Universiteit Utrecht

European Working Group on Labour Law 2017

Privacy in labour law

21 – 24th of March 2017

Dutch Report

Annique Slagter

Lara Thomae

Linda van der Vaart

Laura de Vries

Table of contents

1. Privacy in the Dutch legal system

"Right to privacy": Is a right to privacy recognized in your system of law (apart from art. 8 ECHR and art. 7 and 8 of the Charter of Fundamental Rights of the European Union [CFR]), i.e. in the constitution, in statutes, in national case law? If there is no explicit recognition of such a right, how are elements of it protected in your legal system? What has the role of the right to privacy in art. 8 ECHR and art. 7, 8 EU-CFR been in your domestic legislation and case law?

The Dutch legal system contains a multitude of rules regarding privacy, both general rules and rules specifically tailored to labour law. In the first part of this report, we will provide a brief overview of the general rules with regard to privacy in Dutch law. This section will contain, first, an answer to the question which Dutch rules exist. Second, this section will discuss the way in which Dutch legislation and case law deal with the European right to privacy – that is, Articles 8 ECHR and Articles 7 and 8 CFR.

1.1. Right to privacy in Dutch legislation

1.1.1. Constitution

The right to privacy is most generally and fundamentally set out in Article 10 of the Constitution:

1. *Everyone shall have the right to respect for his private life, without prejudice to restrictions laid down by or pursuant to Act of Parliament.*
2. *Rules to protect private life 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.*

This provision deals with several aspects of privacy, or "private life" as the Dutch version of the article more aptly refers to ('*persoonlijke levenssfeer*'). "Private life" refers traditionally to the right to inviolability of the home, but it has a wider scope, including for example private conversations outside of the home and numerous aspects of family life.[1] The right to a private life has been defined as the series of situations in which a person wishes to freely be himself.[2] A narrow definition has deliberately been rejected by the legislator, acknowledging that the doctrine of privacy is constantly evolving.

It is clear that the definition of private life also extends to situations in the workplace.[3] This does not, however, mean that every situation in the workplace is covered by Article 10. The nature and extent of the intimacy of the specific circumstances are essential for the assessment whether the right to privacy has been breached.[4] Purely commercial or business situations do not normally fall under the scope of Article 10. For an employee, this means that for example a conversation with his employer or a co-worker discussing no intimate personal details will not be classified as a

[1] *Parliamentary paper* II, 13 872, p. 39.
[2] *Parliamentary paper* II 1975/76, 13 872, nrs. 1-5 p. 41.
[3] *Parliamentary paper* II 1976-1977, 13 872, nr. 7, MvA, p. 35.
[4] Schedule to *Proceedings* II, 1975–1976, 13 872, nrs. 1–5, p. 41.

situation falling under Article 10.[5] Article 10 has indirect horizontal effect and can therefore be invoked by the employee against the employer, for example through the use of the principle of good employer practices (Article 7:611 Dutch Civil Code (DCC)).

The right to privacy is furthermore elaborated in subsequent articles in the Constitution, dealing with for example integrity of the person and of the home. For the purposes of this report, Article 13 is especially important. This provision deals with the privacy of letters ("*briefgeheim*") and of the use of telephone and telegraph. This provision states that:

1. *The privacy of letters 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 shall not be violated, except in the cases laid down by Act of Parliament, by or with the authorization of those designated for the purpose by Act of Parliament.*

While it is not completely clear whether Article 13 has direct horizontal effect, it is clear that the general principle of law laid down in it has found its way into many horizontal relationships. Application of the principle in these horizontal relationships will normally take the form of a balancing of interests.[6]

Article 13 is, in its current literal form, slightly outdated, referring in the first paragraph to post (letters) and in the second paragraph to telephone and telegraph. The lack of a specific mention of electronic correspondence has led to uncertainty whether this is covered by this provision. Therefore, there has been a legislative endeavour to update Article 13 to cover new technology.[7] The proposed provision reads:

1. *Everyone shall have the right to respect of his privacy of correspondence and telecommunication.*
2. *Restriction of this right shall be possible only in cases laid down by Act of Parliament with authorization of the court or, in the interest of national security, by or with the authorization of those designated for the purpose by Act of Parliament.*

The endeavour to amend the constitution has, however, proven to be a lengthy process, and adoption of the proposal has been postponed.[8]

1.1.2. Personal Data Protection Act

It is laid down in Article 10 of the Constitution, that the Parliament has the right to adopt Acts with regard to the recording and dissemination of personal data and the rights of persons to be informed of such recorded data. There are several laws in which the legislator has carried out this assignment. An important example of this, which has horizontal effect and is therefore also directly applicable

[5] See for example Dutch Supreme Court 16 October 1988, ECLI:NL:HR:1998:ZC2693 (*Driessen/Van Gelder*).
[6] J.M.J.W. Dreessen, *Commentary on article 13 Constitution* 2008, par. C.4.
[7] See *Parliamentary paper* II 2013/14, 33989, 1 – 3.
[8] Most recently (*Parliamentary paper* II 2013/14, 33989, 9), the Minister of the Interior and Kingdom Relations has stated in a letter to the House of Representatives dated 9 November 2016 that the legislative proposal will be postponed pending another legislative proposal.

in the relationship between employer and employee, is the Personal Data Protection Act 2001 (*Wet bescherming persoonsgegevens*). This Act implements the European Data Protection Directive[9] into Dutch law.

The Personal Data Protection Act (*PDPA*) applies to: "the fully or partly automated processing of personal data, and the non-automated processing of personal data entered in a file or intended to be entered therein".[10] This provision contains several aspects that require further examination.

1. *Personal data*: This includes any information concerning an identified or identifiable natural person.[11] It covers both written information and other types, such as video and audio taping.[12] Furthermore, it may cover information that is not directly about the person, but about a product or process which can be used to inform oneself about that person – such as phone numbers, number plates and postal codes. Information be may covered by the act if it is not about an identified but an identifiable person, which means that it can be used to determine the identity of the person without a disproportionate effort. In for example a small firm, it might be easy to use information collected about employees to identify the employee in question.[13]

2. *Processing*: This is any operation or set of operations which is/are performed upon personal data.[14] This does not cover fully automated processing of data, but does not necessarily require human intervention either – semi-automated processing, in which human intervention is *possible*, is covered by the PDPA.

3. *File*: This is "any structured set of personal data, whether centralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria and relates to different persons".[15]

If certain information falls under this scope, the PDPA contains principles determining under what conditions it may be processed. Pivotal is Article 8, which contains the grounds for permissible processing of data, including, *inter alia*, express permission, necessity for compliance with a legal obligation and "legitimate interests". With respect to the latter, the processor must carry out a balancing exercise, answering the following questions:[16]

- Is there an actual interest justifying the processing of personal data?
- Will the processing have a breach of interests of fundamental rights of the concerned subject as a result and, if so, should the processing not be carried out?
- Can the aim be reached in a different way?

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L 281/31.
[10] Article 2, paragraph 1, of the Personal Protection Data Act; this is in line with Article 3, paragraph 1, of the Data Protection Directive 95/46/EC.
[11] Artikel 1 sub a PDPA.
[12] H.H. de Vries, 'Commentary on Article 1 PDPA', in: *Tekst & Commentaar Telecommunicatie- en privacyrecht* 2016, par. 2.
[13] I.J. de Laat & D.J. Rutgers, *Commentary on Article 1 PDPA* 2016, par. C.2.1.
[14] Article 1 sub b PDPA.
[15] Article 1 sub c PDPA.
[16] I.J. de Laat & D.J. Rutgers, *Commentary on Article 1 PDPA* 2016, par. C.2.2.

- Is the processing proportionate to the aim pursued?

If there is a ground for processing, and the operation is furthermore carried out in a proper and accurate manner, and the information is collected for specified, explicit and legitimate purposes, the processing will normally be deemed permissible.[17] In the next chapter, the permissibility of a number of specific activities by the employer will be discussed in more detail.

1.2. ECHR and CFR in the Dutch legal system

1.2.1. ECHR

While the Dutch legal system thus has an extensive complex of privacy rules in place, the European provisions on privacy, in particular Article 8 ECHR and Articles 7 and 8 CFR, also have an impact. Article 8 ECHR, specifically, has a wide applicability in the Dutch legal system. In fact, it has been argued that Article 10 of the Dutch Constitution has limited use for individuals, as Article 8 is more all-encompassing,[18] and allows for positive obligations as well. Furthermore, unlike Article 13 of the Constitution, the European Court of Human Rights (ECtHR) has explicitly ruled that privacy of correspondence also extends to e-mails and internet usage.[19]

As early as 1987, the Dutch Supreme Court (*Hoge Raad*) has accepted horizontal effect of Article 8 ECHR.[20] There is some debate as to whether this effect is direct or indirect. If it is direct, an employee can rely on a breach of Article 8 in court. By contrast, if it is indirect, it may only be used to flesh out other norms, which may then form the basis for the claim. Regardless of the answer to these questions, labour law allows that the employee can use this provision against infractions committed by their employer. The infraction may for example be the basis for a tort case, in which article 8 ECHR is used to flesh out the open norm of Article 6:162 DCC (the general tort provision in the civil code), or a case on the basis of the principle of good employer practice (Article 7:611 DCC).[21]

In this respect, it is especially interesting to see how Dutch courts deal with potential justifications for infringements of Article 8 ECHR. Under Article 8, paragraph 2 of the ECHR, interferences in fundamental rights can be justified if the following conditions are fulfilled.[22]

1. The interference has taken place in accordance with the law;
2. The interference is necessary in a democratic society;
3. The interference serves a legitimate purpose, namely of the following: national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others;
4. The interference is proportionate to the legitimate aim pursued.

[17] Articles 6 and 7 PDPA.
[18] I.J. de Laat & D.J. Rutgers, *Commentary on Article 1 PDPA* 2016, par. C.1.3.
[19] ECtHR 03-04-2007, nr. 62617/00 (*Copland v. United Kingdom*), par. 41.
[20] Dutch Supreme Court 09-01-1987, ECLI:NL:HR:1987:AG5500 (*Edamse bijstandsmoeder*).
[21] I.J. de Laat & D.J. Rutgers, *Commentary on Article 1 PDPA* 2016, par. C.1.2; A.H. Pool, *Particuliere recherche door werkgevers. De beoordeling van recherchegedrag van werkgevers in het Nederlands recht in het licht van artikel 8 EVRM* (diss. Radboud Universiteit Nijmegen), 2014, p. 47.
[22] See e.g. S. Greer, *The exceptions to Articles 8 to 11 of the European Convention on Human Rights* (Human Rights File No. 15), Strasbourg: Council of Europe Publishing 1997.

