/98, 25 443, No. 5, p. 20.

[90] *Kamerstukken II* 2000/01, 27 460, No. 1, pp. 25-26.

[91] See Koops 2002, pp. 46-47, who argues for the latter interpretation.

of the Second Chamber, which included, without much argumentation, traffic data in the amended Article 13 (see above), the Cabinet's stance, like the CFRDA, is opposed to protecting traffic data within the context of the secrecy of communications. The main arguments are that there is no reason to treat traffic data differently from other types of privacy-related data, and that traffic data are less sensitive than the content of communications. This has been challenged by some scholars and the Data Protection Authority, who argued that traffic data are an integral part of the communications process and that excluding them from Article 13 creates the risk of a chilling effect on the secrecy of communications.[92] Moreover, academic literature has argued that the borderline between traffic data and content is becoming blurred, and that even 'traditional' traffic data like (e-mail) addresses and phone dialing (e.g., 'For information about sexual diseases, press 2') may nowadays reveal information about content. They therefore recommend at least providing traffic data with the same level of protection as the content of communication.[93]

The secrecy of communications in relation to criminal investigation

The secrecy of communications in relation to criminal investigation is too broad a topic to go into detail in the context of this chapter. There are extensive investigation powers to intercept telecommunications – including, since 1 September 2006, private telecommunications –, for direct eavesdropping (oral interception), and to order production of traffic and identification data from communication service providers. Also, telecommunication providers have to make their networks interceptable. We refer to general literature on the subject.[94]

Two aspects, however, are worthy of mention here given the discussion of the scope and nature of the constitutional protection. First, the Code of Criminal Procedure contains specific protection measures for sealed letters in the context of a search, which comes on top of the general protection against searching a dwelling. This provision, Article 102a DCCP, is difficult to comprehend in light of the historical constitutional right to secrecy of letters (which covers letters entrusted to a carrier) and with the general preference of the legislator to have the right to secrecy of communication end after transport. It is also discriminating against other forms of communications, such as voice messages on an answering machine or stored fax messages. It has therefore been recommended to adapt this provision, along with the revision of Article 13.[95]

Second, a draft Bill was launched in January 2007 to implement the 2006 Data Retention Directive.[96] This would alter the Telecommunications Act and the cur-

[92] Registratiekamer 2001; Asscher 2002, p. 104 and 245; Blok 2002, p. 55.
[93] Koops 2003a, p. 69; Smits 2006, pp. 418-420.
[94] Koops 2002; Smits 2006; for a journalistic account, see Van de Pol 2006.
[95] Koops 2003b.
[96] Directive 2006/24/EC of 15 March 2006 on data retention.

rent, limited, data-retention provision.[97] Article 13.4 would now be extended to require all telecommunication providers to store the traffic data as designated in an Order in Council for a period of 18 months. These data would include not only the location of the cell of origin and the cell of receipt of mobile telecommunications, but also the location of any other cell during the communication.[98] The draft Bill has triggered critical reactions not only by the telecommunications industry,[99] but also by the Dutch Data Protection Authority. The latter argued that the 18-month retention period was unsubstantiated and should be changed to the European minimum period of 6 months, and that no retention should be required of location data generated *during* a call, since this would enable 'an all too intrusive, comprehensive secret surveillance of the movements of very large numbers of unsuspected citizens' [our translation].[100]

6.5.2 **Freedom of expression**

Constitutional protection

A certain liberty of the press has always prevailed in the Netherlands. As early as the 16th century, no prior censorship was applied.[101] This freedom was, however, not absolute: anonymous publications, seditious libel against the government, and defamation of princes or authorities of neighbouring states were all forbidden.[102] The freedom of the press entered the Dutch Constitution in 1815 as Article 227. Since 1848, when this provision was amended, the wording of the freedom of the press has not been changed any more. In the present Constitution, the freedom of the press, as well as other aspects of the freedom of expression, are laid down in Article 7:

> '1. No one shall require prior permission to publish thoughts or opinions through the press, without prejudice to the responsibility of every person under the law.
> 2. Rules concerning radio and television shall be laid down by Act of Parliament. There shall be no prior supervision of the content of a radio or television broadcast.
> 3. No one shall be required to submit thoughts or opinions for prior approval in order to disseminate them by means other than those mentioned in the preceding paragraphs, without prejudice to the responsibility of every person under the law. The holding of

[97] Draft Telecommunications data-retention Bill [*concept Wet bewaarplicht telecommunicatiegegevens*], available at <http://www.justitie.nl/images/5454571%20Wet%20cons_tcm34-31070.pdf>. Cf., the Ministry of Economic Affairs' consultation web site <http://www.minez.nl/content.jsp?objectid=149504&rid=144530>.

[98] Draft Explanatory Memorandum, ibid., p. 4.

[99] Letter on the data-retention Bill consultation, 18 January 2007, available at <http://www.xs4all.nl/opinie/wp-content/uploads/2007/gez_reactie_aanbieders_wetsvoorstel_dataretentie.pdf>.

[100] Dutch Data Protection Authority 2007.

[101] Alkema 1990, cited in Besselink 2004, pp. 183-193.

[102] Van Gelder 1972, pp. 154-161, cited in Alkema 1990, p. 375.

performances open to persons younger than sixteen years of age may be regulated by Act of Parliament in order to protect good morals.
4. The preceding paragraphs do not apply to commercial advertising.'

Paragraph 1, which is identical to the old Article 227, requires a statutory provision to limit the freedom of expression via the press.[103] It is only in case of broadcasting that delegated legislation is permissible (para. 2). Other means of expression are also subject to statutory regulations, with the exception of performances of persons younger than sixteen years of age (para. 3).[104] Although Article 7 does not explicitly mention the right to spread information, this right has been recognised in the case law of the Supreme Court (usually called 'dissemination case law' [*verspreidingsjurisprudentie*]).[105] The right to receive information does not fall under the scope of Article 7 of the Constitution. This right is, however, protected by Article 10 ECHR, which can, through Article 94 of the Constitution, be directly invoked in Dutch Courts.[106] The right to collect information [*recht op nieuwsgaring*] does not fall under the scope of either Article 7 of the Constitution or Article 10 ECHR, but is protected by Article 19 of the International Covenant on Civil and Political Rights.[107]

Freedom of expression in a digital environment

The wording of Article 7 of the Constitution is technology-specific: it protects particular means of communication. Paragraph 1 protects the press, paragraph 2 protects broadcasting through radio and television, and paragraph 3 protects other means of expression, for example the performance of a play on stage.

