27. ANONYMITY AND THE LAW IN THE NETHERLANDS

SIMONE VAN DER HOF, BERT-JAAP KOOPS, AND RONALD LEENES

I. INTRODUCTION

Anonymity is important in current society. The feeling that anonymity is disappearing has raised the question of whether a right to anonymity exists, or whether such a right should be created given technological and societal developments. In this chapter, we address this question from a Dutch legal perspective. Our analysis of the hypothetical legal right to anonymity in the Netherlands may contribute to the overall research into the status and importance of a right to anonymity in contemporary society.

The core of this chapter consists of an overview of relevant areas in Dutch law where a right to anonymity may be found, construed, or contested. Section 2 discusses anonymity in constitutional law. Sections 3 and 4 explore the status of anonymity in criminal law and private law, respectively. Section 5 provides an overview of anonymity in public spaces. In section 6, we focus on anonymity in citizen-government relationships: service delivery, e-voting, anonymized case-law, and naming and shaming. Finally, we draw conclusions regarding the right to anonymity in current Dutch law—something that turns out to be only piecemeal, and rather weak. The chapter concludes with a reflection on these

conclusions: should a right to anonymity (or, at least, a more powerful right than the current one) be created in Dutch law?

II. ANONYMITY IN CONSTITUTIONAL LAW

A right to anonymity in the Dutch Constitution (Grondwet, hereafter: DC)[1] could be construed in several ways: as a general right to anonymity (i.e., as a separate constitutional right), or as a right subsidiary to or included in other constitutional rights, such as the rights to privacy, secrecy of communications, and freedom of expression. In the following, we explore the DC; the scope of this chapter does not allow us to discuss the equally important *European Convention on Human Rights* (ECHR)[2] as a source of constitutional rights.

A. A General Right to Anonymity

There is no general right to anonymity in the DC, and it is unlikely that one will be created in the foreseeable future. Anonymity was discussed in the late 1990s in relation to the amendment of Art. 13, DC (confidential communications).[3] After the amendment floundered in the First Chamber, the Dutch government decided to investigate a broader update of the fundamental rights in the Constitution in light of information and communications technologies.

To this aim, the Committee on Fundamental Rights in the Digital Age was instituted to advise the government. The Committee, surprisingly, considered a right to anonymity as an alternative to the right to privacy. Predictably, this was not found to be a sound alternative, anonymity being further-reaching than privacy and therefore requiring more exceptions.[4] The Cabinet, in its reaction, agreed, adding that a right to anonymity is unnecessary to substitute or complement the right to privacy. Art. 10, DC (the general right to privacy), provides sufficient protection even if anonymity were considered to be a starting point in society.[5] Moreover, the cabinet stated that knowability rather than anonymity is the norm in society, and although there is sometimes a need for anonymity, this need does

1. An English version of the Dutch Constitution is available at http://www.minbzk.nl/contents/pages/6156/grondwet_UK_6-02.pdf.

2. European Convention on Human Rights, (November 4, 1950).

3. Dutch Constitution, 1983 (*Grondwet*), Art. 13. See generally Bert-Jaap Koops and Marga Groothuis, "Constitutional Rights and New Technologies in the Netherlands," in *Constitutional Rights and New Technologies: A Comparative Study*, eds. Ronald Leenes, Bert-Jaap Koops, and Paul de Hert (The Hague: T.M.C. Asser Press, 2008), 159.

4. Committee on Fundamental Rights in the Digital Age, "Grondrechten in het digitale tijdperk" (Fundamental Rights in the Digital Age), *Kamerstukken II* 27460, 2000/01, no. 1, p.125 (appendix), http://www.minbzk.nl/actueel?ActItmIdt=6427.

5. *Ibid.*, 20.

not warrant safeguards at a constitutional level.[6] This view generally reflects academic literature.[7]

B. Anonymity as Part of Other Constitutional Rights

Although the DC lacks a proper right to anonymity, the government holds the view that anonymity often goes hand in hand with privacy and data protection.[8] (Art. 10, DC). Furthermore, other rights can "shelter" anonymity, such as the right to confidential communications (Art. 13, DC) and the right to freedom of expression (Art. 10, ECHR).[9] For example, the anonymity of a whistleblower can be protected by a journalist's right to protection of sources.[10]

In light of the "shelter" provided by these constitutional rights, there seems to be no need to establish a separate right for anonymity. However, it is unclear how far this protection stretches, for conditions for sheltering are lacking. Presumably, these conditions will be fairly strict, in light of the repeated statement by the government that identification rather than anonymity is the norm in current society:

> [A]gainst a certain desirability of anonymity, there is the fact that the functioning of our society is based, rather, on identifiability. In order to meet obligations and for law enforcement, knowability is appropriate and necessary in order to adequately protect the interests of third parties. In these frameworks, it is important that the responsibility for acts can be attributed to identifiable persons.[11]

Also, in Dutch academic literature there is little support for explicit constitutional protection of anonymity, even though anonymity itself is seen as important. The subsumption of anonymity under other constitutional provisions seems sufficient, freedom of expression being a more likely candidate than the right to privacy or the right to secrecy of communications.

---

6. *Kamerstukken II* 27460, 2000/01, no. 2, p. 44 (n. 3).

7. For an extensive discussion on the constitutional grounds for anonymity in public speech, see A. H. Ekker, *Anoniem communiceren: van drukpers tot weblog* (Den Haag: Sdu, 2006).