The first question is whether interferences by an employer in the private life of an employee have a basis in law. As a general rule, "law" in this context may be interpreted broadly, as long as the provision is accessible to the employee and sufficiently precise.[23] As a result, a number of legal bases can be identified.[24]

- The employment contract, if it contains specific clauses allowing certain measures;
- A substantiated suspicion of the employer;[25]
- The employer's right to issue instructions (article 7:660 DCC), in so far as the measure is connected to these instructions;
- Customary practices.

Whether the other conditions of Article 8, paragraph 2, ECHR are fulfilled depends on the circumstances of the specific case. We will therefore not make any general remarks as to these criteria at this point.

1.2.2. CFR

The EU Charter of Fundamental Rights (CFR) also contains provisions regarding the right to privacy, which are directly applicable in the Dutch legal system. Specifically, Article 7 deals with the respect for private and family life and Article 8 lays down that "everyone has the right to the protection of personal data concerning him or her". According to paragraph 2 of Article 8, personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. This reflects the same principle as the European Data Protection Directive (and consequently the PDPA).

The CFR is applicable in vertical relations (between State and citizen) as a consequence of Article 51 CFR, which states that the provisions "are addressed to the institutions and bodies of the Union (…) and to the Member States only when they are *implementing Union law*" (emphasis added). This has been broadly interpreted in case law, equating the implementation of Union law with "acting within its scope".[26] While some scholars have held that the CFR must be held to have horizontal direct effect, as well, the practical implications on a horizontal level in the Netherlands have been small. Most of the case law concerning privacy interferences by employers has been decided upon the basis of either national law or Article 8 ECHR.

[23] S. Greer, *The exceptions to Articles 8 to 11 of the European Convention on Human Rights* (Human Rights File No. 15), Strasbourg: Council of Europe Publishing 1997, p. 10 – 11.
[24] A.H. Pool, *Particuliere recherche door werkgevers. De beoordeling van recherchegedrag van werkgevers in het Nederlands recht in het licht van artikel 8 EVRM* (diss. Radboud Universiteit Nijmegen), 2014, p. 97 – 107.
[25] Acknowledged in Dutch case law in Dutch Supreme Court 27 April 2001, ECLI:NL:HR:2001:AB1347 (*Wennekes Lederwaren*); the ECtHR has acknowledged the same legal basis for interference in ECtHR, *Karin Köpke against Germany*, Application no. 420/07, Judgment of 5 October 2010.
[26] Case C-617/10 *Åklagaren v Hans Åkerberg Fransson*, judgment of 26-02-2013 (not published).

2. Surveillance of employees at work

In what cases and in which form is surveillance of employees at work legal and in which cases/forms is it prohibited? Please consider: (secret) video and audio taping, monitoring of computer and email activities, GPS tracking, personal searches etc. What are the relevant sources of law?

Surveillance measures fall, generally, under the scope of Article 10, paragraph 2, of the Constitution, as discussed in the previous chapter. More specifically, the Personal Data Protection Act will often be applicable to these measures, as surveillance measures often entail the processing of personal data.[27] In the previous paragraph, we have set out the scope of this Act and described the conditions under which the collection and processing of personal data are lawful. In this chapter, we will describe how this relates to several specific measures, namely: videotaping (camera surveillance), audio taping/telephone conversations, monitoring of computer and email activities, GPS tracking and personal searches. Social media, as the subject of question 8, will be dealt with in chapter 8.

The Personal Data Protection Act is not the only relevant source of law in this context. The employer's behaviour is also subject to the rule that he has to act as a good employer, as is codified in the Civil Code (Article 7:611 DCC). Furthermore, an employer might need consent by the Work's Council to adopt a certain scheme. This requirement of consent will be discussed in the next chapter in order to answer question 3.

This chapter will only address whether certain surveillance measures are allowed, or constitute a breach of fundamental rights or other legal norms. Whether any evidence obtained through an unlawful surveillance measure can be used in court, for example in a dismissal case, is the subject of chapter 6 of this report.

2.1. Camera surveillance

Camera surveillance by the employer may serve a legitimate purpose and it is therefore not always forbidden. However, it is only allowed under specific circumstances. Importantly, a balancing of interests between, on the one hand, the aim of the employer, and on the other hand, the privacy of the employee is always required. This is especially the case if the camera surveillance is hidden: in that case, the interest of the employer must far outweigh the right to privacy of the employee if it is to be allowed.[28]

2.1.1. The privacy test

As the PDPA applies to camera surveillance, a ground for permissible processing of personal data is required.[29] This can be the consent of the employees, but it is generally believed that due to the unequal power balance between employer and employee unequivocal consent cannot normally be

[27] C. Loonstra & W.A. Zondag, *Arbeidsrechtelijke themata*, Den Haag: Boom Juridische uitgevers 2015, par. 8.3.
[28] M.C.H.I. van der Dussen & M.P.E. Oomens, "Gebruik van (verborgen) camera's op de werkplek", *ArbeidsRecht* 1998/20.
[29] The PDPA applies to videotaping, H.H. de Vries, 'Commentary on Article 1 PDPA' in: *Tekst & Commentaar Telecommunicatie- en privacyrecht* 2016, par. 2.

given. A more likely ground under the PDPA is the "legitimate interest" of the employer.[30] There are several scenarios in which the use of cameras to survey employees may be legitimate: for example, to survey the conduct of an employee, or a legitimate need to search for suspect behaviour.[31] As mentioned above, this legitimate aim must be weighed against the interests of the employee, carrying out the following 'privacy test'.[32]

1. Is the use of camera surveillance *necessary*?
2. Can the aim be achieved through *less intrusive* measures?
3. Is the use of camera surveillance *proportionate*? In other words, does the interest of the employer weigh against the interest of the employee, and have measures been taken to make the intrusion as limited as possible?

If the camera is hidden, an additional requirement follows from criminal law. Cameras, while hidden, cannot normally be *secret*. The employer is required by law to make known that camera surveillance is carried out; failure to do so is punishable with a jail sentence of at most six months or a fine.[33] Realisation of the obligation is easily achieved by hanging up signs informing people that camera surveillance is being carried out.

To pass the privacy test, the employer must make sure that the surveillance is as least intrusive as possible. This means, for example, that hanging cameras in the bathroom is not permissible, and that camera surveillance with the aim of protecting property may not be used also to establish the performance of an employee. An example of a case where the privacy test was failed was the *Koma*-case, in which the employees were able to see the cameras, but not whether the cameras were turned on or off at any specific time. The cameras furthermore covered the entire space and could be monitored from the board room. The court determined that this interference was too far-reaching.[34]

2.1.2. Covert camera surveillance

Sometimes, the employer might have cause to deploy covert surveillance. This may, for example, be the case in the aforementioned situation of suspect conduct. The Dutch Supreme Court has explicitly established that Article 8 ECHR is applicable to these situations.[35]

Dutch case law in the context of covert camera surveillance has mostly concerned cases where camera surveillance was carried out following a concrete suspicion of fraudulent or criminal activities.[36] As explained in section 1.2.1, a substantiated suspicion may constitute a legal basis for interference.[37] There have, however, also been cases where covert surveillance was carried out following a suspicion that an employee claiming illness or incapacity for work was lying, in which

[30] Article 8, sub f, PDPA.
[31] See for example Court of Schiedam 08 July 1997, ECLI:NL:KTGSCH:1997:AG1555.
[32] As published by the Dutch Data Protection Authority (Dutch DPA) on 28 January 2014 <accessible online: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/cbp-do-s-dont-s-werkgevers-privacyrechten-werknemers.pdf> (last accessed: 18 February 2017).
[33] Article 139f of the Dutch Criminal Code.
[34] Court of Appeal 's Hertogenbosch, 02-07-1989, ECLI:NL:GHSHE:1986:AC9463.
[35] Dutch Supreme Court 27-04-2001, ECLI:NL:HR:2001:AB1347 (*Wennekes Lederwaren*).
[36] Dutch Supreme Court 27-04-2001, ECLI:NL:HR:2001:AB1347 (*Wennekes Lederwaren*); Court of Appeal of 's Hertogenbosch, 21-03-2006, *ECLI:NL:GHSHE:2006:BD4089*; Central Appeals Tribunal, 10 July 2008, ECLI:NL:CRVB:2008:BD8005.
[37] ECtHR, *Karin Köpke against Germany*, Application no. 420/07, Judgment of 5 October 2010.

the employee was actually followed home.[38] This type of surveillance might not have a solid legal basis.[39]

As covert camera surveillance has more far-reaching consequences than normal surveillance, it requires a more substantial legitimate aim at the side of the employer. It may, in fact, only be used as a last resort in case of a concrete suspicion: the employer must first have taken other measures, which have proven to be ineffective. If the employer chooses to rely on covert camera surveillance, this must be used as targeted as possible and for as short a time frame as possible.[40] The employees concerned must furthermore be notified of the surveillance after the fact.

Finally, under Dutch law, the employer is obliged to notify his employees *beforehand*, for example through the use of a memorandum in which the employer lays down the circumstances under which the employer reserves the right to make use of a hidden camera.[41] It is not necessary for him to inform the employees of the exact locations of the cameras.