It is not clear from the wording of Article 7 whether this provision also protects the expression of ideas or the publication of information through digital media, such as the Internet, and if so, which of the three paragraphs of Article 7 applies. This issue was addressed by the CFRDA in its advisory report to the Cabinet.[108]

[103] The freedom of the press can only be limited *after* the publication; it follows from the text of Art. 7, para. 1, that censorship before publication is not allowed. See however the decision of the Dutch Supreme Court in the case *Vestigingsbesluit Grafische Bedrijven*, HR 23 May 1961, *Nederlandse Jurisprudentie* 1961, No. 427, where a form of prior censorship was accepted under very specific circumstances (the measure did not intend to limit the freedom of the press, although it did in practice constitute a limitation).

[104] Alkema 1990, gives an extensive analysis of Art. 7 of the Constitution and relevant regulations that limit the freedom of expression.

[105] HR 28 November 1950, *Nederlandse Jurisprudentie* 1951, No. 137 (*APV Tilburg*); HR 17 March 1953, *Nederlandse Jurisprudentie* 1953, No. 389 (APV Nuth). It follows from this case law that this right to disseminate can be limited by delegated legislation.

[106] Afdeling Bestuursrechtspraak Raad van State [Council of State, Administrative Section], 10 October 1978, *Ars Aequi* 1979, 477 (*Antenneverbod Leerdam*).

[107] It can be argued that the right to collect information is also protected by an extensive interpretation of Art. 10 ECHR: *Yearbook of the European Convention on Human Rights* 1975, p. 74.

[108] CFRDA 2000, pp. 116-134.

They concluded that, because of its technology-specific wording, Article 7 of the Constitution is not suitable for application in a digital environment and therefore should be revised.

The Committee proposed a new, technology-neutral wording for Article 7, which would protect 'the right to express an opinion'. This right would contain the freedom to publish, spread, and receive thoughts or other information (proposed para. 1). With regard to limitations to the freedom of expression, the proposal of the Committee stated that

a) this right can be limited by Act of Parliament,
b) there can be no prior censorship, and
c) the right to spread or receive information can be limited by delegated legislation and by means of prior censorship, if this restriction on the freedom of expression is made in the interest of public order and does not refer to the content of the expression.

Furthermore, the Committee proposed to bring commercial information under the scope of the new Article 7 (para. 3) and to include a paragraph on the promotion of the pluriformity of ideas and information (para. 4).

As described above (6.2.1), the Cabinet announced in 2000 to draft a Bill of Amendment to Article 7 of the Constitution, following the advice of the CFRDA. After a negative advice of the Council of State, however, this Bill was withdrawn in 2004. In that year the Cabinet announced a new Bill of Amendment to Article 7. As of June 2007, this Bill had not yet been sent to Parliament.

Meanwhile, the right to freedom of expression in a digital environment such as the Internet has been recognised in the case law of the Dutch Supreme Court and the Courts of Appeal.[109] In most cases in which the freedom of expression on the Internet is invoked in Dutch courts, this claim is based on a combination of Article 7 Gw and Article 10 ECHR.[110] In such cases, the courts investigate the case under both provisions and do (in most cases) not specify which of the three paragraphs of Article 7 applies.[111]

Although the judiciary does recognise the freedom of expression in a digital environment under the present wording of Article 7, it would in our view be better

[109] Examples of recent case law are: HR 25 November 2005, LJN AU4019 (anonymous opinion on Internet); Gerechtshof [Court of Appeal] Amsterdam, 17 November 2006, LJN AZ3011 (discrimination of Jews and homosexuals on the Internet); Rechtbank [Lower Court] 's-Hertogenbosch 21 December 2004, LJN AR7891 (denial of the Holocaust on the Internet). All these cases are published at <http://www.rechtspraak.nl>.

[110] The European Court of Human Rights (ECtHR) has in its case law recognised the right to freedom of expression on the Internet under Article 10 ECHR. A recent example is ECtHR 18 October 2005, No. 5446/03, *Perrin* v. *United Kingdom*, published at <http://www.echr.coe.int/ECHR/>.

[111] Nieuwenhuis 2006, p. 204, points out that the three paragraphs of Art. 7 should be seen 'as a whole' and that the case law under Art. 7 of the Constitution and Art. 10 ECHR shows that the freedom of expression under these two provisions is a 'genus'.

if the legislator amended this provision. The technology-specific and already partly outdated wording of Article 7 causes legal uncertainty, and this will increase as new means of communication are developed in the coming decades. A new, more technology-neutral formulation would address this problem. The proposal of the CFRDA offers a clear and sufficiently technology-neutral legal framework for the freedom of expression in the information society. One aspect of this proposal, however, should be considered with care by Parliament: the reference to 'the interest of public order' [*het belang van de openbare orde*] as a ground for limiting the right to spread or receive information by delegated legislation and by means of prior censorship. It needs to be made absolutely clear what is meant by 'the interest of public order', both in a non-digital environment (e.g., on the street) and in a digital environment (e.g., on blogs or in virtual communities).

Proposals to amend the Constitution can be made by the Government and by the Second Chamber of Parliament (see above 6.2.1). If the Government does not proceed to submit a proposal for amending Article 7 in the near future, Members of the Second Chamber can, and in our view should, take the initiative for proposing an amendment.