8. The General Right to Privacy, Dutch Constitution, 1983 (*Grondwet*), Art. 10.

9. Dutch Constitution, 1983 (*Grondwet*), Art. 13; European Convention on Human Rights, Art. 10.

10. Explanatory Memorandum, p. 5, from Letter from the Minister, October 29, 2004, with a Draft Bill and Explanatory Memorandum to amend Art. 10 Dutch Constitution (n. 8), and the advice of the Council of State, http://www.minbzk.nl/aspx/get.aspx?xdl=/views/corporate/xdl/page&VarIdt=109&ItmIdt=101328&ActItmIdt=12755; see *Voskuil v The Netherlands* ECHR November 22, 2007, for a case in point.

11. *Ibid.*, 4. Unless otherwise stated, all translations in this chapter are the authors'.

III. ANONYMITY IN CRIMINAL LAW

Anonymity plays a clear role in criminal law enforcement. First, anonymity is of interest when reporting a crime. Generally, reporting a crime is done in writing or orally, put to paper by an officer and signed by the person reporting (Art. 163 Dutch Code of Criminal Procedure (hereafter: DCCP)).[12] Signing implies identification that negatively affects people's willingness to report crimes. To stimulate crime reporting by people who fear retribution, an anonymous reporting system, "M.," was introduced in 2002; its catch-phrase, "Report Crime Anonymously" (*Meld Misdaad Anoniem*), is actively promoted in the media.[13] M. is a toll-free number (0800-7000) that can be called to report serious crimes that will then be forwarded to the police or other law-enforcement agencies with a guarantee of anonymity. The reporting system is likely to be supplemented by anonymous reporting by victims—of intimidation, for example. This requires changes in the DCPP in order for anonymous reports to be admissible as evidence in court.[14]

Second, and more important, witnesses can remain anonymous in specific situations. *The Witness Protection Act* of 1994 has introduced the concept of "threatened witness" (*bedreigde getuige*)—a witness whose identity is kept secret during interrogation at the court's order (Art. 136c, DCCP).[15] The court first has to determine whether a witness really requires anonymity, something judged to be the case only if there is reasonable fear for the life, health, security, family life, or social-economic subsistence of the witness, and if the witness has declared his or her intent to abstain from witnessing because of this threat (Art. 226a, DCCP).[16] If anonymity is granted, the witness is heard by the investigating judge (who knows the witness's identity but makes sure that the interrogation safeguards anonymity, Art. 226c, DCCP), if necessary in the absence of the defendant, attorney, and prosecutor (Art. 226d, DCCP).[17] The judge investigates and reports the witness's reliability (Art. 226e, DCCP).[18] The Act also provides a witness-protection program.[19]

---

12. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 163.

13. See http://www.meldmisdaadanoniem.nl/ (in Dutch), http://www.meldmisdaadanoniem.nl//article.aspx?id=203 (English). C.f., *Gerechtshof* [Court of Appeal] Amsterdam, February 7, 2005, LJN AS5816.

14. http://www.nu.nl/news/1118441/14/rss/Ministers_werken_aan_anonieme_aangifte_bij_politie.html.

15. Witness Protection Act (*Wet getuigenbescherming*) of November 11, 1993, *Staatsblad* 1993 (Netherlands) 603, entry into force February 1, 1994. The provision is included in the Dutch Code of Criminal Procedure as Art. 136c.

16. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 226a.

17. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 226c and 226d.

18. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 226e.

19. See Art. 226f, DCCP, the Witness Protection Decree (Besluit getuigenbescherming), and the Ruling on the Witness Protection Police Register (*Reglement politieregister getuigenbescherming*). Note that the latter implies that many identifying data of threatened

A recent change in the DCCP enables intelligence officers to testify anonymously as a "shielded witness" (*afgeschermde getuige*, Art. 136d, DCPP) in criminal court proceedings.[20] The identity of a shielded witness is kept secret in a way similar to that of a threatened witness if interests of state security or a considerable interest of the witness or another party so requires (Art. 226g and 226h, DCPP).[21] Only the Rotterdam investigating judge is authorized to hear shielded witnesses (Art. 178a(3), DCCP).[22] Testimony reports should contain no information that undermines the interests of the witness or the state and are only shown to the defense and included in the case records if the witness consents (Art. 226j(2) and (3), and 226m, DCCP).[23] A result of these far-reaching provisions is that the defense has limited possibilities to question the evidence given by intelligence officers. Here, the right to anonymity as a safeguard of state security seems to prevail over the right of the defendant to a fair trial.

A right to anonymity for suspects is absent in Dutch law. Fingerprinting suspects to facilitate identification is deemed lawful on the basis of the Police Act (Art. 2, Police Act).[24] Recent "measures in the interest of the investigation" go even further to identify anonymous suspects. They are "indirect means of coercion to force the suspect to reveal identifying data himself."[25] Among other measures, Art. 61a DCCP allows the police to take photographs and fingerprints, bring about a witness confrontation, conduct a smell-identification test, and cut hair or let it grow.[26] To facilitate identification, these measures can only be used in cases involving crime allowing custody. Anonymous suspects who are stopped or arrested can also be asked for their social-fiscal number and frisked (Art. 55b DCPP), and suspects may be held for interrogation, with the purpose of determining their identity, for a maximum of 6 to 12 hours (Art. 61, DCCP).[27]

Parties in criminal proceedings have very limited rights to remain anonymous.

In contrast, law-enforcement agencies have abundant powers to collect identifying data that bear on the overall picture of anonymity in Dutch law.

---

witnesses can be registered by the police, including old and new identity, address, description and photograph, birth data, and transport and communication data, in order to execute the witness-protection program.