2.2. Telephone conversations

Employees have a right to privacy while taking a call at work. Article 8 ECHR is applicable to telephone conversations.[42] The ECthR has determined that processing information on telephone conversations – such as date, length and called numbers – may constitute a breach of Article 8 ECHR.[43] Article 13 of the Dutch Constitution also protects the privacy of telephone; however, this provision does not apply directly in horizontal relationships.[44]

2.2.1. Listening in

A distinction must be made between *listening in* to telephone conversations and *recording* telephone conversations. The PDPA does not apply to the former, as it does not constitute the 'processing' of personal data. This does not mean, however, that listening in to a phone call is always allowed. The employee may, however, be able to rely on Article 8 ECHR and on the duty to be a good employer according to Article 7:611 DCC.[45] The ECtHR has determined in the *Halford*-case that listening in on phone calls constituted a breach of Article 8 ECHR as the employee had relied on the fact that his phone calls would be private.[46]

Where there is an unjustified breach of privacy depends on the specific circumstances. Most importantly, there are several situations where listening in will normally be allowed. This includes, for example, listening in to a business call of a receptionist, but only by means of a random check

[38] Court of Breda 05 August 2010, ECLI:NL:RBBRE:2010:BN8224; Court of Gouda 27 May 1999, ECLI:NL:KTGGOU:1999:AH7898.
[39] That is not to say that the evidence obtained is necessarily also inadmissible in a dismissal procedure. This topic will be discussed in chapter 6.
[40] C. Loonstra & W.A. Zondag, *Arbeidsrechtelijke themata*, Den Haag: Boom Juridische uitgevers 2015, par. 8.3.
[41] *Parliamentary paper* II 2000/01, 27 732, nr. 7, p. 2-3.
[42] ECtHR, *Halford against United Kingdom*, Application No. 20605/92, Judgment of 25 June 1997.
[43] ECtHR, *Copland against United Kingdom*, Application No. 62617/00, Judgment of 3 April 2007.
[44] J.M.J.W. Dreessen, *Commentary on article 13 Constitution* 2008, par. C.4.
[45] I.J. de Laat & D.J. Rutgers, *Commentary on Article 1 PDPA* 2016, par. C.4.3.
[46] ECtHR, *Halford against United Kingdom*, Application No. 20605/92, Judgment of 25 June 1997.

– that is to say, not on a continuous basis – and only if the employees have been informed that this might occur. The results of the spot check must then be discussed with them.

2.2.2. Recording

The PDPA does apply to audio taping (i.e. recording), as this constitutes the processing of data. This means that a ground for permissible processing of personal data must exist. Depending on the context of the recording, there might be several. First, the employee may have given express consent to record these data. Due to the unequal relationship between employer and employee, this might not be considered unequivocal consent if the extent of audio taping is very far reaching, but the consent will likely be sufficient in case of the recording of a single phone call. In case of spot checks, the ground for processing might also be that this is "necessary for the performance of a contract", in order to be able to provide supervision and coaching to individual employees. In these cases, the checks must be proportionate to the legitimate aim and as least intrusive as possible.[47] Finally, the employer might have other legitimate interests, such as when he has a concrete suspicion of fraudulent activities or misbehaviour. The Dutch Data Protection Authority provides that *secret* recordings are only allowed in case of (bomb) threats or suspected criminal behaviour.[48]

An example from Dutch case law is a case from 2007, where the employer recorded a phone call between himself and the employee. The employee had issued threats during this call, after which the employer filed for immediate dismissal at the Dutch court. The court held that this could not be seen as a breach of Article 8 ECHR, because the phone call was made in a business context in which the "private life" of the employee was not at issue.[49] Under these circumstances, the employee would have had a low privacy expectation and the phone call did not expose intimate details of the employee's private life.[50]

2.3. Monitoring of computer and email activities

As mentioned in chapter 1, the Constitution contains a provision regarding the privacy of correspondence in Article 13, which does not (yet) cover computer activities. Despite this lacuna monitoring of computer and email activities in the Netherlands is (to an extent) regulated. First of all, there are international standards that employers have to adhere to. The ECtHR has established that Article 8 ECHR also covers electronic communication.[51] On a national level, too, courts have determined that there is a certain level of a right to privacy with regard to electronic correspondence in the workplace.[52]

Both the ECtHR and Dutch courts have acknowledged that the employer has to accept, within limits, that 'privatisation' of the work place has occurred and that, therefore, employees maintain private

[47] W.J. Koppert, "Privacy op de werkvloer" in: S.M. Huydekoper, *Wet bescherming persoonsgegevens en ICT*, Den Haag: Sdu Uitgevers 2006, p. 184.
[48] Dutch Data Protection Authority (Dutch DPA), "Opnemen van telefoongesprekken op de werkplek", *Informatieblad* 2004, no. 24.
[49] Court of Breda 15 February 2007, ECLI:NL:RBBRE:2007:AZ8381.
[50] A.H. Pool, *Particuliere recherche door werkgevers. De beoordeling van recherchegedrag van werkgevers in het Nederlands recht in het licht van artikel 8 EVRM* (diss. Radboud Universiteit Nijmegen), 2014, p. 155.
[51] ECtHR, *Copland against United Kingdom*, Application No. 62617/00, Judgment of 3 April 2007, par. 41.
[52] Court of Haarlem 16 June 2000, ECLI:NL:KTGHAA:2000:AG5277; Court of Amsterdam 26 April 2001, ECLI:NL:KTGAMS:2001:AG2741.

contacts during working hours.[53] As the workplace has become more electronic, stricter rules have come into place regulating the employee's privacy. Within reasonable limits, the computer at the workplace may be used for private purposes. On the other hand, the employer is allowed to control the way in which his network and computers are used.

The PDPA covers emails and internet data of an employee. There are several grounds that may be used to permit processing of these data, such as express consent, necessity for the performance of the (employment) contract or legitimate interests of the employer.[54] As for the latter, an inspection of the network, the screening of a sick employee's inbox or the examination of a suspicion may constitute such interests.

The Dutch Data Protection Authority has compiled guiding rules for monitoring of electronic correspondence.[55] Under these rules, the employer should draft clear guidelines on its monitoring policy. He must also lay down to what extent private use of computers in the workplace is allowed. Complete prohibition of private use will normally be seen as being too strict.[56] Prohibited computer or internet activities should be made impossible, so far as is feasible, through the use of software.

The guiding rules of the Dutch Data Protection Authority also lay down that private and business emails must be separated as much as possible. A case brought before the National Ombudsman concerned an employer who had opened the employee's inbox during a period of sickness of the latter. This was in itself allowed, as the employer had a legitimate interest in continuing her work and the guidelines within the company explicitly mentioned that emails could be opened by the employer. However, the Ombudsman decided that the employer had gone too far by opening and reading emails that were clearly (as evidenced by their subject lines) personal in nature.[57]

While reading the employee's (personal) emails may constitute breach of Article 8 ECHR, there are also justifications for doing so. Importantly, this may be the case where (similarly to camera surveillance and audio taping) the employer has a concrete suspicion regarding criminal behaviour of misbehaviour. In a 2001 case, the court of Rotterdam dealt with a case where allegations of sexual intimidation had been made about an employee. After an internal investigation, there were serious suspicions that emails had been misused in this context. The court decided that the decision to open the employee's emails was not an unjustified breach of privacy rules.[58] This case concerned a police officer, who has a special position in society. The decision must therefore not be generalised in the absence of other examples.

Finally, there are criminal law rules to be taken into account when monitoring internet and emails, such as Article 138a of the Criminal Code, which prohibits computer trespassing, and Article 139b of the Criminal Code, which prohibits the intentional and unlawful interception of data transferred on a telecommunication network. However, these rules do not apply in case of interception "by or

[53] ECtHR, Niemitz v Germany, Application No. 13710/88, Judgment of 26 December 1992; Court of Haarlem 16 June 2000, ECLI:NL:KTGHAA:2000:AG5277.
[54] Article 8 sub a, b and f of the PDPA.
[55] Dutch Data Protection Authority, Goed werken in netwerken: Regels voor controle op e-mail en internetgebruik van werknemers <accessible online: https://autoriteitpersoonsgegevens.nl/nl/nieuws/goed-werken-netwerken-regels-voor-controle-op-e-mail-en-internetgebruik-van-werknemers> (last accessed: 18 February 2017).
[56] I.J. de Laat & D.J. Rutgers, *Commentary on Article 1 PDPA* 2016, par. C.6.8.
[57] National Ombudsman 07 June 2007, *JAR* 2007/164.
[58] Court of Rotterdam 29 March 2001, ECLI:NL:RBROT:2001:AB0812.

on the instructions of the person entitled to use the telecommunication connection, except in cases of obvious misuse". As the employer is usually the entitled person, he will therefore not be punishable under the provisions except in case of obvious misuse.[59]

2.4. Personnel information systems, including GPS tracking

A final category that we want to shortly address is personnel information systems that an employer might have. It has become more normal that companies have pass systems, which may serve to keep outsiders out of the building, but usually also has the consequence, that it can be registered which employee is where at a certain point in time. Other personnel administration systems include the system in which sickness absences are registered and the system in which working times are clocked. The data collected under these information systems are covered by the PDPA, which means that a ground for permissible processing is required.[60]

Another specific example of these systems is a GPS tracking system. If for example a cab-company is able to register the locations of its taxis, these data can be used to deduce data about the individual cab drivers. This information can therefore be seen as personal data under the PDPA.[61] There are several Dutch cases in which the courts had to decide on a situation in which the combination of GPS tracking and other personnel administration systems were used to determine that the employee was lying about their working hours. One court held in this context, that because the employee was aware of the presence of the GPS system, the fact that the employer had employed this to check his working hours did not constitute covert surveillance.[62] In another case, a court held that even installing a covert GPS device after a suspicion arose did not constitute an unjustifiable breach of the employee's privacy, as the system only registers where the company car was during working hours.[63]

2.5. Conclusion

The Dutch legal system contains a multitude of rules that are applicable to surveillance measures by the employer. Importantly, Article 8 ECHR and the PDPA usually apply to these measures. This means that a balancing exercise between the interests of the employer and of the employee must be carried out. Generally, a measure will be less likely to pass the 'privacy test' the more secret and systematic it is. An employer must try to use measures in the least intrusive way possible.

[59] I.J. de Laat & D.J. Rutgers, *Commentary on Article 1 PDPA* 2016, par. C.6.3.
[60] I.J. de Laat & D.J. Rutgers, *Commentary on Article 1 PDPA* 2016, par. C.3.7.
[61] H.H. de Vries, 'Commentary on Article 1 PDPA' in: *Tekst & Commentaar Telecommunicatie- en privacyrecht* 2016, par. 2.
[62] Court of Lelystad 17 November 2004, *JAR* 2005/19.
[63] Court of 's-Hertogenbosch 24-08-2010, *AR* 2010-0772.

3. Health data protection

Data protection relating to health: In which cases (if at all) may the employer ask employees (or applicants) to reveal information relating to their health or submit themselves to medical tests? What are the relevant sources of law?