Liability of Internet Service Providers

The Dutch Criminal Code [*Wetboek van Strafrecht*] contains a specific provision on the liability of Internet Service Providers (ISPs).[112] Article 54a of the Criminal Code[113] prescribes that intermediaries, including ISPs, shall not be prosecuted (for data stored on their web servers) if they obey to an order of the Public Prosecutor, after permission from a judge, to take all measures which can be reasonably expected in order to make the data inaccessible. Thus, if the ISP has 'taken all measures which can be reasonably expected from it', the freedom to spread information will prevail. The idea behind this wording is that preventive censorship by ISPs should be as limited as possible.[114] In recent documents of the Cabinet, however, this idea seems to be abandoned in the context of counter-terrorism measures.[115] In these documents, the Cabinet analyses a number of problems relating to the threat of terrorism and invocations of hate and violence on the Internet. According to the Cabinet, co-operation with ISPs is needed in order to cope with this threat of terrorism. The Cabinet indicates that ISPs are called upon to remove information which is not illegal but can be 'harmful to society', from their web services. The new

[112] A recent analysis of the liability of Internet Services Providers under Dutch criminal and civil law and the relation to the freedom of expression on Internet can be found in Peters and De Vré 2005, pp. 58-67.

[113] This provision is a result of the implementation of EC Directive 2000/31/EC (Directive on electronic commerce). The complete text of the provision can be found at <http://www.wetten.nl> (search for *Wetboek van Strafrecht*).

[114] *Kamerstukken II* 2001/02, 28 197, No. 3.

[115] *Kamerstukken II* 2004/05, 29 754, No. 24 and No. 6.

Cabinet, which took office in February 2007, intends to make a next step: in the Coalition Agreement for the new Cabinet, it announced that, 'in order to combat messages of terror and invocations of violence, new legislation will be prepared to prohibit ISPs to spread such information'.[116]

The Dutch Civil Code [*Burgerlijk Wetboek*] also contains a provision on the liability of ISPs. Article 6:196c regulates the liability for ISPs, distinguishing three types of services:[117] mere conduit (paras. 1 and 2), caching (para. 3) and hosting (para. 4). The provision indicates for each of these services under which conditions the ISP shall not be liable for information stored on its web server.

The liability of ISPs and the risk of 'hidden censorship' by ISPs have recently been addressed by the Council of Europe in the 'Declaration of the Committee of Ministers on human rights and the rule of law in the information society'.[118] In this Declaration, the Council of Europe calls upon ISPs and their customers to develop a framework of self-regulation:

> 'With regard to self- and co-regulatory measures which aim to uphold freedom of expression and communication, private sector actors are encouraged to address in a decisive manner the following issues:
> - hate speech, racism and xenophobia and incitation to violence in a digital environment such as the Internet;
> - private censorship (hidden censorship) by Internet service providers, for example blocking or removing content, on their own initiative or upon the request of a third party;
> - the difference between illegal content and harmful content.'

This is important for the Dutch debate on constitutional protection, as the government has repeatedly stressed the importance of this Declaration for adapting the Dutch Constitution in relation to new technologies.

Search engines

The meaning of search engines has been debated in the literature in recent years. A major contribution to this debate was made by Van Eijk who argued in his inaugural lecture ('Search engines, seek and ye shall find') that search engines should be seen as a 'connected right' to the freedom of expression.[119] Search engines are used to 'release' information which is already available elsewhere. Van Eijk argues that,

---

[116] *Regeerakkoord* [Coalition Agreement], 7 February 2007, p. 34, available at <http://www.kabinetsformatie20062007.nl/>.

[117] This provision is the result of the implementation of EC Directive 2000/31/EC (Directive on electronic commerce). The complete text of the provision can be found at <http://www.wetten.nl> (search for *Burgerlijk Wetboek*).

[118] COM(2005)56 final, available via <http://www.coe.int>.

[119] Van Eijk 2005, pp. 14-15; an English version is available at <http://www.obs.coe.int/oea_publ/iris/iris_plus/iplus2_2006.pdf.en>.

since search engines facilitate access to information, they are essential for the constitutional right of freedom of expression and information and should be recognised as such.

Weblogs

Since 2000, weblogs have become a more widespread phenomenon in the Netherlands. In reaction to this development, the legal status of 'bloggers' should be analysed. Particularly, the question has been raised whether 'bloggers' qualify as journalists and should have journalistic privileges. It is too early to draw conclusions based on case law or academic literature, but the general line in the debate so far seems to be that the question which medium is used to publish articles or other works is not crucial to determine whether someone is a journalist or not. What is decisive is the extent to which a work or series or works contributes to the public debate, as part of the rationale for journalistic privileges.

6.6 Other and new constitutional rights

Five other issues have featured more or less prominently in the Dutch debate on constitutional rights and new technologies. One relates to another right that is worded in a technology-specific way: the right to petition the government in writing, and another issue relates to the application of the right of association and assembly in a digital environment. The other three concern discussions about the possible inclusion of new rights: a right to anonymity, a right to access government information and a right to Internet voting.

6.6.1 Petition

The right to submit a petition is guaranteed by Article 5 of the Constitution, which holds: 'Everyone shall have the right to submit petitions in writing to the competent authorities.' This entails the right to submit a view or statement to the administration, legislation, and judiciary, but not the right to receive a reply.[120] In 2000, the CFRDA advised the Cabinet to propose an amendment of Article 5 of the Constitution, aimed at removing the words 'in writing'.[121] The amended provision would entail, besides the right to submit petitions on paper, the right to submit electronic and oral petitions. In a letter to Parliament in 2004, the Cabinet wrote that it would not propose an amendment of the Constitution, but instead proposed a 'dynamic interpretation' of the words 'in writing'.[122] Thus, 'in writing' would mean both

[120] Riezebos 1992, Ch. 5.
[121] CFRDA 2000, pp. 196-200.
[122] Letter to the Parliament of 29 October 2004, *Kamerstukken II* 2004/05, 27 460, No. 3, pp. 1-2.

characters on paper and characters on an electronic information carrier, such as a hard disk or a USB stick. According to this interpretation, citizens would under Article 5 have the right to submit petitions by electronic means.[123] We consider this interpretation convincing. Since 2000, an increasing number of government agencies have opened electronic mailboxes on their web sites to which citizens can submit petitions, and citizens have begun to use these channels to submit their petitions electronically.

Related to the right to submit electronic petitions is the – broader – right to communicate by electronic means with government agencies. In 2004, this issue was regulated by law, by adding a new provision to the General Administrative Law Act [*Algemene wet bestuursrecht*]. This holds that citizens have the right to send electronic messages to government agencies, if the agency has announced that 'its electronic mailbox has been opened'.[124]

6.6.2 Association and assembly

The CFRDA has raised the question how the fundamental rights of association (Art. 8) and of assembly and demonstration (Art. 9) – both formulated in a sufficiently technology-neutral way – should be viewed in a digital environment.