20. Shielded Witnesses Act (*Wet afgeschermde getuigen*), *Staatsblad* 2006, 460 (Netherlands), in force since November 1, 2006.

21. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 226 and 226h.

22. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering)*, Art. 178a(3).

23. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 226j(2) and (3), and 226m.

24. Police Act (*Politiewet*), Art. 2.

25. According to the legislator, as quoted in C. P. M. Cleiren and J. F. Nijboer, *Tekst & Commentaar Strafvordering*, 2nd edition (Deventer: Kluwer, 1997), note 1 to Dutch Code of Criminal Procedure, Art. 61a.

26. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 61a.

27. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 55b.

As of January 1, 2006, a broad range of data-production orders have been put in place allowing any investigating officer to order the production of identifying data in case of any crime (although not misdemeanors),[28] provided that the data are processed for purposes other than personal use (Art. 126nc, DCCP). The production order can also be given in case of "indications" of a terrorist crime—a lower standard than the "probable cause" normally required for investigation (Art. 126zk, DCCP).[29] Identifying data that are processed for personal use (e.g., a citizen's address book) can be ordered by a public prosecutor for a crime for which preliminary detention is allowed (Art. 126nd).[30]

A separate rule with similar conditions (Art. 126na, 126ua, and 126zi, DCCP) allows the identification of telecommunications data, such as IP addresses.[31] Separate powers provide for the identification of prepaid-card users, because even telecom providers do not know their identity. A mandatory registration and identification scheme for prepaid-card buyers was briefly considered in the 1990s, but, this being considered too extensive, two less infringing measures were taken instead. Art. 126na(2), DCCP, allows providers to be ordered to retrieve the phone number of a pre-paid card user by means of data mining if the police provide them with two or more dates, times, and places from which the person in question is known to have called.[32] To make sure that providers have these data available, a three-month data retention obligation is in place.[33] If data mining by the telecommunications provider is impossible or overly inefficient, the police can also use an IMSI catcher—a device resembling a mobile phone base station that attracts the mobile phone traffic in its vicinity (Art. 126nb and 126ub, DCCP, Art. 3.10(4), Telecommunications Act).[34] An IMSI catcher may only be used to collect an unknown telephone number (or IMSI number), not to collect traffic data or to listen in on communications.

28. Or in cases of planned organized crime, on the basis of the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art.126uc.

29. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 126zk.

30. Or in cases of planned organized crime (Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 126ud) or of 'indications' of a terrorist crime (Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 126zl).

31. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 126na, 126ua, and 126zi.

32. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. a126na(2).

33. Art. 13.4(2) Telecommunications Act (*Telecommunicatiewet*) *juncto* Decree on Special Collection of Telecommunications Number Data (*Besluit bijzondere vergaring nummergegevens telecommunicatie*), *Staatsblad* 2002, 31, in force since March 1, 2002. Note that the Data Retention Directive, 2006/24/EC, has not yet been implemented in Dutch law. This directive requires electronic-communications providers to store traffic data for a period of 6 to 24 months. A bill is pending in Parliament with a retention period of 12 months.

34. Dutch Code of Criminal Procedure, Art. 126nb, 126ub; Telecommunications Act (*Telecommunicatiewet*), Art. 3.10(4).

IV. ANONYMITY IN PRIVATE LAW

A. Civil Proceedings

Identification is the cornerstone of the enforcement of citizens' rights in civil proceedings. Serving a summons, for example, is very difficult if a person's identity, including his or her address, is unknown.[35]

Anonymity is, however, not a priori excluded in the Dutch Civil Procedure Code (DCPC). Under exceptional circumstances (e.g., in case of genuine fear of retaliation), anonymous witness statements are admissible in civil proceedings.[36] In these cases, the identity of the witness is unknown to the other party in the proceedings but is known to the court. Statements of anonymous witnesses differ from those of regular witnesses but produce the same result; it is up to the court to weigh them in the case at hand.

Another example concerns summonses to quit vacant properties, which can be given to anonymous persons under certain conditions.[37] First, such a summons must relate to (a part of) real estate. Second, the name and the place of residence of the person(s) concerned must not be able to be identified with reasonable effort. This case obviously applies to squatters, whose identity can only be retrieved with great difficulty—if at all. Their anonymity cannot be maintained in appeal; by then, their identity must be known.

Internet Service Providers (ISPs) may be requested to identify subscribers in civil proceedings as a result of the Dutch Electronic Commerce Act.[38] In civil proceedings, the court may order ISPs to disclose the identity of users who post information on sites hosted by the ISPs.[39] The Dutch High Court confirmed this position in *Lycos v. Pessers*.[40] It decided that ISPs may have a duty to provide a third party with identity information, the non-observance of which may amount to tort,[41] even if the allegations on that person's Web site are not prima facie illegal or unjust. The following considerations are relevant:

- The possibility that the information is unjust and damaging to a third party is sufficiently reasonable.
- The third party has a reasonable interest in receiving the identity information.

35. See Dutch Civil Procedure Code (*Wetboek van Burgerlijke Rechtsvordering*), Art. 45(2).

36. See Dutch Civil Procedure Code (*Wetboek van Burgerlijke Rechtsvordering*), Art. 165ff.

37. See Dutch Civil Procedure Code (*Wetboek van Burgerlijke Rechtsvordering*), Art. 45(3) and 61.

38. Dutch Electronic Commerce Act (*Aanpassingswet elektronische handel*).

39. *Kamerstukken II* 28197, 2001/2, no. 3, p. 28. See also Art. 15(2) of Directive 2000/31/EC on e-commerce (which was, however, not implemented into Dutch law).