The employer is bound to 'privacy-limits' when it comes to processing health data of employees or applicants. In which cases the employer can ask an employee or applicant to reveal information relating to his health or submit to medical tests will be explored in this chapter. The first part of the question will be discussed in view of work related situations. Submitting to medical tests is dealt with in a separate paragraph. First, the legal framework regarding health data protection in the ordinary work situation will be explained. Second, the rules that apply when an employee reports himself sick are discussed. Third, it is dealt with how personal health data is protected in case of sickness and reintegration into work. Then follows the regulation concerning health data protection in the selection procedure. The second part of the question, the rules on submitting an employee or applicant to medical tests, is discussed after this.

3.1. Employment

The Dutch Personal Data Protection Act ('PDPA') provides rules for the processing of personal data. Personal data is all data which concerns an identified or identifiable person.[64] For example a name or an email address. With 'processing' is meant every act that relates to personal data.[65] Basically all possible acts fall under processing, from asking for information to filing and passing on information.[66]

The PDPA also applies to employers. Data about health is qualified by the PDPA as special personal data.[67] As a general rule, the processing of personal health data is forbidden.[68] An employer should bear in mind that asking to reveal health information is an act of processing personal data and because it concerns health, this 'act' is in principle forbidden. The sanctions that can be imposed for non-compliance with the PDPA will be discussed in chapter 5.

In case of an explicit consent of the employee there is an exception to the prohibition of the processing of health data.[69] However, such consent is almost always considered as non-existing, as the consent must be given in free will. Because of the power relationship between the employer and employee, an employee might feel to be under pressure to give his consent and then it is not given voluntarily.[70] There are cases where processing health data by the employer, with consent of the employee, can be necessary because of other reasons. For example when an

[64] Article 1 under a PDPA.
[65] Article 1 under b PDPA.
[66] R.A. Heida, 'Kritiek op de beleidsregels over de zieke werknemer van de Autoriteit Persoonsgegevens', *ArbeidsRecht* 2016/54, under 2.1.
[67] M.L Storm and A.M. Korremans, 'Privacy: risico op hoge boetes voor werkgevers van zieke werknemers', *ArbeidsRecht* 2016/27, under 2.
[68] Article 16 PDPA.
[69] Article 23 paragraph 1 subsection a PDPA.
[70] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 11.

employee is epileptic or a diabetic, then it may be necessary for colleagues to be able to give first aid in an emergency situation.[71] One could say that here the roles are reversed, it is the employee who 'asks' the employer to register his health information. The other exceptions to the prohibition of the processing of health data will be discussed in the corresponding paragraph.

3.2. When the employee reports ill

When an employee is unable to work because of sickness, he has to report this as soon as possible to his employer. The employer will require the employee to contact the company doctor or a doctor of a health service enterprise working for several companies. The medical doctor will acquire the relevant information or will do his or her own medical investigations. The doctor is subject to the general oath of secrecy and can only give non-medical information to the employer, including what work the employee still can do, how long it is expected that the employee is ill and what is the best way to get him back into work. This will be discussed more thoroughly in the next paragraph.

Obviously, the employer has an interest to know whether his employee is ill, because he might have to look for replacement or make some changes in the organisation.[72] Moreover, the employer has the statutory obligation to continue to pay 70 percent of the wages to a sick employee for a maximum of two years.[73] This makes that during these two years the employer provides the sick employee with a partial replacement income and in this situation the employee cannot rely on the Dutch Sickness Benefits Act ('SBA'). Another obligation for the employer is to discuss the possibilities for reintegration with the sick employee and to document this.[74] Because of such statutory obligations the employer is allowed to ask questions to the employee, but the protection of the employee's privacy makes that these questions are limited. According to the PDPA it can concern solely the necessary data, including information about the ability of the employee to adhere to the employment contract, data to be able to comply with the law or data which is of importance to the business of the company.[75]

In case of an employee reporting ill, the employer cannot ask about the nature or cause of sickness[76]. The employer can only ask and register the following information:

[71] *Ibidem*, p. 22.
[72] *Ibidem*, p. 19.
[73] Article 7:629 DCC.
[74] Article 25 Work and Income (Capacity for Work) Act.
[75] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 19.
[76] *Parliamentary paper II* 1997/98, 25 892, nr.3, p. 113 and 114.

- *The phone number and address where the employee is staying*
  With this information, the employer is able to communicate with the employee and therefore to check on the employee.[77] The employer can require that the sick employee has to be at home at certain times for this check, but that cannot be for a whole day.[78]

- *The supposed length of absence*
  The employer has an interest to know the supposed length of absence because he might have to make some changes within the organisation. The employer can ask the company doctor's judgement, if the employee does not have an idea about when he will be able to work again.[79]

- *The current affairs and work activities*
  Depending on the circumstances, for instance the supposed length of absence, the employer may have to look for replacement. Thus the employer has to think about which affairs cannot wait until the employee is recovered.[80]

- *If the employee receives benefit or is entitled to receive this under the SBA*
  On the basis of the SBA certain groups of employees, for example employees who are unable to work because of pregnancy, are entitled to sickness benefit, so here the employer does not have to continue to pay wages. The employer can only ask if, but not on what ground the employee receives benefit under the SBA.[81] Here it is interesting to clarify more the position of the pregnant employee. If she is absent because of pregnancy related complaints, she also does not have to mention the nature or cause of the absence.[82] Because the SBA prescribes that the employer can be reimbursed the sickness benefit paid to the employee with retroactive effect[83], there is no problem if the pregnant employee tells the employer only after some time about the pregnancy[84] if that was the cause of being unable to work. Thus the pregnant employee does not, when she is absent because of pregnancy related complaints, have to notify the employer that she falls under the protection of the SBA.[85]

- *If the sickness has a connection with a work accident*
  The employer can ask whether the sickness is caused by a work accident. Under article 9 Dutch Working Conditions Act the employer has to report work accidents to the labour

[77] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 19.
[78] G.A. Diebels, 'Controle- en verzuimvoorschriften bij arbeidsongeschiktheid', *ArbeidsRecht* 2016/23, under 2.2.
[79] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 19, 20.
[80] *Ibidem*, p. 20.
[81] *Ibidem*, p. 19, 20.
[82] Central Appeals Tribunal (for the public service and social security matters) 24 September 2002, ECLI:NL:CRVB:2002:AF8109.
[83] Article 38b paragraph 2 SBA.
[84] According to article 3:3 paragraph 1 under a Work and Care Act the employee can mention the pregnancy or ask for pregnancy leave not later than three weeks before the pregnancy leave starts.
[85] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 20.

inspectorate if they have led to permanent damage to the health of the employee or to hospitalisation. The employer also has to make a list of the reported work accidents and the ones which led to absence for more than three days and register the nature and date of the work accident.[86] This obligation is an example of a ground for data processing as mentioned in article 8 under c PDPA, because asking whether the sickness is caused by a work accident is necessary for the employer to comply with the law.[87]

- *If there has been a traffic accident where a third party is held responsible*
  The employer has the obligation to continue to pay wages to a sick employee for a maximum of two years. When the absence is a result of a traffic accident where a third party can be held responsible, the employer can take recourse against this third party.[88] In this situation the employer has a financial interest in having the relevant information. The employer's possibility of recourse invades the sick employee's privacy, because the employer needs to process information about the cause of absence. On the basis of the exception laid down in article 21 PDPA[89] the employer is allowed to process this information. Next to this exception the employer also can rely on a ground for doing this in article 8 PDPA. It follows from article 8 subsection f PDPA that, when the sickness is caused by a traffic accident, the legitimate interest to process health data of the employer prevails above the employee's interest of privacy.[90]

The list above illustrates that the employer in some situations, mainly to be able to comply with the law, needs to inquire after the employee's health. The employer cannot register more health data than the aforementioned list, even when the information is given voluntarily by the employee.[91]

The theory of health data protection does not always work so strictly in practice. Employees think it is logical that they have to inform the employer about their illness or they mention it spontaneously. The employers, often in good faith, make a note of the spontaneously given information when the employee has reported himself sick.[92]

3.3. Reintegration

After the employee has reported himself sick, the reintegration phase starts. In this phase the employee and the employer have the obligation to do their utmost to get the employee back to his job. If that job is no longer possible, the activities are to be focused on other suitable employment, and if even that is not possible, on work by another employer.[93] Reintegration is

[86] Article 9 paragraph 2 Working Conditions Act.
[87] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 21.
[88] Article 6:107a paragraph 2 DCC.
[89] Article 21 paragraph 1 subsection f under 1 PDPA.
[90] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 21, 22.
[91] *Ibidem*, p. 22.
[92] I.J. de Laat and R.A. Heida, 'Privacy en de zieke werknemer: de gespannen verhouding tussen theorie en praktijk', *ArbeidsRecht* 2013/57.
[93] Article 7:658a paragraph 1 DCC.

primarily the responsibility of the employer and the employee.[94] Their obligations to collaborate during reintegration can be found in the Gatekeeper Improvement Act.

According to article 14 Working Conditions Act supporting sick employees to get back to work is assigned to the company doctor or Health and Safety Service[95] ('HSS'). In the reintegration phase the employer is obligated to be assisted by a registered company doctor or a certified HSS.[96] Hereafter: by company doctor is also meant HSS. The employee has the obligation to cooperate with both the employer and the company doctor to make them able to satisfy their obligations and duties regarding reintegration.[97] Thus the employee has to see the company doctor and give him all the relevant information.[98] This information is safe with him, because of the earlier mentioned general oath of secrecy in relation to the employer.[99]

The employer is assisted by the company doctor, but the reintegration of the employee maintains to be his responsibility.[100] He has to take the necessary steps to enable the sick employee to return to work.[101] As mentioned in the previous paragraph the employer cannot ask the employee about the nature or cause of sickness. The employer is also not allowed to inquire about his work limitations nor work possibilities.[102] When it comes to medical health data, the company doctor, having a duty of professional confidentiality, functions as a buffer between the employer and the employee.[103] The employer asks the company doctor for advice about the limitations/possibilities and thus what kind of work the employee is still able to do. The company doctor knows the nature and cause of sickness and has the medical knowledge to give an expert judgement.[104]

The company doctor can only provide the sick employee's health data which is necessary[105] for the employer to determine his obligation to continue to pay wages during sickness and to satisfy his reintegration obligations.[106] The rest falls under the company doctor's duty of professional confidentiality. The following information can be given by the company doctor to the employer:

[94] Article 7:658a in conjunction with article 7:660a DCC.
[95] HSS is an external medical service if the employer does not have a company doctor.
[96] Article 14 paragraph 1 and 2 subsection b Working Conditions Act.
[97] Article 11 under subsection f Working Conditions Act.
[98] *Parliamentary paper II* 2000/01, 27678, nr.5, p.20.
[99] R.A. Heida, 'Reikwijdte medisch beroepsgeheim onderschat', *ArbeidsRecht* 2015/36, under 1.
[100] Central Appeals Tribunal (for the public service and social security matters) 18 November 2009, ECLI:NL:CRVB:2009:BK3704; *Parliamentary paper II* 2004-2005, 29814, nr. 6, p. 20.
[101] Article 7:658a DCC.
[102] Explanation on article 2 Regulatory procedure for first and second year of sickness; Court of Amsterdam 4 February 2014, ECLI:NL:RBAMS:2014:564, par. 7.
[103] G.A. Diebels, 'Controle- en verzuimvoorschriften bij arbeidsongeschiktheid', *ArbeidsRecht* 2016/23, under 3.
[104] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 30.
[105] Article 23 PDPA.
[106] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 24.