Article 8 reads: 'The right of association shall be recognised. This right may be restricted by Act of Parliament in the interest of public order. The CFRDA argued that an 'electronic association', i.e., an association established and functioning solely or primarily by electronic means, could equally claim constitutional protection as a 'physical' association, just as they can equally be forced to disincorporate when they infringe public order.[125] In horizontal relationships, the question has been raised to what extent providers of virtual games have the right to limit virtual associations within the game world, illustrated by a prohibition and subsequent allowing of a gay-friendly Guild in World of Warcraft. Van Balen, et al. argue that besides the freedom of association of players, a significant factor is that the players themselves have accepted the terms and conditions of the game, which may include limitations on associations or assemblies. Therefore, it is unlikely that association bans by a game provider constitute tort.[126]

With respect to the freedom of assembly and demonstration, the CFRDA noted that electronic assemblies, such as telephone conferences, are also protected by Article 9, which reads: 'The right of assembly and demonstration shall be recognised,

[123] In its letter, the Cabinet furthermore indicated that it would not propose an amendment to allow oral petitions.

[124] Art. 2:15 para. 1 General Administrative Law Act.

[125] CFRDA 2000, pp. 200-202.

[126] Van Balen, et al. 2006, pp. 77-78.

without prejudice to the responsibility of everyone under the law' (para. 1). More importantly, they argue that one of the limitation grounds in Article 9, paragraph 2 – 'in the interest of traffic' [*in het belang van het verkeer*] – also covers Internet traffic in relation to the right of assembly.

> 'The "regular" [i.e., non-constitutional, bjk & mg] legislator could use this ground, if so desired, to establish rules aimed at preventing people to use the Internet, with reference to the right of assembly, in such a way that Internet traffic is hindered.'[127]

We appreciate this interpretation as creative and useful, but we feel some caution is warranted, because 'off-line traffic' and 'on-line traffic' are rather diverse things,[128] and because interpreting 'traffic' in the Constitution as encompassing Internet traffic sets a precedent for interpreting 'traffic' in other laws, such as the Criminal Code. More reflection and analysis of the specific goals of protecting 'traffic' in legislation is needed, but, in principle, the CFRDA's interpretation is a fruitful direction to study.

Article 9 can likewise cover electronic demonstrations, i.e., demonstrations, made electronically in public, of political or societal feelings or desires, according to the CFRDA. Also with electronic means of expression, Article 9 has an added value over the freedom of expression (Art. 7) because a demonstration adds a 'demonstrative element' to this, like blocking a search engine, and hence, such expressions should not only fall under the protection of Article 7 but also, in principle, under Article 9. The CFRDA noted that the concrete circumstances will determine how far such electronic demonstrations should be allowed to go.[129]

6.6.3 **Anonymity**

A right to anonymity has been briefly discussed in the context of digital constitutional rights. The CFRDA, somewhat oddly, considered it as an alternative to the right to privacy; it is not surprising that this was not found a practicable alternative, since a right to anonymity would be larger than a right to privacy and would have more exceptions.[130] The Cabinet, in its reaction, agreed, and added that a right to anonymity was not needed as a replacement or as an addition to the right to privacy. Article 10 offers sufficient protection even if anonymity should be considered a starting point in society.[131] They moreover added later that knowability rather than anonymity is the basic rule in society. Although there sometimes is a need for

[127] CFRDA 2000, p. 203 [our translation], noting that the current rules to protect traffic in the Public Demonstration Act [*Wet openbare manifestaties*] can only be read as applying to physical traffic and physical demonstrations.

[128] Cf., Schellekens 2006.

[129] CFRDA 2000, pp. 203-204.

[130] Id., p. 125.

[131] *Kamerstukken II* 2000/01, 27 460, No. 1, p. 20.

anonymity, this need is not fundamental enough to safeguard it at a constitutional level.[132]

This view is by and large shared in the literature. The most extensive discussion has been provided by Anton Ekker in his dissertation on the constitutional grounds for anonymity in public speech. He drew the conclusion that anonymity is important in the context of constitutional rights, in particular freedom of speech, but also freedom of religion, demonstration, and the right to privacy and data protection. It is currently being protected in a very piecemeal fashion, and there are many different legal procedures to infringe anonymity; hence, Ekker recommends introducing a systematic, general right to anonymity, to provide a firmer basis for anonymity in the increasingly complex, and technologically converging, sphere of communications. However, he does not consider that such a general right to anonymity should be created at the constitutional level, given the nature of the Dutch Constitution as only safeguarding the most essential constitutional interests. Instead, he offers some recommendations to shape the right to anonymity in lower legislation, with a procedure for providing identifying data in civil proceedings and a provision in the Telecommunications Act.[133]

6.6.4 Access to government information

A right on access to public information is guaranteed by law,[134] but not by the Constitution. In 2000, the CFRDA advised the Cabinet to propose an amendment to the Constitution, which would guarantee access to legislation, government information, and judicial decisions.[135] The CFRDA proposed the following text for a new provision of the Constitution:

> '1. Everyone shall have the right on access to public information. This right can be restricted by or pursuant to Act of Parliament.
> 2. The Administration has a positive obligation to promote access to public information.'

The CFRDA indicated in its explanatory memorandum that the proposed provision would entail a right for citizens on access to both information stored on paper and information stored on digital carriers (i.e., computer networks). Furthermore, it would

---

[132] Id., No. 2, p. 44.

[133] Ekker 2006, Ch. 10.

[134] The Freedom of Information Act [*Wet openbaarheid van bestuur*] regulates access to government information. The Act on the Publication of Acts of Parliament and Regulations [*Bekendmakingswet*] prescribes that Acts and Regulations shall be published in official publication journals. Access to judicial decisions is guaranteed by the Constitution, which prescribes in Art. 121 that trials shall be held in public, except in cases laid down by Act of Parliament.