40. *Hoge Raad* [Dutch High Court] November 25, 2005, LJN AU4019. (LJN refers to the publication number at the Dutch official case-law publication Web site, http://www.rechtspraak.nl).

41. See Dutch Civil Code (*Burgerlijk Wetboek*), Art. 6:162.

- It is reasonably certain that less invasive possibilities of obtaining the information do not exist.
- The third party's interests carry more weight than those of the ISP and the Web site owner (if known).

In the 2006 case *Brein v. UPC*, the court added as a further requirement that the person whose identity information is requested must be, beyond reasonable doubt, the person who conducted the allegedly illegal activities.[42] In the same year, the court ruled in *Stokke v. Marktplaats* that online marketplaces do not have to provide their users' identifying information to third parties unless withholding such information would be unreasonable.[43]

B. Contract Law

Contracting parties are free to stipulate the conditions of a contract, which means they can decide not to exchange identifying information or to remain mutually anonymous. Anonymity can be purposeful, even instrumental, to the transaction process, as witnessed by the popularity of online marketplaces and brokers remunerated for the matching of the orders and offering contracts that guarantee buyer and seller anonymity (even as the broker knows the identity of both).

Anonymity in contract law is often restricted for practical and legal purposes. From a practical perspective, identity information may be required to perform contractual obligations, such as when physical delivery or payment of the products is involved (there are limited possibilities for delivering or paying anonymously). Moreover, identity information plays a role in building trust; the perceived trustworthiness of an identified business partner appears to be greater than that of an anonymous one. The risks and importance of a transaction determines the required level of assurance regarding the provided identity information. If payment is made up front, there may be no need to know the buyer's identity. In other cases, a check of the trade register will suffice. And yet, in others, digital certificates may be required to build a high level of trust. Identity data is also collected for the purpose of personalizing services and in determining the value of customers. And, furthermore, identity data is nowadays considered economically valuable—a business asset that provides businesses with incentives to not do business anonymously, even though they could.

From a legal perspective, the identity of a defaulting party may be necessary to be able to hold the party accountable. There are also legal obligations requiring

42. *Rechtbank Amsterdam* [District Court], August 24, 2006, LJN AY6903. Note that Ekker, *Anoniem communiceren* (n. 7), offers some recommendations to shape the right to anonymity in legislation, with a procedure for providing identifying data in civil proceedings and a provision in the Telecommunications Act, Ch. 10.

43. Rb. Zwolle, May 3, 2006, LJN AW6288.

online businesses to provide identity information.[44] "Identity" in this respect means the name of the natural person or of the business providing the online service.[45] In the case of businesses, the identity of the owner need not be disclosed on the Web site; this information can be obtained for a marginal fee from the trade register, something that was established long ago to provide data about businesses in order to facilitate trust in commerce.

Dutch contract law is ruled by the principle of consensualism (see Art. 3:37(1), DCivC), yet, in some instances, a certain form (e.g. a signed writing) is required, without which a contract may be void or annulled. Because, according to Dutch case law, signatures are constituted by individualization and identification under Dutch law, signed writings undercut anonymity; a cross, drawn picture or a stamp (unless equivalent to the hand-written signature) are not considered legally valid signatures.[46]

Electronic signatures are legally valid. The DCivC defines an electronic signature as data in electronic form that are attached to or logically associated with other electronic data and that serve as a method of authentication. Authentication does not necessarily mean identity authentication but may be restricted to data (e.g., the contents of the contract) authentication. In our view, the law, therefore, does not necessarily require an electronic signature to fulfill the identification function. Hence, signing electronically (contrary to what is legally allowed in respect to hand-written signatures) can be done anonymously, although possibly bringing with it less legal certainty about the evidential value such a signature holds in court.[47] The court may consider nonidentifying electronic

44. See Art. 7:46c(1a), Dutch Civil Code (*Burgerlijk Wetboek*). In this respect, this provision overlaps with the Dutch Civil Code (*Burgerlijk Wetboek*), Art. 3:15d(1a), although these provisions address different kinds of information to be provided by online businesses. Another difference between these provisions is the scope of application: the Dutch Civil Code (*Burgerlijk Wetboek*), Art. 7:46c, is not restricted to online consumer contracts but covers distance contracts more generally.

45. *Kamerstukken II* 28197, 2001/02, no. 3, p. 38.

46. S. M. Huydecoper and R. E. van Esch, *Geschriften en handtekeningen: een achterhaald concept?*, ITeR Series, Vol. 7 (Alphen aan den Rijn: Samsom Bedrijfsinformatie, 1997).

47. The principle of contractual freedom, however, also allows contracting parties to determine the evidential value of an electronic signature between them in a probative contract; see also Dutch Civil Code (*Burgerlijk Wetboek*), Art. 3:15a(6), and consideration 16 of Directive 1999/93/EC. Moreover, the law expressly leaves room for such signatures, which may, nonetheless, be legally equivalent to handwritten signatures so long as the method of authentication is sufficiently reliable in view of the purpose for which the electronic signature was used, and of all other circumstances (see Dutch Civil Code (*Burgerlijk Wetboek*), Art. 3:15a(1)). This is also called the functional approach. Compare Art. 7 of the UNCITRAL Model Law on Electronic Commerce of 1996, which also takes a functional approach with respect to electronic signatures but expressly requires a method for identifying the signer.

signatures less reliable than identifying electronic signatures or secure identifying electronic signatures.