- *The work the sick employee is able or not able to do.* (Meaning the function limitations, remaining work possibilities and what these limitations/possibilities imply for the kind of work the employee is still able to do.)[107]
- *To what extent (percentage) the sick employee is unable to work.* (This is based on the above mentioned point.)[108]
- *The supposed length of absence.*[109]
- *Advice about adjustments or work facilities the employer has to make regarding reintegration.*[110]

Regarding reintegration the employer and the employee have to make a reintegration approach scheme[111] and a reintegration file[112]. Next to the health data which can be processed by the employer when the employee reports himself ill, the above mentioned list of health data can be processed and therefore used to make the reintegration approach scheme and reintegration file.[113]

3.4. Selection procedure

In the job interview the potential employer will ask the applicant questions to see whether the applicant is fit for the job. These questions cannot concern health or sickness absence in the past. The employer is also not allowed to obtain information about this in another way, e.g. by asking the former employer.[114] The applicant does not have to give information about his health when it is not of immediate importance to do the job.[115] He does have a duty to communicate health problems when he knows or must understand that it makes him not a suitable candidate for the position (e.g. serious hart or eye problems in case of a pilot).[116]

Also questions whether the applicant is expecting or wants to get pregnant are not permitted. If an employer asks a woman about child wishes all the same, she can give false information[117], because she is not obliged to give information relating to pregnancy.[118] The employer can find the basic rules for recruitment and selection process in the NVP Recruitment Code.[119]

3.5. Medical tests

Medical examinations can have serious consequences. If the applicant or employee turns to be unhealthy, this could lead to rejection to his application, and in the case of an employee,

[107] Article 6 paragraph 1 under j Regulatory procedure for first and second year of sickness; Rechtbank Amsterdam, 4 februari 2014, ECLI:NL:RBAMS:2014:564, par. 7.
[108] Article 6 paragraph 1 under f, I and j Regulatory procedure for first and second year of sickness.
[109] Article 2 paragraph 2 and article 3 Regulatory procedure for first and second year of sickness.
[110] Explanation on article 2 paragraph 2 Regulatory procedure for first and second year of sickness.
[111] Explanation on article 4 Regulatory procedure for first and second year of sickness.
[112] Article 5 Regulatory procedure for first and second year of sickness.
[113] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 27, 30 and 31.
[114] Article 4 paragraph 2 MEA.
[115] Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 17.
[116] Court of Limburg 29 April 2015, ECLI:NL:RBLIM:2015:3667; Court of Utrecht 4 June 2010, ECLI:NL:RBUTR:2010:BN3552.
[117] A.J.C. Theunissen, *Commentary on art. 4 MEA 2016*, par. C.4.
[118] *Parliamentary paper II* 1992/93, 22899, 8, p.28.
[119] NVP Recruitment Code, <accessible online: https://nvp-plaza.nl/sollicitatiecode> (last accessed on 10-3-2017).

demotion or maybe his employment contract will not be extended.[120] The obligation of being submitted to medical tests is restricted by the Dutch Medical Examinations Act ('MEA'). However the MEA only applies when the employer and applicant enter into an agreement (the pre-employment stage), and if the employment contract of the employee changes.[121] Thus, there is no general prohibition to conduct medical examinations. During employment[122], the situation does not concern an entering into an agreement or an alteration of the employment contract, the possibility to conduct medical examinations is examined for compatibility with articles 10[123] and 11[124] of the Dutch Constitution and therefore with article 8 ECHR.[125] The admissibility of the medical examination depends on the aim of the examination. This aim must be legitimate and must not go further than strictly necessary. It means that without the consent of the employee or an exception laid down by law, medical examinations cannot be conducted.[126] For example, the Dutch Working Conditions Act prescribes that a regulation[127] adopted by the government to give specific rules to elaborate an act, can determine that doing certain work, in special (health threatening) circumstances, is forbidden when there has not been a medical examination.[128] These regulations are used in cases where employees have to work with overpressure (diving) or when they work with radiation.[129]

Another example is the Dutch Security Regions Act ('SRA') which coordinates administrative and operational integration at regional level of fire services, disaster management, crisis management and medical assistance.[130] For these professions medical examination within the meaning of the MEA is mandatory prior to employment according to the SRA.[131] If the employee has been employed, the monitoring of his health is done by, for instance, offering periodic medical examinations or providing training and exercise.[132]

In practice medical examinations do not seem to occur very often. The obligation of undergoing periodic medical examinations is in some professions with special health risks, for instance the fire services or paramedics, mentioned in a collective labour agreement.[133] During employment medical examinations are also permitted when their aim is preventing illness or supporting sick employees in the reintegration phase.[134] The employee may refuse this examination. Because of his constitutional rights to physical integrity and respect private life, the employee cannot be

[120] W.L. Roozendaal, 'Verplichte medische keuringen', *TRA* 2017/4, under 1.
[121] Article 4 paragraph 1 MEA.
[122] W.L. Roozendaal, 'Verplichte medische keuringen', *TRA* 2017/4, under 3; See also Dutch Supreme Court 30 October 2015, ECLI:NL:HR:2015:3193 (*Loodkeuring*).
[123] Right to respect private life.
[124] Right to physical integrity.
[125] A.J.C. Theunissen, *Commentary on art. 4 MEA 2016*, par. A.
[126] *Ibidem*.
[127] This regulation is called 'algemene maatregel van bestuur (AMvB)' in Dutch.
[128] Article 16 paragraph 3 subsection e in conjunction with article 16 paragraph 5 Working Conditions Act.
[129] Chapter 6 section 5 Decree on Working Conditions; Decree on Radiation Protection.
[130] Security Regions Act; W.L. Roozendaal, 'Verplichte medische keuringen', *TRA* 2017/4, under 3.
[131] Article 18 paragraph 2 under c in conjunction with article 4 paragraph 4 Decree Personnel Security Regions; W.L. Roozendaal, 'Verplichte medische keuringen', *TRA* 2017/4, under 3.
[132] Explanation on the Decree Personnel Security Regions under 7.1; W.L. Roozendaal, 'Verplichte medische keuringen', *TRA* 2017/4, under 3.
[133] W.L. Roozendaal, 'Verplichte medische keuringen', *TRA* 2017/4, under 3.
[134] Article 21 subsection f under 2 PDPA.

forced to undergo the medical examination.[135] At the same time this signifies that the employer can postpone the payment of wages.[136] It means that only formally the employee cannot be forced to undergo the medical examination, as often the employee will not have the luxury to refuse the examination because then he will be without income.[137]

The MEA determines that medical examinations are only allowed in the pre-employment stage and when the employment contract changes, if the position asks for special requirements on medical suitability to perform the work.[138] The special requirements have to be met to protect the health and safety of the employee and third parties.[139] In the pre-employment stage, the medical examination can only be the last element of the selection procedure, i.e. the situation in which the employer really wants to employ the applicant and needs information about his medical suitability to do so.[140] Another condition for medical examinations prior to employment is that these are only permitted when, in spite of a good working conditions policy, the risks to health and safety which the position involves cannot be taken away.[141] Whether the job asks for special requirements on medical suitability, this is in the first place defined by the HSE. The employer has to ask the HSS for advice on the legitimacy and the content of the medical examination before the special requirements can be linked to the job.[142]

The 'medical test' can consist of conducting a medical examination, but also of questions about health.[143] For example questions about wearing glasses or body weight is 'testing' within the meaning of the MEA.[144] Questions like 'do you smoke' or 'do you practise a sport' refer to psychological examination and the MEA does not apply to psychological examination.[145]

According to the Complaints Committee for Pre-employment Medical Examinations ('CCPME') 'changing the employment contract' means every substantial alteration of employment.[146] This can also be an alteration of the scope of work as it could signify more physical and/or mental pressure for the employee.[147] In case of a transfer of business ownership, the employee cannot be submitted to medical tests, as the transfer does not change the

[135] G.A. Diebels, 'Controle- en verzuimvoorschriften bij arbeidsongeschiktheid', *ArbeidsRecht* 2016/23, under 2.2.
[136] Article 7:629 paragraph 6 DCC.
[137] G.A. Diebels, 'Controle- en verzuimvoorschriften bij arbeidsongeschiktheid', *ArbeidsRecht* 2016/23, under 3.
[138] Article 4 paragraph 1 MEA.
[139] *Ibidem.*
[140] Article 4 paragraph 2 MEA.
[141] Guideline of pre-employment medical examinations, p. 33 <accessible online: https://www.aanstellingskeuringen.nl/~/media/files/cka/regelgeving/leidraad_aanstellingskeuringen.ashx> (last accessed on 10-3-2017).
[142] Article 3 paragraph 2 Decree pre-employment medical examinations.
[143] Article 1 under a MEA.
[144] CCPME Advice 2012-03; A.J.C. Theunissen, *Commentary on art. 4 MEA 2016*, par. C.1.
[145] Guideline of pre-employment medical examinations, p. 87 <accessible online: https://www.aanstellingskeuringen.nl/~/media/files/cka/regelgeving/leidraad_aanstellingskeuringen.ashx> (last accessed on 10-3-2017).
[146] CCPME Advice 2012-03.
[147] A.J.C. Theunissen, *Commentary on art. 4 MEA 2016*, par. C.1.

employment contract. This is different when the employee is appointed for an actual other position after the transfer.[148]

The medical examination itself is not conducted by the employer himself, but by a person who has a pledge of secrecy.[149] A qualified and independent doctor, not being the family doctor or the doctor who treats the employee. The medical examination is limited to the special requirements on medical suitability linked to the position. Thus it cannot be used to investigate the risk of future failing.[150] The result of the medical examination is made known to the examined employee/applicant first. With his permission the company doctor can make the result of the examination known to the employer.[151]

[148] CCPME Advice 2014-11, <accessible online: http://www.aanstellingskeuringen.nl/~/media/files/cka/adviezen/2010_2014/2014/2014-11.ashx> (last accessed on 10-3-2017).
[149] Article 21 paragraph 2 PDPA.
[150] A.J.C. Theunissen, *Commentary on art. 4 MEA 2016*, par. C.3.
[151] A.J.C. Theunissen, *Commentary on art. 4 MEA 2016*, par. C.3; R.A. Heida, 'Reikwijdte medisch beroepsgeheim onderschat', *ArbeidsRecht* 2015/36, under 1.1.; Policy rules for the processing of personal data concerning the health of employees of the Dutch Data Protection Authority, p. 18.