[135] CFRDA 2000, pp. 190-194. See for a general analysis of constitutional protection of access to public-sector information, including policy dilemma's, Prins 2004.

impose an obligation on government agencies to make public information accessible by electronic means of communication, such as the Internet.

In 2001, the Cabinet announced that it intended to follow the advice of the CFRDA to propose this amendment of the Constitution and would ask the advice of the Council of State. Since then, successive Cabinets have been silent on the issue. The advice of the Council of State has not been published and the Bill of Amendment has not yet been sent to Parliament. In 2004, the Cabinet wrote to Parliament that a decision on the proposal for the amendment to the Constitution would be postponed until the Cabinet had made a decision regarding a revision of the Freedom of Information Act.[136] In May 2006, the Ministry of the Interior and Kingdom Relations published a proposal for a new Freedom of Information Act, which had been drafted by an external expert.[137] As of June 2007, this proposal had not yet been sent to Parliament.[138] The Cabinet is expected to decide in the coming year on both the Bill for amending the Constitution and the Bill for revising the Freedom of Information Act.

Furthermore, special attention is given to access to legislation documents and to Internet consultation during the legislative process. In November 2006, the Minister of Justice announced the development of a system for Internet consultation during the first stage of the legislative process.[139] This system will enable individuals and organisations to give their views on proposals for new legislation via the Internet while the legislation is being drafted by the ministries. Thus, individuals and organisations can present their views on new draft legislation at the earliest possible stage.

6.6.5 **Internet and electronic voting**

On 31 December 2003, the On-line Voting Experiments Act [*Experimentenwet Kiezen op Afstand*] entered into force.[140] It contains interim rules for experiments

[136] The announcement of a revision was made after publication of an evaluation of the Freedom of Information Act. The evaluation report – Van der Hof, et al. 2004 – which was commissioned by the Ministry of the Interior and Kingdom Relations, was sent to Parliament on 10 May 2004 and is available at <http://www.tweedekamer.nl> (reference number bzk0400352). See also Van der Hof 2007, pp. 251-252.

[137] Van der Meulen 2006.

[138] In answer to questions from Parliament, the Minister wrote in June 2006 that he would send a Bill for a revised Freedom of Information Act to Parliament 'as soon as possible', *Handelingen II* [Parliamentary Proceedings Second Chamber] 2005/06, Aanhangsel, No. 1637, pp. 3489-3490. In April 2007, the new Minister of the Interior and Kingdom Relations wrote to Parliament that she had consulted several organisations about the draft Bill and she expected to be able to send a Cabinet Opinion about the draft Bill within a few months (Letter of 25 April 2007, reference number bzk0700149, available at <http://www.tweedekamer.nl>).

[139] Letter of the Minister of Justice to Parliament, 9 November 2006, *Kamerstukken II* 2006/07, 29 279, No. 41, p. 11 and attachment 1, *Startnotitie Openbare internetconsultatie bij voorbereiding van regelgeving* [Memorandum on Public Internet consultation during the legislative process]. For an analysis of the constitutional aspects of this proposal, see Prins 2006, p. 2401 and Groothuis 2005, pp. 36-38.

[140] *Staatsblad* 2003, 569.

conducted with new facilities enabling voters abroad to cast their votes 'with the help of information and communication technology, in a manner other than by post'. The explanatory memorandum mentions voting by Internet or telephone. The Act is of an interim nature and will expire on 1 January 2008. It is expected that it will then be replaced by a 'permanent' law.

In the elections for the Second Chamber of Parliament in November 2006, 19,929 voters abroad cast their votes through the Internet.[141] An expansion of Internet voting to the general population has been briefly discussed in the context of a revision of the Elections Act [*Kieswet*], but is not expected before 2008, the year in which the Online Voting Experiments Act expires.

Electronic voting machines [*stemcomputers*] – to be distinguished from Internet voting techniques – have been used in the Netherlands for more than twenty years, and electronic voting has become the method of balloting for 90 per cent or more of the electorate. In the period preceding the November 2006 elections, a public debate arose on the integrity and confidentiality of the voting machines. A pressure group, Wij vertrouwen stemcomputers niet ['We do not trust voting computers'], complained of inadequate security protection for the machines, and their vulnerability to manipulation. Moreover, it demonstrated that it was technically feasible, in certain circumstances, to intercept from a distance radiation from the machines in such a manner as to undermine the secrecy of the ballot.[142] The government responded to these concerns with a series of security measures to limit the risks indicated and nominated a committee of experts which was asked to further investigate the risks and advise whether additional measures are necessary for future elections. The committee published a critical report in May 2007, recommending, among other things, to stipulate a series of requirements for integrity and confidentiality of voting machines, including limits on radiation, in the Regulation on voting machines 1997. The set of requirements should be revised every two years, given the on-going technological developments.[143] Moreover, a Committee on the Voting Process Design [*Commissie Inrichting Verkiezingsproces*] is to publish recommendations in October 2007 for a future-proof system of dealing with voting machines.

6.7 Conclusion

Around the turn of the millennium, the developments in new technologies, in particular ICT, led to serious debates about amending the Dutch Constitution. This was

---

[141] Experiments with voting by telephone have not yet taken place. In March 2007, the Organisation for Security and Co-operation in Europe (OSCE) published an Assessment Mission Report of the last elections, which includes an assessment of the Internet voting. The report is available at <http://www.osce.org/documents/odihr/2007/03/23602_en.pdf>.

[142] See <http://www.wijvertrouwenstemcomputersniet.nl/>. The public debate and the findings of the pressure group are described in the OSCE report, available at <http://www.osce.org/documents/odihr/2007/03/23602_en.pdf>.

[143] Commissie Besluitvorming Stemmachines 2007.

particularly triggered by the technology-specific formulation of several constitutional rights, aggravated by the prohibition on constitutional review of Acts of Parliament by the courts, but also by several suggestions being made – some stronger than others – for new fundamental rights. The debate focused largely on the technology-specific rights (particularly Art. 7 on freedom of expression and Art. 13 on secrecy of communications), the general right to privacy, and a new right on access to public information. Some of the academic literature has called for attention to other rights at stake due to new technologies, such as the inviolability of the home and of the body, and a right to anonymity. Despite all debates and intentions, unfortunately, no Bills to amend the Constitution have been submitted to Parliament so far, as of June 2007. We hope that the recent comparative study[144] will lead to concrete amendments soon, since we consider several amendments to be urgently needed. We summarise here the findings of our overview that are relevant to the Constitution.