Directive 1999/93/EC on e-signatures, on which the Dutch Electronic Signature Act is based,[48] explicitly permits the use of pseudonyms, yet both the Dutch act and the explanatory memorandum to the act are silent on this point.[49] The principle of contractual freedom also allows parties to agree to use pseudonymous certificates in their transactions. If the law stipulates a specific form of contract encompassing identified parties, pseudonymous digital certificates are not allowed, unless the identity of the certificate's holder can be obtained from the CSP when necessary. Pseudonym use may also be restricted as a result of the aforementioned information obligations regarding online services. In light of the lack of case law in the area of electronic signatures, the legal status of pseudonymous certificates and identification requirements is not entirely clear.

The identification of the signer is one of the basic requirements of advanced and qualified electronic signatures,[50] which provide strong and nearly conclusive evidential value, respectively, in court.[51]

Identification of the parties is a requirement in the regulation concerning the equalization of written and electronic contracts (see Art. 7: 227a(1d), DCivC). This provision requires the identity of the parties to be determinable with sufficient certainty. The requirement also has to be interpreted with respect to the reason why a written contract is obligatory in a certain case. If a written document is required solely to provide evidence of the contents of the document, and not identification of the parties, then identification in an electronic environment is not required (as in the offline world).

V. ANONYMITY IN PUBLIC

In recent years, the ability to move anonymously in public spaces has decreased as a result of a combination of legal and *de facto* technological developments.

Until January 1, 2005, the *Compulsory Identification Act* contained identification obligations only in special circumstances (such as during soccer matches and in public transport, when boarding without a ticket). After this date, a general identification obligation applies: Dutch citizens aged 14 and older have to show

48. Which is (mainly) incorporated in the Dutch Civil Code (*Burgerlijk Wetboek*).

49. The Dutch Minister of Justice has pointed out that special attention to the identification of individuals in an electronic environment is necessary in view of, among other considerations, identity fraud risks and the expected development of anonymous and pseudonymous interaction on the Internet. See *Kamerstukken II* 27400 VI, 2000/01, no. 2, p. 8.

50. See Dutch Civil Code (*Burgerlijk Wetboek*), Art. 3:15a(2b).

51. See Dutch Civil Code (*Burgerlijk Wetboek*), Art. 3:15a(2) and (3).

an official ID when ordered by a police officer or a public supervisor, provided this is necessary to fulfill the police task (Art. 2, Compulsory Identification Act *juncto* Art. 8a, Police Act 1993).[52] Failure to comply is punishable with a fine of up to €3,350 (Art. 447e, Dutch Criminal Code, henceforth DCC). The extended compulsory identification was somewhat controversial when introduced; for example, the group ID Nee ("ID No") campaigned against it. This group also runs an Identification Abuse Hotline.[53] Nevertheless, Parliament accepted the act without much opposition. The effect of the general compulsory identification on public safety has not been empirically studied so far, but there are indications that the law is often used to fine people committing banal offenses, or found in apparently "suspect" circumstances. For example, the police ordered a man who sat idly on the window ledge of a post office to show his ID.[54]

Although less omnipresent than in the UK, CCTV surveillance is constantly increasing. Different laws apply to camera surveillance depending on the context in which it is used and the person or organization responsible. According to Art. 151c, Municipal Act, the city council can authorize the mayor to decide upon camera surveillance in public areas for purposes of public order for a specified period of time.[55] In case of a justified interest (protection of employees, customers, and property), private parties, such as employers and shop owners, may also install cameras for surveillance at the work place, in stores, and so on, so long as these do not cover public areas (e.g., a whole street or public square) and do not infringe upon privacy interests (e.g., by monitoring private places). Camera surveillance at the work place requires the consent of the employees' council (Art. 27(1l), Employees' Councils Act).[56] In all instances, camera surveillance must be clearly indicated at the respective locations. Secret camera surveillance of individuals in public and private places is illegal pursuant to Art. 441b and 139f, DCC respectively.[57]

The public prosecutor can order camera surveillance without the recording of confidential information (monitoring) in criminal investigations on suspicion of a crime (Art. 126g(3), DCCP).[58]

In addition to camera surveillance, other anonymity-decreasing technologies are used or experimented with in different areas. For example, shopping areas in Amsterdam and Utrecht are experimenting with facial recognition technologies aiming at identifying shoplifters. The city of Groningen and the Netherlands

52. Compulsory Identification Act (*Wet op de identificatieplicht*). Extended Compulsory Identification Act (*Wet op de uitgebreide identificatieplicht*), *Staatsblad* 2004, 300.

53. See http://www.id-nee.nl/English.html.

54. *Algemeen Dagblad* March 2, 2007, see http://www.id-nee.nl/Actueel.html#499.

55. Municipal Act (*Gemeentewet*), Art. 151c.

56. Employees' Councils Act (*Wet op de ondernemingsraden*), Art. 27(11).

57. Dutch Criminal Code (*Wetboek van Strafrecht*), Art. 441b and 139f.

58. Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*), Art. 126g(3).

Railways, amongst others, have installed systems to detect aggressive behavior. Soccer club ADO Den Haag has introduced a crowd control system to help locate hooligans (relying on facial recognition at the entrance and in the stadium and microphone detection of aggressive or otherwise undesirable speech).

Furthermore, a public transport chipcard (OV-chipkaart) is being introduced in the Netherlands that facilitates massive tracking and tracing of travelers throughout the country. The card scheme allows for anonymous and personalized cards. The former option is more expensive and excludes card usage for age discounts, season tickets, and so on.