4. Collective representation bodies.

What is the role of collective representation bodies in regard of secret or open surveillance measures? Is the works council's prior approval necessary?

Trade unions and the works council are collective representation bodies that protect the interests of the employees. In the Netherlands there is a certain relation between these two bodies which will become clear in this chapter. The role of trade unions in regard of secret or open surveillance measures will be examined first. Thereafter follows the examination of the role of the works council concerning those types of surveillance measures.

4.1. Trade unions

In the Netherlands, trade unions can enter into an agreement with employers or employers organisations on the conditions of employment.[152] The parties can also consider matters of secret or open surveillance measures. For example an employee monitoring system to observe the activities of the employees and thus to be able to support specific developments.[153] When an agreement is reached the arrangements on secret or open surveillance measures are laid down in a collective labour agreement. A few examples follow of what kind of matters are arranged on this subject in different industries. In the call centre industry the parties have agreed that the employer can arrange regulations relating to employee assessments with the works council primarily. If the employer does not organise the matter with the works council then the regulation in the collective agreement is the standard.[154] Every employee has the right to inspect his personal file as regulated in the Personal Data Protection Act; this is the only regulation relating to the handling and protection of personal data of employees.[155] Nothing is settled on measures aimed or suitable for monitoring or checking the attendance, behaviour or performance of employees. In the security sector the parties have agreed upon the criteria with respect to content on which employee assessments take place[156] and when the employer provides data of employees this is done in accordance with privacy legislation.[157] The fashion, sport and lifestyle industry has set down the criteria[158] for the employee assessment too. One of the criteria is that the assessment procedure must be in writing and known to the employee, and in case the company has a works council, the procedure needs the consent of the works council.[159] The parties of the fashion, sport and lifestyle sector have also established that privacy

[152] R.H. van het Kaar, *Commentary on article 27 WCA* 2011, par. 1.4.5.3.5.
[153] Collective Labour Agreement for personnel of CNV <accessible online: http://files.flexnieuws.nl/wp-uploads/2012/06/CAO-CNV-Vakmensen-2013-2014.pdf > (last accessed on 2-3-2017).
[154] Article 14 CLA for call centres <accessible online: https://www.fnv.nl/site/alle-sectoren/caos/caos/25158/Facilitaire_Contactcenters_cao_2010-2012.pdf> (last accessed on 2-3-2017).
[155] *Ibidem*, under privacy.
[156] CLA for private security, Protocol VI <accessible online: https://www.fnv.nl/site/alle-sectoren/caos/caos/41453/Particuliere_Beveiliging___cao_2014-2015.pdf.> (last accessed on 2-3-2017).
[157] *Ibidem*, article 102 par. 4.
[158] CLA Fashion, sport and lifestyle industry, p. 69 <accessible online: https://www.inretail.nl/Uploaded_files/Zelf/161031-cao-f-s-l-2016-2018-hvb.e2adc5.pdf> (last accessed on 2-3-2017).
[159] *Ibidem*, p. 70.

legislation applies to personal health data.[160] Still there are also industries like the construction industry[161] is laid down on anything related to open or secret surveillance measures.

Thus, trade unions can play an important role in regulations relating to secret or open surveillance measures. The previous example given shows that either these measures are not arranged or they have to be established with the consent of or in consultation with the works council. If a collective agreement does not regulate the issue, it seems that the trade unions prefer to leave the matter to the works council.

4.2. Works council

When rules on secret or open surveillance measures concerning content are not included in the collective agreement, a scheme about this is subject to the consent of the works council. [162] If the topic is fully dealt with in the collective labour agreement, the works council does not have the right of consent. If the topic is dealt with in the collective labour agreement, but only roughly, the consent of the works council is still a necessity.[163] Thus the privilege to regulate the conditions of employment lies with the trade unions and employer('s organisation).[164]
The works council's right of consent can be found in the Works Council Act (''WCA''). Article 27 paragraph 1 WCA states:

"*The consent of the works council shall be required for every proposed decision on the part of the employer to lay down, amend or withdraw:*

a. Any regulation relating to a pension insurance scheme, a profit-sharing scheme or a savings scheme;
b. Regulations relating to working hours and rest periods or holidays;
c. Pay or job-grading systems;
d. Regulations relating to working conditions, sick leave or reintegration;
e. Regulations relating to policy on appointments, dismissals or promotion;
f. Regulations relating to employee training;
g. Regulations relating to employee assessments;
h. Regulations relating to industrial social work;
i. Regulations relating to job coordination meetings;
j. Regulations relating to complaints procedures;
k. Regulations relating to the handling and protection of personal information of employees;
l. Regulations relating to measures aimed at or suitable for monitoring or checking the attendance, behaviour or performance of employees;

all the above matters being insofar as they relate to all the employees or any group thereof."

Regarding secret and open surveillance measures the subsections g, k and l are relevant. These subsections will be discussed more thoroughly further in this chapter.

[160] *Ibidem*, schedule 2.
[161] CLA construction industry <accessible online: http://www.bouwendnederland.nl/download.php?itemID=1894533> (last accessed: 2-3-2017).
[162] Article 27 paragraph 3 WCA.
[163] R.H. van het Kaar, *Commentary on article 27 WCA* 2011, par. 1.4.5.3.5.
[164] F.G. Laagland, *Commentary on art. 27 WCA 2016*, par. C.6.

There are a few requirements set forth in article 27 WCA, for making that the proposed decision of the employer falls under the works council's consent. Paragraph 1 lists the following four elements:

1) The proposed decision. The subject of that decision must be put in a concrete manner. If it concerns potential policy only this is not actual or concrete enough to speak of a proposed decision.[165]
2) To lay down, amend or withdraw a regulation. The decision involves either an arrangement, a modification or withdrawal of a regulation. The right also applies when the regulation is established, modified or withdrawn because of factual actions of the employer. [166] The word 'regulation' refers to decisions with a general effect. Meaning, if the surveillance regulation would be put in to use more than occasionally, the decision has to be presented to the works council. [167]
3) Subjects of the regulation. The subsections of paragraph 1, demanding the prior consent of the works council, is an exhaustive[168] list.[169] The criterion is the regulation's purpose: Does the regulation try to regulate one of the subjects of paragraph 1.[170]
4) All or a group. The decision must affect all or a part of the employees and not a single employee.

According to article 27 paragraph 2 WCA the employer presents the proposed decision in writing. It has to contain the reasons for the decision and the possible consequences it can have for the employees. Before the works council decides whether or not to give its consent for the employer's decision, there must have been at least one consultation meeting. The works council provides its decision in writing along with the reasons for their decision.[171]

When there is no consent regarding the proposed open or secret surveillance measures, the court can, on request of the employer, grant permission for carrying out the measures.[172] Without the consent of the works council or the permission of the court the measures are invalid if the works council submits a written appeal to the employer against these measures on the grounds of invalidity. The works council has to do this within a month after knowing about the measures.[173] If the works council acts like that, the measure is null and void.

Before taking a closer look at subsections g, k and l of article 27 paragraph 1 WCA, it is important to keep in mind the following about the functioning of the works council. Bigger companies are obliged[174] to have a works council. In these companies works council members

[165] R.H. van het Kaar, "Artikel 27 WOR", in: *Groene Serie Rechtspersonen* 2013.
[166] *Ibidem.*
[167] F.G. Laagland, *Commentary on art. 27 WCA*, par. C1; See also Court of Appeal of 's Hertogenbosch 17 November 2016, ECLI:NL:GHSHE:2016:5163, par. 3.5.3.
[168] Dutch Supreme Court 20 December 2002, ECLI:NL:HR:2002:AF0155 (*Holland Casino*), par. 3.3.2.
[169] According to article 32 paragraph 4 WCA it is possible that the employer and the works council agree on an extension of the subjects of article 27 WCA.
[170] Dutch Supreme Court 20 December 2002, ECLI:NL:HR:2002:AF0155 (*Holland Casino*), par. 3.3.2.
[171] Article 27 paragraph 2 WCA.
[172] Article 27 paragraph 4 WCA.
[173] Article 27 paragraph 5 WCA.
[174] According to the article 2 paragraph 1 WCA the threshold for establishing a works council is 50 employees employed by the employer.

usually have good facilities and contact possibilities. In smaller enterprises the works council is generally more vulnerable.[175] Well-functioning of the works council depends among other things on the employer's willingness to involve the works council in time in the decision making process.[176] Nowadays many employers see the advantages of the works council and accept the works council with open arms.[177]

4.2.1. Subsection g

As discussed above, regulations relating to employee assessments are dependent on the consent of the works council. The consent is required both for the employee assessment procedure to be followed and for the criteria on which the assessment takes place.[178] Decisions to extend a temporary assessment system are in principle an issue of article 27 WCA (so requiring consent of the works council). This is likely when the length of the regulation must be considered as an essential part of the regulation, as to that by expiring a certain time the regulation ends.[179] Whether that is the matter, must be judged in light of the circumstances of the case and what the parties could assume in the given circumstances with respect to that aspect of the regulation.[180]