The general right to privacy (Art. 10, para. 1) is sufficiently technology-neutrally formulated. In practice, however, it plays hardly an important role as a constitutional right in political or legal debates and decisions on privacy; instead, Article 8 ECHR is usually referred to. In our opinion, Article 10, paragraph 1, could be strengthened and given more power if crucial elements of Article 8 ECHR were included, in particular the ground for limitation of necessity for the purpose of specifically mentioned interests.

The right to data protection (Art. 10, paras. 2-3) should in our opinion be separated from the right to privacy in a separate provision, to make clear its distinct nature; because of its link to privacy, it could be placed in the catalogue of privacy-related rights (current Arts. 11-13). It is also recommendable to study which elements of data protection should be explicitly mentioned in the constitutional provision, since the current selection may seem somewhat arbitrary; perhaps the European Charter could provide inspiration in this respect. Moreover, the right to data protection should also be studied in light of the consequences of profiling, given that (group) profiles do not as such count as personal data.

The inviolability of the home (Art. 12) is currently formulated too physically ('entry'), and it should be replaced by a more general wording, such as 'The home is inviolable', so that also monitoring the home from outside falls within its scope. The obligation of prior identification (para. 2) could remain as is, since it is tied with physical entry, but the notification requirement (para. 3) should be extended with electronic monitoring of the home. In the longer term, the notion and importance of the 'home' as the key physical place to be left alone should also be studied, because technological developments will increasingly blur the borders of 'home' and 'outside world' and may thus shift the function of the home in the societal context. The inviolability of the body (Art. 11) is overall well-regulated, but given the increasing possibilities of scanning bodies without people necessarily noticing

[144] Koops, et al. 2007.

this, an obligation of notification could be added in this provision, in cases in which the infringement is not by its nature known to those involved. A long-term issue for future research is how the right to bodily integrity should be applied in the case of man-machine combinations or cyborgs.

Article 13 on secrecy of (tele)communications is in urgent need of amendment; the media-specific formulation should be replaced by a more technology-neutral one, which should at least cover e-mail. We do not, however, necessarily agree with most proposals to date to make it complete technology-neutral by speaking only of the secrecy of communications, given the historical background of protecting *tele*communications where a third party by definition has access to the communication. Fundamental reflection is needed on the nature of what is to be protected – 'communication' or 'transport' – and following this, which stages of communication are to be protected. It is not easy to make a choice here; perhaps most important is that the legislator simply makes a choice and provides a clear and consistent explanation of what exactly is to be covered by the new formulation. Equally important is that the requirement of a judge (or in cases of national security: a minister) to authorise infringements remains in place, and that a duty of notification is created.

Because of its media-specific and partly outdated formulation, Article 7 on freedom of expression is also in need of amendment. Although there is perhaps more leeway for interpretation in light of new technologies than with Article 13, the media-specific wording causes uncertainty. The proposal for amendment as suggested by the CFRDA is to be recommended, providing the freedom to publish, spread, and receive thoughts or other information, with some limitations. The only catch in the CFRDA's proposal is the phrase 'in the interest of public order'; this should be very carefully and strictly explained, in order to prevent the legislator from too easily passing laws to restrict freedom of expression.

Three other rights discussed – the right to petition, association, and assembly – seem adequately formulated in light of new technologies, particularly with the 'dynamic interpretation' that can be given phrases like 'in writing' to meet developments in technologies and society.

With respect to suggestions for new fundamental rights, there is insufficient reason to raise valid claims to anonymity or to distance voting to the level of constitutional protection, but it is important to study these claims in light of new technologies and to see which mechanisms – legal, organisational, or technical – should be fostered to safeguard them. Another right is more important, however, from the perspective of new fundamental rights: the right to access public information. The CFRDA has convincingly argued that in our current society, this right merits protection at the constitutional level, and hence we hope that a Bill to insert a right to access public information in the Constitution is submitted to parliament in the current session. However, it is equally important, and rather more urgent, that the existing legislation on access to public information, the Freedom of Information Act, be revised and updated, along the lines recommended in the 2004 evaluation report.

Last and foremost, a recurring issue in the debate on digital constitutional rights in the Netherlands is constitutional review. The current prohibition in Article 120 for the judiciary to review Acts of Parliament on conformity with the Constitution is a spectre hovering over future amendments in light of new technologies. 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. The desire to formulate fundamental rights in a more technology-neutral way implies that more general and abstract wordings are used, which necessarily give more scope for interpretation. In order to prevent the legislature from interpreting the constitutional rights in too free a manner – and limiting citizens' rights more than intended by the Constitutional legislature –, checks and balances by the judiciary are needed. Therefore, when the Constitution is amended to update and extend several provisions in light of new technologies, constitutional review should be created, so that the constitutional rights at issue can effectively provide protection to citizens in actual practice.

References

ALKEMA 1990
E.A. Alkema, 'The Protection of the Freedom of Expression in the Constitution and in Civil Law', in *Netherlands Reports to the International Congress of Comparative Law* (The Hague, Asser Instituut 1990), pp. 375-389.

ASSCHER 2002
L. Asscher, *Communicatiegrondrechten. Een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving* [Communications-Related Constitutional Rights] (Amsterdam, Otto Cramwinckel Uitgever 2002).

ASSCHER 2000
L. Asscher, 'Trojaans Hobbelpaard. Een analyse van het rapport van de commissie Grondrechten in het Digitale Tijdperk' [Trojan Rocking Horse. An Analysis of the CFRDA Report], *Mediaforum* (2000), pp. 228-233.

ASSCHER 1999
L. Asscher, *Constitutionele convergentie van pers, omroep en telecommunicatie* [Constitutional Convergence of Press, Broadcasting, and Telecommunications], ITeR Series Vol. 26 (Deventer, Kluwer 1999).