VI. ANONYMITY IN CITIZEN-GOVERNMENT RELATIONSHIPS

A. Service Delivery

Citizens do not have an explicit right to anonymity with respect to public service delivery, but the rule of law requires the government to have specific legal grounds to oblige citizens to identify themselves. If there are no such legal grounds, citizens actually have a right to be or stay anonymous in their relationship with the government, or at least have no obligation to identify themselves.

Irrespective of the requirement for legal grounds, identification plays a key role in government-citizen relationships regarding service delivery, because entitlement to particular services is sometimes hard to establish without having access to personal data contained in government records. This requires identification of the individual.

Anonymous interaction with the government is increasingly difficult. A recent research report discusses two important causes: the use of new technologies (CCTVs, data-mining, data-sharing, and data-linking) and the ongoing informatization of government (and private-sector) administrations. As a result, new kinds of personal information are collected and used, and on a bigger scale than before.[59] Although the report focused on the impact of trends in criminal investigations and national security on ordinary (nonsuspect) citizens, similar patterns can be expected in public service delivery. The newly introduced biometric passports, which allow automatic identity verification, may spur more obligations to identify for services. Personal data is increasingly linked in order to detect fraudulent use of government benefits, for optimizing children's aid, and for providing proactive and personalized public services.

A crucial aspect of the public sector identification web is likely to be the recently introduced Citizen Service Number (Burger Service Nummer; hereafter CSN), which will be used in all communications between citizen and public

59. A. Vedder et al., *Van privacyparadijs tot controlestaat? Misdaad—en terreurbestrijding in Nederland aan het begin van de 21ste eeuw* (The Hague: Rathenau Instituut, February 2007), available at http://www.rathenau.nl/showpage.asp?steID=1&item=2097.

administration. After decades of opposition to a unique identification number for citizens in the Netherlands tracing back to the aftermath of World War II, the legislature adopted the CSN with little discussion in July 2007.[60] The name CSN is a misnomer, because it is a registration number rather than an instrument to improve service delivery for citizens. The CSN facilitates the sharing and linking of personal data across the public sector and may turn out to be an important inhibiter of anonymity. The CSN consists of the existing social-fiscal number but may be used by many more public entities and in fact replaces other sector-specific numbers.

Most public services, especially transaction services, require citizens to prove their identity, whether actively (by showing an ID card or using a digital identifier called DigiD) or passively (by, for example, using their postal address as recorded in the Municipal Registry). Information services can usually be obtained anonymously, although even in this sector numerous instances exist in which individuals have to identify themselves in order to receive public-sector information. The Dutch Government Information (Public Access) Act 1991 embraces the principle that public information should be public to all.[61] In practice, public-sector information is sometimes disclosed selectively (e.g., for scientific purposes only), implying the identification of the requester.[62]

From an identification perspective, conventional and electronic communications, in principle, should adhere to the same requirements.[63] The emerging electronic identification infrastructure for electronic public service delivery and the potential for the eNIK (an electronic national identity card, which was expected to be deployed in 2008 but the status of which is presently unknown) to introduce advanced electronic signatures therein will likely promote secure identification in public service delivery.[64] Because of the limited possibilities for using pseudonymous digital certificates, these ID schemes could increase citizen identification.

60. *Staatsblad* 2007, 288.

61. Dutch Government Information (Public Access) Act 1991 (*Wet openbaarheid van bestuur*).

62. S. van der Hof et al., *Over wetten en praktische bezwaren, Een evaluatie en toekomstvisie op de Wet openbaarheid van bestuur* (Tilburg: Tilburg University, 2004), 19.

63. Electronic communications between citizens and government are regulated by the Act on Electronic Government Communications (*Wet elektronisch bestuurlijk verkeer*), which has amended the General Administrative Law Act (*Algemene Wet Bestuursrecht*). Pursuant to this law, electronic messages should be as reliable and confidential as conventional communications can be (functional approach). Additionally, the electronic signature provisions in the DCivC apply to electronic communications within the public sector.

64. C.f. B. J. Koops, H. Buitelaar, and M. Lips, eds., *D5.4: Anonymity in electronic government: a case-study analysis of governments' identity knowledge*, FIDIS report, May 2007, available at http://www.fidis.net.

B. e-Voting

Anonymity in voting is closely related to secrecy of the vote, which is an important principle in Dutch democracy. Public elections should reflect the voters' choices and should be free from undue influence. Secrecy and privacy are, therefore, essential characteristics of public elections. Secrecy of the vote is established in Art. 53(2), DC, and is further detailed in the Voting Act for the different Dutch types of casting votes: ballot boxes (Art. J 15), voting machines (Art. J 33), and postal votes (Art. M 7).[65]

Although voting secrecy could be seen as optional—the voter may opt to vote anonymously—it is usually taken as a strict mandatory lawful duty, meaning that voter anonymity has to be guaranteed (by the state) for all voters.[66] The effect is that voters may tell anyone whom they voted for without being able to prove their claims.

Interestingly, voting secrecy is traditionally guaranteed by social control. The polling station officials observe that voters enter the voting booth alone, where they can cast their vote without anyone looking over their shoulder. The ballot paper is subsequently deposited in an opaque box.

Electronic voting machines have been in operation in Dutch polling stations since the early 1980s. The voting secrecy is safeguarded in the same manner as for paper ballots. These electronic voting machines have recently caused controversy. The machines leave no paper trail, nor is their software open (or certified), which basically means that only the manufacturer knows what the machines actually count.[67] Also a group of concerned people, WijVertrouwenStemcomputersNiet ("We don't trust voting machines"), have proven that the votes cast in the machines used in the Netherlands can be remotely monitored through interception of residual screen radiation, which undermines the secrecy of the vote and therefore affects the anonymity of the voting process.