Also assessments which take place by using Mystery Guests fall under subsection g.[181] Mystery Guests assess employees on how they do their work and the outcome of the assessment is laid down in their file. Thus the regulation concerns the assessment of employee work performances. As the aim and purpose of the regulation is the assessment, the decision to have such mystery guests needs the consent of the works council.[182]

Camera surveillance comes as well within subsection g.[183] The court has set strict conditions for the criteria of a '*legal basis*'. In order to comply, the employer needs to outline a clear policy.[184] This policy must regulate the conditions, the duration and the manner of camera surveillance.[185] In the Netherlands the camera surveillance policy of the employer also needs the prior consent of the works council. The stringent requirements of the Court are probably met sooner when the company has a works council which has to give its prior consent.[186]

4.2.2. Subsection k

[175] F. Dijkstra, *Ondernemingsraden in Nederland* <accessible online: http://www.orsucces.nu/content/28323/download/clnt/59885_OR-en_in_Nederland.pdf.> (last accessed: 2-3-2017).
[176] *Ibidem.*
[177] *Ibidem.*
[178] R.H. van het Kaar, *Commentary on article 27 WCA* 2011, par 1.4.5.3.14.
[179] Court of Utrecht 25 April 2001, ECLI:RBUTR:2001:ZL1148, par. 4.5.
[180] *Ibidem*, par. 4.6.
[181] Court of Appeal of 's Hertogenbosch 17 November 2016, ECLI:NL:GHSHE:2016:5163, par. 3.5.5.
[182] *Ibidem.*
[183] Court of Appeal of 's Hertogenbosch 17 November 2016, ECLI:NL:GHSHE:2016:5163, par. 3.5.4.2.
[184] ECHR 18 October 2016, application no. 61838/10 *(Vukota-Bojic vs. Switzerland).*
[185] ECHR 18 October 2016, application no. 61838/10 *(Vukota-Bojic vs. Switzerland), annotation of F.G. Laagland.*
[186] *Ibidem.*

Subsection k affects mainly a regulation regarding the protection of private life of employees, for instance when they report sick.[187] So the works council's prior consent is necessary when deciding on rules which concern the processing of information gathered from the monitoring or checking employees systems.[188] These systems will be explained under subsection l. Also a proposal to adopt or amend a medical test policy which relates to handling and protection of personal data requires the works council's consent.[189]

4.2.3. Subsection l

This subsection tries to ensure the works council's involvement with regulations relating to measures aimed at or suitable for monitoring or checking the attendance, behaviour or performance of employees. These measures are called employee monitoring- and information systems.[190] An example of an employee monitoring system is hidden camera surveillance. The use of this surveillance is not allowed without the prior consent of the works council.[191] A measure does not have to be presented as an employee monitoring- and information system, relevant is whether it can be used as such.[192] With an internal videophone the manager is able to overhear the conversations made. The words 'suitable for' in subsection l imply that prior consent for those measures is also necessary.[193] Other examples are security cameras, telephone recordings, pagers, but also having access to the employee's email inbox, as it can be used to check the attendance, behaviour or performance of the employee.[194] It is important to note that measures which include surveillance purely by the human eye are not measures within the meaning of subsection l. It conveys that in addition the use of a technical or administrative (aid)system is required.[195]

[187] R.H. van het Kaar, "Artikel 27 WOR" in *Groene Serie Rechtspersonen* 2013.
[188] I.J. de Laat, 'Verborgen cameratoezicht en de rol van de ondernemingsraad', *ArbeidsRecht* 2006/55.
[189] W.L. Roozendaal, 'Verplichte medische keuringen', *TRA* 2017/4, under 2.
[190] R.H. van het Kaar, "Artikel 27 WOR" in *Groene Serie Rechtspersonen* 2013.
[191] I.J. de Laat, 'Verborgen cameratoezicht en de rol van de ondernemingsraad', *ArbeidsRecht* 2006/55.
[192] Court of Amsterdam 17 August 2012, ECLI:NL:RBAMS:2012:BX4940, par. 9 and 11.
[193] R.H. van het Kaar, "Artikel 27 WOR" in *Groene Serie Rechtspersonen* 2013.
[194] Court of Amsterdam 17 August 2012, ECLI:NL:RBAMS:2012:BX4940, par. 11.
[195] Dutch Supreme Court 20 December 2002, ECLI:NL:HR:2002:AF0155 (*Holland Casino*), par. 3.4.

5. The Dutch Data Protection Authority

Do executive and/or independents authorities occupied with data protection (= authorities which uphold the laws protecting personal data) exist and what is their role in this context? Can such authorities impose sanctions for non-compliance with data protection legislation? Is it a (criminal) offense to collect or process data in violation of the applicable protective provisions?

In the Netherlands, there is an independent authority who supervises the processing of personal data in order to ensure compliance with laws that regulate the use of personal data: the Dutch Data Protection Authority (in Dutch: Autoriteit Persoongegevens). This section will contain, firstly, an answer to the questions what the role of the Dutch Data Protection Authority is in order protect personal data. Secondly, it will contain an answer to the question if the Authority can impose sanctions for non-compliance with data protection legislation and if this is criminal offense. Lastly, the last section of this chapter discusses briefly the role of the Dutch Data Protection Authority by the protection of personal data at work.

5.1. The Dutch Data Protection Authority

The Personal Data Protection Act (hereafter: "PDPA") requires an independent authority, who supervises processing of personal data in order to ensure compliance with laws that regulate the use of personal data.[196] The Dutch Data Protection Authority (hereafter "Authority") has been appointed as the supervisory authority with respect to the PDPA. The Authority has different tasks, which can be divided into four sections:

i. Supervision;
ii. Providing advice;
iii. Providing information, education and accountability;
iv. International assignments.

i. Supervision

The Authority supervises compliance with the statutory regulations for data protection. The supervising task includes:

- Investigation assessing compliance with the law;
- Preliminary examinations to assess the legitimacy of certain processing operations that involve specific risks;
- Assessing codes of conduct for specific sectors relating to the processing of personal data;
- Mediating in disputes;
- Keeping a public register of notifications of processing operations;
- Assessing requests for granting exemptions from the prohibition to process sensitive data.

[196] Article 51 PDPA.

ii. Providing advice

Another task of the Authority is providing advice. First of all, the Authority provides advice on legislative proposals and draft texts of general administrative regulations that wholly or significantly deal with the processing of personal data. The government has a legal obligation to request advice from the Authority when it draft legislative proposals or general administrative regulations that relate wholly or to a large extent to the processing of personal data. Secondly, the Authority provides advice to the Minister of Security and Justice about the transfer of personal data to a third country which does not ensure an adequate level of protection.

iii. Providing information, education and accountability

The Authority also provides information on how to interpret privacy legislation and general information regarding the protection of personal data.

iv. International assignments

Lastly, the Authority is monitoring the processing of personal data in the Netherlands when personal data are processed in accordance with the law of another Member State of the European Union. Besides that, the Authority must give all necessary assistance to the supervisory authorities of other Member States if this is requested.

5.2. Sanctions

The penalties which can be imposed for an infringement of the data protection law can be classified in three types of enforcement: (i) civil enforcement, (ii) administrative enforcement and (iii) criminal enforcement.

5.2.1. Civil enforcement

First of all it is possible to start a civil proceeding against the party that processes data (e.g. the employer), if the personal data of a data subject[197] are processed in violation of the PDPA. In that case, the data subject can claim compensation for its damages or an injunction.

5.2.2. Administrative enforcement

Secondly, the Authority has the right to impose administrative measures if the PDPA is violated. The Authority has the power to conduct investigations regarding compliance with the PDPA on its own initiative and on the request of interested parties such as data subjects.[198] In case of a violation, the Authority is authorized to apply administrative measures; they can take an administrative enforcement order.[199] An administrative enforcement order is a remedial

[197] Data subject means an individual who is the subject of personal data; the individual whom particular personal data is about.
[198] Article 60 PDPA.
[199] Article 65 PDPA.

sanction and not a criminal charge. It is a non-punitive order focused on the end of a violation and recovering of a legitimate situation.

Besides that, in some cases the Authority has the power to impose an administrative penalty for the violation of a large number of general obligations.[200] This power has been greatly expanded since the 1st of January 2016. The Authority can impose an administrative penalty, for example, if a government institution or company process personal data negligently, if they store personal data longer than necessary, if they inadequate secure the personal data or in the case that a controller did not notify the Authority of a breach of security which results in a substantial probability of serious adverse consequences or which has serious adverse consequences for the protection of personal data. An administrative penalty is a penalty that can be imposed without the intervention of the public prosecutor or a judge by a competent public authority. The administrative penalty is a punitive sanction focused on punishing the offender and deterring future offenders and therefore a criminal charge within the meaning of Article 6 ECHR. Paragraph 5.3 will elaborate further on the concept of criminal charge. The height of the administrative penalty can reach up to € 820.000 or, if that is not an appropriate punishment, 10% of the annual turnover.

5.2.3. Criminal enforcement

Aside from the civil and administrative enforcement, criminal enforcement measures can be imposed in limited cases.[201] For example in the case of the transfer of personal data outside the EU to a country without an adequate level of protection.[202] The difference between the administrative penalty and the criminal sanction, is that the administrative penalty can be imposed without the intervention of the public prosecutor service by a competent public authority. A criminal sanction can be only imposed by the public prosecutor.

Concluding, there are three types of enforcement which can be imposed for an infringement of the data protection law. First of all, a data subject can start a civil proceeding against the party that processes its data, if its personal data is processed in violation of the PDPA. Secondly, the Authority can impose administrative measures in case of violation of the PDPA (an administrative enforcement order or an administrative penalty). Thirdly, the public prosecutor can impose in some cases criminal enforcement measures. Administrative penalties and criminal enforcement measures are a criminal charge within the meaning of Article 6 of the European Convention on Human Rights (hereafter: ECHR).

5.3. Criminal charge

From the foregoing, it appears that there are two sorts of criminal charges possible in the case of a violation of the PDPA: (i) an administrative penalty and (ii) a criminal sanction. As a result of this Article 6 of the ECHR applicable: the right to a fair trial. This provision protects the

[200] Article 66 PDPA.
[201] Article 75 PDPA.
[202] Article 78 section 2 PDPA.

right to a public hearing before an independent and impartial tribunal within reasonable time, the presumption of innocence, and other minimum rights for those charged in a criminal case.