BERKVENS AND PRINS 2007
J.M.A. Berkvens and J.E.J. Prins (eds.), *Privacyregulering in theorie en praktijk* [Privacy Regulation in Theory and Practice] (Deventer, Kluwer 2007).

BESSELINK 2004
L.F.M. Besselink, *Constitutional Law of the Netherlands* (Nijmegen, Ars Aequi Libri 2004).

BLOK 2002
P. Blok, *Het recht op privacy* [The Right to Privacy] (Den Haag, Boom Juridische uitgevers 2002).

CFRDA 2000
CFRDA, *Grondrechten in het digitale tijdperk* [Fundamental Rights in the Digital Age] (May 2000), available at <http://www.minbzk.nl/actueel?ActItmIdt=6427>.

COMMISSIE BESLUITVORMING STEMMACHINES 2007
Commissie Besluitvorming Stemmachines, *Stemmachines, een verweesd dossier* [Voting Machines, an Abandoned File], 2nd edn. (May 2007), available at <http://www.wijvertrouwenstemcomputersniet.nl/images/3/36/Rapport_stemmachines_2e_druk.pdf>

CUSTERS 2004
B. Custers, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, diss. Tilburg (Nijmegen, Wolf Legal Publishers 2004).

CUIJPERS 2007
C. Cuijpers, 'Privacy in context', in J.M.A. Berkvens and J.E.J. Prins (eds.), *Privacyregulering in theorie en praktijk* (Deventer, Kluwer 2007).

DE MEIJ 2000
J.M. de Meij, *Grondrechten in het digitale tijdperk. Van drukpersvrijheid en briefgeheim naar communicatievrijheid en communicatiegeheim* [Fundamental Rights in the Digital Age. From Freedom of the Press and Secrecy of Letters to Communications Freedom and Secrecy of Communications] (Report for the Vereniging voor Media- en Communicatierecht 2000).

DOMMERING 2000
E.J. Dommering, 'De nieuwe Nederlandse Constitutie en de informatietechnologie' [The New Dutch Constitution and the Information Technology], *Computerrecht* (2000), pp. 177-185.

DUTCH DATA PROTECTION AUTHORITY 2007
Dutch Data Protection Authority, Letter on the draft data-retention Bill (22 January 2007), available in Dutch at <http://www.cbpweb.nl/documenten/adv_z2006-01542.shtml?refer=true&theme=purple>.

EKKER 2006
A.H. Ekker, *Anoniem communiceren: van drukpers tot weblog* [Communicating Anonymously: From Printing Press to Weblog], diss. Amsterdam (UvA) (Den Haag, Sdu 2006), available at <http://dare.uva.nl/document/19656>.

GROOTHUIS 2005
M.M. Groothuis, 'Digitalisering en Wetgeving. Preadvies voor de Nederlandse Vereniging voor Wetgeving en Wetgevingsbeleid' [Digitisation and Legislation], in L. Loeber (ed.), *Wetgeving en ICT-toepassingen* [Legislation and ICT applications] (Amsterdam, WEKA Uitgeverij 2005) pp. 9-54.

HOFMAN 1995
J.A. Hofman, *Vertrouwelijke communicatie: een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht* [Confidential Communications: a Comparative Legal Study], diss. Amsterdam (VU) (Zwolle, W.E.J. Tjeenk Willink 1995).

KOEKKOEK, ET AL. 2000
A. Koekkoek, 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 of 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).

KOOPS, ET AL. 2007

B.J. Koops, et al. (eds.), *Constitutional Rights & New Technologies, A Comparative Study Covering Belgium, Canada, France, Germany, Sweden, and the United States* (Tilburg: TILT February 2007).

KOOPS 2006

B.J. Koops, 'Should ICT Regulation Be Technology-Neutral?', in B.J. Koops, et al. (eds.), *Starting Points for ICT Regulation* (The Hague, T.M.C. Asser Press 2006) pp. 77-108, available at <http://ssrn.com/abstract=918746>.

KOOPS, ET AL. 2004

B.J. Koops, et al., *Recht naar binnen kijken. Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken* [Seeing Right Through. Exploring the Future of Inviolability of the Home and the Body and New Investigation Techniques], ITeR Series Vol. 70 (Den Haag, Sdu 2004).

KOOPS 2003A

B.J. Koops, 'Verkeersgegevens en strafrecht: een agenda voor discussie' [Traffic Data and Criminal Law: an Agenda for Discussion], in L.F. Asscher and A.H. Ekker (eds.), *Verkeersgegevens. Een juridische en technische inventarisatie* [Traffic Data, a Legal and Technical Survey] (Amsterdam, Otto Cramwinckel Uitgever 2003) pp. 59-92.

KOOPS 2003B

B.J. Koops, 'Van brieven, geschriften en onbegrijpelijke wetgeving' [Of Letters, Writings, and Incomprehensible Law], 33 *Delikt & Delinkwent* (2003), pp. 850-878.

KOOPS 2002

B.J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy* [Criminal Investigation of (Tele)communications 1838-2002] (Deventer, Kluwer 2002).

KUITENBROUWER 2000

F. Kuitenbrouwer, 'Hoe sterk zijn de digitale grondrechten' [How Strong are the Digital Fundamental Rights], *Computerrecht* (2000), pp. 172-175.

KUITENBROUWER 1991

F. Kuitenbrouwer, *Het recht om met rust gelaten te worden. Over privacy* [The Right to Be Left Alone. On Privacy] (Amsterdam, Balans 1991).

LEENKNEGT 2002

G. Leenknegt, 'The Protection of Fundamental Rights in a Digital Age', in: E. Hondius and C. Joustra (eds.), *Netherlands Reports to the Sixteenth International Congress of Comparative Law, Brisbane 2002* (Antwerp etc., Intersentia 2002) pp. 325-344.

NIEUWENHUIS 2006

A.J. Nieuwenhuis, *Over de grens van de vrijheid van meningsuiting* [Of/Crossing the Border of Freedom of Expression] (Nijmegen, Ars Aequi Libri 2006).

NOUWT, ET AL. 2000

J. Nouwt, et al., 'Grondrechten in het digitale tijdperk. Een reactie op het rapport' [Fundamental Rights in the Digital Age. A Reaction to the Report], *Nederlands Juristenblad* (2000), pp. 1321-1327.