Voter anonymity is even more problematic in postal and Internet voting. Postal voting is an option for Dutch nationals living or residing abroad at the time of general elections (Art. M 1 Voting Act).[68] The voter can be coerced, and the voting ballot inspected, before being sent to the election officer. Furthermore, the vote can be linked to the voter because it is sent with a separate letter stating that the voter personally cast her vote. Therefore, voter anonymity depends on the election officers who receive the postal votes.

---

65. Dutch Constitution (*Grondwet*), Art. 53(2); Voting Act (*Kieswet*), Art. J 15, J 33 and M 7.

66. See H. Buchstein, "Online Democracy, Is It Viable? Is It Desirable? Internet Voting and Normative Democratic Theory," in *Electronic Voting and Democracy—A Comparative Analysis*, eds. N. Kersting and H. Baldersheim (London: Palgrave, 2004).

67. See http://www.wijvertrouwenstemcomputersniet.nl/English.

68. Dutch Voting Act (*Kieswet*), Art. M 1.

Since the late 1990s, the Dutch government has actively pursued the introduction of Internet voting. Experiments with Internet voting for expatriates were conducted during the Dutch elections for the European Parliament in 2004 and the November 2006 general elections. Internet voting is even more problematic than postal ballots are. Not only is family-voting unavoidable, but also the voting process itself is highly opaque. An interesting question regarding postal ballots and Internet voting is whether the European Court of Human Rights will sanction them if challenged in the light of Art. 3, protocol 1, of the *European Convention on Human Rights* (secrecy of the vote).[69]

C. Anonymized Case-Law and "Naming and Shaming"

Anonymity, for privacy and data-protection reasons, features in administrative law regarding the publishing of court cases. The official court cases Web site, www.rechtspraak.nl, generally anonymizes cases by replacing names with neutral indications such as "plaintiff" or "defendant." Names of professionals (such as judges, lawyers, interpreters, and expert witnesses) are not, however, anonymized. Names of legal persons, such as companies, are also published, unless these are directly linkable to individual persons.[70]

However anonymous the cases thus published may be, there are several legal provisions that require complete publication of a case, which may be viewed as a form of "naming and shaming." Examples are

- Fines or penalties delivered in competition cases (implying that a case is open for inspection at the Dutch Competition Authority (NMa)) must be published in the official journal *Staatscourant* (Art. 65, Competition Act);
- The Netherlands Authority for the Financial Markets (AFM) can publish the names and addresses of people fined for violating financial-market legislation (see, for example, Art. 48m, Stock Trade Supervision Act). Moreover, the AFM can, in order to "promote compliance with the Act," apart from imposing possible fines, publish facts that violate the Act (Art. 48n);
- The yearly publishing in the *Staatscourant* of a list of companies who have submitted insufficient emission rights in the context of environmental-law obligations (Art. 18.16p(1), Environmental Protection Act).[71]

Whereas these "naming sanctions" largely affect legal persons, a similar provision affecting citizens can be found in criminal law. The publication of a criminal sentence can be ordered in criminal cases as an additional

69. L. Pratchett, *The implementation of electronic voting in the UK* (London: Local Government Association, 2002).

70. See http://www.rechtspraak.nl/Over+deze+site/ under "Anonimiseringsrichtlijnen."

71. Competition Act (*Mededingingswet*), Art. 65; Stock Trade Supervision Act (*Wet toezicht effectenverkeer*), Art. 48m; Environmental Protection Act (*Wet milieubeheer*), Art. 18.16p(1).

sanction (Art. 9(1)(b)(3) DCC) or as an alternative sanction (Art. 9(1)(b)(3) *juncto* Art. 9(5), DCC); this is also possible with economic offences (Art. 7(g), Economic Offences Act).[72] Whether publishing a criminal verdict with the name of the convicted person is justified depends on the kind rather than the seriousness of the crime. For example, it may be a useful response to convictions for selling health-threatening food, death by neglect in official functions, embezzlement, or fraudulent bankruptcy. The sanction of publishing is, however, hardly ever given in practice.[73]

VII. CONCLUSION

A. Does a Right to Anonymity Exist in Dutch Law?

Our overview clearly shows that no general right to anonymity exists in Dutch law. Rather, identification is the default. In criminal law, this is unsurprising in light of the obvious importance of identification in crime detection and prosecution. In civil and administrative law, however, anonymity might have been expected to be more important than it actually is. After all, there is often no intrinsic need to know the identity of someone engaged with in a legal act.

In today's society, however, with its pervasive ICT infrastructures that increasingly facilitate the performance of legally relevant acts at a distance, the trust that often used to come with face-to-face relationships must be reconstructed by other means. Identification is a prime tool for re-establishing trust between unfamiliar parties who often lack other indicators of the other party's likelihood of keeping his or her part of the deal. This may at least partially explain why anonymity currently does not feature in the legal framework for e-commerce and e-government.

On the contrary, powerful identification infrastructures are built in the private sector, with e-signatures and PKIs, and even stronger ones in the public sector, with the Citizen Service Number and the eNIK. Furthermore, the legal frameworks for these infrastructures are far from sympathetic to anonymity: the possibility of pseudonymous e-signature certificates is not embedded in Dutch law (and is even prohibited in e-government relationships), and the CSN will be used across all areas of government. Moreover, identification duties are on the rise, with recent laws requiring e-commerce providers and—most importantly—citizens aged 14 and older, in general, to identify themselves when requested by an officer. Another significant detail is that many "naming and shaming" provisions, particularly in

72. Dutch Criminal Code (*Wetboek van Strafrecht*), Art. 9(1)(b)(3) and Art. 9(1)(b)(3) *juncto* Art. 9(5); Economic Offences Act (*Wet op de economische delicten*), Art. 7(g).