PETERS AND DE VRÉ 2005

J. Peters and I. De Vré, 'Vrijheid van meningsuiting: de betekenis van een grondrecht in tijden van spanning' [Freedom of Expression: the Meaning of a Fundamental Right in

Times of Tension], *Preadvies voor de Vereniging voor de Vergelijkende Studie van het Recht van België en Nederland* (Deventer, Kluwer 2005) pp. 53-75.

PRINS 2004

J.E.J. Prins, 'Access to Public Sector Information: In Need of Constitutional Recognition?', in: G. Aichholzer and H. Burkert (eds.), *Public Sector Information in the Digital Age* (Cheltenham, Edward Elgar 2004) pp. 48-68.

PRINS 2006

J.E.J. Prins, 'Bruikbare Internetconsultatie' [Practicable Internet Consultation], *Nederlands Juristenblad* (2006), p. 2401.

RAAD VAN STATE 2002A

Raad van State [Council of State], Letter of 24 January 2002, available at <http://www.minbzk.nl/aspx/get.aspx?xdl=/views/corporate/xdl/page&VarIdt=109&ItmIdt=101328&ActItmIdt=12755>.

RAAD VAN STATE 2002B

Raad van State [Council of State], Letter of 25 January 2002, available at <http://www.minbzk.nl/aspx/get.aspx?xdl=/views/corporate/xdl/page&VarIdt=109&ItmIdt=101328&ActItmIdt=12755>.

REGISTRATIEKAMER 2001

Registratiekamer, 'Grondrechten in het digitale tijdperk' [Fundamental Rights in the Digital Age], letter to the Minister of Internal Affairs and Kingdom Relations (6 March 2001), available at <http://www.cbpweb.nl/documenten/adv_z2000-1221.htm>.

RIEZEBOS 1992

C. Riezebos, *Recht van petitie. Een rechtsvergelijkend onderzoek naar een juridische mogelijkheid van toegang tot het politieke systeem in Nederland en de Bondsrepubliek Duitsland* [Right to Petition, A Comparative Study] (Zwolle, W.E.J. Tjeenk Willink 1992).

SCHELLEKENS 2006

M.H.M. Schellekens, 'What Holds Off-Line, Also Holds On-Line?', in B.J. Koops, et al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners* (The Hague, TMC Asser Press 2006) pp. 51-75, available at <http://ssrn.com/abstract=952275>.

SMITS 2006

A.H. Smits, *Strafvorderlijk onderzoek van telecommunicatie* [Criminal Investigation of Telecommunications], diss. Tilburg (Nijmegen, Wolf Legal Publishers 2006).

TAK 1973

A.Q.C. Tak, *Het huisrecht* [Inviolability of the Home], diss. Utrecht (Hoenderloo, Hoenderloo's Uitgeverij en Drukkerij 1973).

VAN BALEN, ET AL. 2006

J.V. van Balen, et al., 'Bescherming van mensenrechten in een virtuele spelomgeving' [Protecting Human Rights in a Virtual Game Environment], in A.R. Lodder (ed.), *Recht in een virtuele wereld. Juridische aspecten van Massive Multiplayer Online Role Playing Games (MMORPG)* [Law in a Virtual World] (Elsevier Juridisch 2006) pp. 61-79.

VAN DE POL 2006

W. van de Pol, *Onder de tap. Afluisteren in Nederland* [Being Tapped. Eavesdropping in the Netherlands] (Amsterdam, Balans 2006).

VAN DER HOF 2007

S. van der Hof, 'The status of e-government in the Netherlands', in J.E.J. Prins (ed.), *Designing e-Government*, 2nd edn. (Alphen aan den Rijn, Kluwer Law International 2007) pp. 245-261.

VAN DER HOF, ET AL. 2004
S. van der Hof, et al., *Over wetten en praktische bezwaren, Een evaluatie en toekomstvisie op de Wet openbaarheid van bestuur* [Of Laws and Practical Objections. An Evaluation and Future Vision of the Freedom of Information Act] (Tilburg, Universiteit van Tilburg 2004).

VAN DER MEULEN 2006
B. van der Meulen, *Voorontwerp Algemene wet overheidsinformatie* [Draft Bill For a General Public Information Act], Wageningen University (2006), available at <http://www.minbzk.nl/actueel?ActItmIdt=82265>.

VAN DORST 1982
A.J.A. van Dorst, 'Het postgeheim' [Secrecy of Mail], in A.K. Koekkoek, W. Konijnenbelt and F.C.L.M. Crijns (eds.), *Grondrechten. Commentaar op Hoofdstuk 1 van de herziene Grondwet* [Fundamental Rights. A Commentary on Ch. 1 of the Revised Constitution] (Nijmegen, Ars Aequi 1982) pp. 279-297.

VAN EIJK 2005
N.A.N.M. van Eijk, *Zoekmachines: Zoekt en gij zult vinden? Over de plaats van zoekmachines in het recht* [Seek and Ye Shall Find. About the Place of Search Engines in Law], inaugural lecture Amsterdam (UvA) (Amsterdam, Otto Cramwinckel 2005).

VAN GELDER 1972
H.A. van Gelder, *Getemperde Vrijheid* [Tempered Freedom] (Groningen, Wolters 1972) pp. 154-161.

VEDDER 1998
A.H. Vedder, 'Het einde van de individualiteit? Datamining, groepsprofilering en de vermeerdering van brute pech en dom geluk' [The End of Individuality? Data Mining, Group Profiling, and the Increase of Brutal Bad Luck and Sheer Good Luck], *Privacy & informatie* (1998), pp. 115-120.

WARWICK 2002A
K. Warwick, 'Identity and Privacy Issues raised by Biomedical Implants', *IPTS Report* 67 (2002), available at <http://www.jrc.es/pages/iptsreport/vol67/english/IPT5E676.html>.

WARWICK 2002B
K. Warwick, *I, Cyborg* (London, Century 2002).

WINTER 2001
R.E. Winter, 'Vernieuwde Grondrechten' [Renewed Fundamental Rights], *Nederlands Juristenblad* (2001), pp. 297-299.