73. C. P. M. Cleiren and J. F. Nijboer, *Tekst & Commentaar Strafrecht* (Deventer: Kluwer, 2000); Dutch Criminal Code (*Wetboek van Strafrecht*), Art. 9 (n. 3).

administrative law, were introduced over the past years, adding to the significance that modern society apparently attaches to identification in public.

This is not to say that anonymity is non-existent in Dutch law. There are various legal fields in which forms of anonymity rights exist. Occasionally, anonymity is the default (in voting, and official case-law publication) or a strong right (in relation to freedom of expression). More often, however, a right to anonymity is the exception to the rule: threatened witnesses, both in civil and criminal cases, can testify anonymously—a right which, ironically, can be claimed both by organized criminals and by intelligence officers—and contracts can be concluded anonymously.

The rationale underlying these anonymity rights is diverse. An intrinsic reason for protecting anonymity clearly seems absent. In all fields where some form of anonymity right exists, this right is instrumental in furthering the purpose of the law and policy in those fields. Anonymity is an important tool for fair voting procedures, for stimulating the public exchange of (unpopular) ideas to enhance the freedom of expression and of thought, and, sometimes, for protecting the life and limb of persons at risk. Anonymity thus is a servant to several masters.

Altogether, we conclude that in Dutch law, there is merely a very piecemeal and rather weak right to anonymity. Only in some very specific areas of law is there a strong claim to anonymity, but the default position in Dutch law is that identification is preferred and, increasingly, mandated.

B. Should a Right to Anonymity Be Created in Dutch Law?

If a substantial right to anonymity does not exist, should it be created? After all, the discussions in the Netherlands about anonymity (for example, in the debate over digital constitutional rights) indicate that there is some reason to cherish anonymity in the current, ICT-pervaded society—if only to a certain extent.

The key questions are whether the need for anonymity is significant enough for a full-bodied right to anonymity, and if so, how and to what extent such a right should be defined. We think there is insufficient reason to answer the first question, generally, in the affirmative. There is some need for anonymity in numerous situations, and this need is perhaps growing, but the contexts in which anonymity plays a part are so diverse, that speaking of "a" right to "anonymity" is hardly justified as such. Instead, the question should be asked in terms of which contexts, sectors of society, and legal areas there exists a substantial need to protect anonymity nowadays.

Ekker, for example, has pleaded for a right to anonymous communications, which should take the form of a procedure for providing identifying data in civil proceedings and a provision in the Telecommunications Act.[74] Much pleads in favor of this suggestion, for (tele)communication is nowadays a crucial enabler for almost all activities. People increasingly generate traces when communicating

74. Ekker, *Anoniem communiceren* (n. 7).

via ICT—not only on the Internet, but also with mobile telecommunications, which increasingly have to be stored as a result of regulation such as the Data Retention Directive. The variety of parties that can somehow access, legitimately or unlawfully, these traces, combined with the deficit of data-protection law to effectively limit the wide-scale processing of personal data in practice, warrants the conclusion that privacy is slowly disappearing.[75] To stop this process, a right to anonymity, rather than reliance on data-protection law only, could be a valuable add-on in an integral effort to save privacy. A right to anonymous communications would also foster other rights, not least the freedom of expression in an online environment. Naturally, such a right could and should not be absolute: it would only be relative to certain parties and could be infringed when sufficient interests required identification. But the important added value would be that the default position would be reversed: rather than the current assumption of identification, there would be an assumption of anonymity, revoked only when necessary.

A right to anonymous communications—something worthy of much more elaboration than we may present here—is one example of an area in which a right to anonymity makes sense. When surveying the developments currently taking place in ICT, and also in DNA fingerprinting and bio-banking, we see that large-scale identification infrastructures are being built.[76] Experience shows that infrastructures persist: they can be adapted or rebuilt, but they are rarely removed. This means that we should carefully analyze the consequences of large-scale identification, for these will become the norm in the coming decades. A result may well be that in situations where previously people used to act anonymously, identification will be a standard instead, whether mandatorily (because of legal obligations) or in practice (because technology just happens to implement identification). And because anonymity used to be taken for granted in such situations—buying groceries in a supermarket, walking in another city, travelling by train, visiting a soccer match—there is no history of a "right to" anonymity in these cases: if something is natural, there is no need to protect it by law. Now that the world is changing, with anonymity no longer a matter of course, it is time to consider embedding the protection of anonymity in law for those areas of social life that entail no intrinsic need for identification.

Although anonymity hardly has a history as a right, it may well have a future as a right, and in many more fields than is the case today. It is perhaps one of the

75. See B. J. Koops and R. E. Leenes, "'Code' and the Slow Erosion of Privacy," *Michigan Telecommunications & Technology Law Review* 12, no. 1 (2005): 115–188, http://www.mttlr.org/voltwelve/koops&leenes.pdf.

76. See also Koops, Buitelaar, and Lips, *Anonymity in electronic government*, 76–77 (n. 42).

few available "tools of opacity"[77] that ensure an acceptable balance between the powerful and the power-poor in today's technology-pervaded, identification-driven society.

77. See S. Gutwirth and P. de Hert, "Privacy and Data Protection in a Democratic Constitutional State," in *D7.4: Implications of profiling practices on democracy and rule of law*, eds. M. Hildebrandt et al., FIDIS report, September 2005, available at http://www.fidis.net, 11–28.