5.4. Personal data protection at work: the role of the Dutch Data Protection Authority

The prime focus of the Authority is supervising the processing of personal data in the employment relationship.[203] Employees are financially and socially dependent on their employer and a weak protection of data protection makes them even more vulnerable. Over the past few years one of the main goals of the authority was to facilitate the compliance with data protection in the workplace. In recent years, the Authority has mainly been engaged in personal data protection of sick employees (the use of medical data), videotaping and (pre-)employment screening. These topics are discussed in more detail elsewhere in this report.

[203] Autoriteit persoonsgegevens, Jaarverslag 2013, 2014, 2015.

6. Illegally obtained evidence

Is it – generally speaking – legally possible to use material (video, photos, testimonies) obtained through illegal (covert) surveillance measures for dismissals? Is such material admissible as evidence in court especially in claims against dismissals?

6.1. Legal basis in the Netherlands: what to be understood by 'illegal'?

In the Netherlands, illegally obtained evidence is material which has been obtained in breach of law. This doctrine of illegally obtained evidence and the consequences of this type of evidence are codified in Dutch criminal law.[204] However, such a legal framework is missing in Dutch civil law.[205] As to Dutch civil law, article 152 of the Dutch Code of Civil Procedure is important. This article is based on the so-called 'free proof doctrine'.[206] This means that evidence can be provided by all legal means available. It is then up to the judges to evaluate the evidence.[207] A Dutch Court of Appeal confirmed this in its 2013 ruling and ruled that the court has the competence to determine whether evidence has been obtained illegally and what consequences should be attached to this illegality.[208] The Court of Appeal however omitted to clarify its assessment framework. More generally it can be said that in practice, judges take into account all circumstances of the case.[209] It is therefore not easy to say when evidence is obtained illegally according to Dutch law.

Academic literature provides some guidance and states that the employer has to respect the privacy of employees (article 8 European Charter of Human Rights) when investigating their behaviour and actions. In case the employer does not respect this obligation, his act is wrongful and the obtained evidence therefore illegal.[210] The Dutch Supreme Court and some lower courts have used this reasoning several times, for example in cases of camera surveillance, recorded phone calls, viewed emails and observance by detective agencies.[211] (See also chapter 2, where this subject is dealt with.)

A breach of Article 8 is not the only ground for potential illegality of evidence. Another ground can be good employment practices. This is the case, for example, when the employer contracts a detective agency to investigate on the whereabouts of one of his (sick) employees.[212]

One of 'the circumstances of the case' that judges take into account is the existence of a concrete suspicion that the employee has acted contrary to provisions of the contract, or that he or she

[204] Article 359a Code of Criminal Procedure.
[205] K.G.F. van der Kraats, "Onrechtmatig bewijs in het arbeidsrecht", *TRA 2012/9*, p. 15-19.
[206] Article 152 Code of Civil Procedure.
[207] Article 152 lid 2 Code of Civil Procedure.
[208] Court of Appeal of Den Bosch 19-03-2013, ECLI:NL:GHSHE:2013:BZ5206, par. 4.4.6.
[209] See for example Court of Amsterdam 12-05-2014, ECLI:NL:RBAMS:2014:2751.
[210] M.M. Koevoets,'Onrechtmatig verkregen bewijs in het arbeidsrecht', *ARA 2004/3*, p. 39-58.
[211] Dutch Supreme Court 16-11-1987, ECLI:NL:HR:1987:AC9997; Dutch Supreme Court 27-04-2001, ECLI:NL:HR:2001:AB1347. See for example Court of Amsterdam 20-05-1998, ECLI:NL:RBAMS:1998:AG2109; Court of Breda 15-02-2007, ECLI:NL:RBBRE:2007:AZ8381; Court of The Hague 05-01-2010, ECLI:NL:RBSGR:2010:BM3315.
[212] Article 7:611 Dutch Civil Code; en K.G.F. van der Kraats, "Onrechtmatig bewijs in het arbeidsrecht", *TRA 2012/9*, p. 15-19.

has committed illegal or criminal acts. A 'fishing expedition' does not meet this requirement and will therefore contribute to the possibility that the obtained evidence will be ruled illegal.[213]

Two other factors that seem to play a role in determining the legality of evidence are proportionality and subsidiarity. Proportionality means that the severity of the measure (to be applied) must be in proportion to the gravity of the offence. A measure does meet the principle of subsidiarity if there is no lighter measure available to produce the achieved result. Particularly the principle of subsidiarity has often been explicitly named by the Dutch courts.[214]

The doctrine of illegally obtained evidence thus seems to be applied arbitrarily by the lack of a legal framework. Sometimes, however, the court does state explicitly why evidence is considered illegally obtained.[215] Such decisions mentioning grounds for declaring evidence illegally are important for legal certainty.

6.2. Consequences of illegally obtained evidence

In several cases, it was ruled that illegally obtained evidence can be considered admissible in dismissal cases.[216] This has been confirmed by the Dutch Supreme Court in 2001. It considered that, "even if the employer acted in violation with the right of privacy of the employee, it would not mean that the evidence should not be used in procedures".[217]

However, the consequences that are be attached to the illegally obtained evidence depend on the extent to which the employee's rights are violated. There are two options: compensation for damage or exclusion of evidence. The bigger the violation, the bigger the consequences will be.[218] Mr. Asser, Advocate General at the Dutch Supreme Court, argued that a balanced weighing of interests is needed when determining the consequences of illegally obtained evidence. He substantiated his position by invoking the process of establishing the truth: *a priori* exclusion of evidence deprives the court of the opportunity to judge based on the facts. And precisely judging on basis of the reality is in his opinion a compelling fundamental principle. Exclusion of evidence would therefore only be justified if other important interests (e.g. the right to a fair trial) were violated by the gathering of evidence. It should therefore be used sparingly.[219]

Nor the Acts, nor case law provide a clear framework of consequences for illegally obtained evidence. What consequence will be justified depends on 'the circumstances of the case'. Lower

[213] Court of Amsterdam 12-05-2014, ECLI:NL:RNAMS:2014:2751.
[214] Court of Rotterdam 29-04-2016, ECLI:NL:RBROT:2016:3327, par. 4.3; Dutch Supreme Court 27-04-2001, ECLI:NL:HR:2001:AB1347 (L/Wekkekes Lederwaren).
[215] Court of Amsterdam 12-05-2014, ECLI:NL:RBAMS:2014:2751.
[216] Court of Utrecht 25-09-1996, ECLI:NL:RBUTR:1996:AG1476; Dutch Supreme Court 01-07-1982, ECLI:NL:PHR:1982:AC7591.
[217] Dutch Supreme Court 27-04-2001, ECLI:NL:HR:2001:AB1347, par. 3.7.
[218] M.M. Koevoets,'Onrechtmatig verkregen bewijs in het arbeidsrecht', *ARA 2004/3*, p. 39-58.
[219] See the opinion of Advocate-General Asser under 4.11 at the ruling of the Dutch Supreme Court of 16-10-1987, ECLI:NL:HR:1987:AC9997; Opinion of Advocate-General Asser under 2.16 at the ruling of the Dutch Supreme Court of 07-02-1992, ECLI:NL:HR:1992:ZC0500; Dutch Supreme Court 18-04-2014, ECLI:NL:HR:2014:942, par. 5.2.3.

courts use a balanced weighing of interests of both parties.[220] Most of the times, the court prefers the truth over protecting the privacy of employees. This is *a fortiori* the case when the illegally obtained evidence proves culpable behaviour of the employee. There are no examples of cases where the district court excluded illegally obtained evidence in case the evidence was (very) incriminating to the employee.[221]

In practice, illegally obtained evidence is often used for dismissal but this does not give the employer a licence to act in violation with good employment practices or the right of privacy of the employee. The employer who does act in violation with these principles, will have to pay compensation. The amount of compensation depends on the severity of the violation, the interest that the provision protects and the process of establishing the truth.[222] This leads to the conclusion that courts have a very pragmatic approach when it comes to illegally obtained evidence: since a dismissal case has been started, both parties are not willing to cooperate anymore, and this leads to a financial compensation. Most literature is, however, very critical when it comes to this approach. Mrs. Van der Kraats is one of these critics. She finds that the Dutch labour law should link up with Dutch criminal law that regulates the consequences of illegally obtained evidence.[223]

6.3. Surveillance measures

The employer can use different kinds of surveillance measures to obtain evidence against the employee, for example camera surveillance, screening of e-mails and recorded phone calls.
Camera surveillance can be legally used as evidence by the employer. Dutch law, however, prescribes that the employer informs the employee prior to the use of a (hidden) camera.[224]
This restriction to camera surveillance is also codified in the Personal Data Protection Act 2000, and has later been confirmed by the Explanatory Memorandum of the Act Expansion Criminalization Hidden Camera Surveillance.[225] The use of a (hidden) camera without prior notice is even a punishable offence.[226] In case the employer does not give prior notice of the camera surveillance, the evidence will be illegal.[227] This does not imply the inadmissibility of the evidence: mostly, the court rather reveals the truth than protecting the privacy of the employee by excluding the evidence.[228] Nevertheless, the employee should be paid compensation since his right to privacy is violated by the employer.[229]

This may be different if the employer has a concrete suspicion of theft by the employee: in these kinds of cases the evidence that is provided by (hidden) cameras without prior notice does not lead to the conclusion that the evidence has been obtained illegally. An example is a case where

[220] K.G.F. van der Kraats, "Onrechtmatig bewijs in het arbeidsrecht", *TRA 2012/9,* p. 15-19.
[221] K.G.F. van der Kraats, "Onrechtmatig bewijs in het arbeidsrecht", *TRA 2012/9,* p. 15-19.
[222] M.M. Koevoets,'Onrechtmatig verkregen bewijs in het arbeidsrecht', *ARA 2004/3,* p. 39-58.
[223] K.G.F. van der Kraats, "Onrechtmatig bewijs in het arbeidsrecht", *TRA 2012/9*, p. 15-19.
[224] Article 139f Dutch Penal Code.
[225] Article 33 and 34 Personal Data Protection Act; Parliamentary Papers of the Second Chamber 2000-2001, 27 732, number 3, p. 13.
[226] Article 139f Dutch Penal Code.
[227] Court of Zaanstad 24-09-2014, ECLI:NL:RBNHO:2014:12275.
[228] See for example Court of Zaanstad 24-09-2014, ECLI:NL:RBNHO:2014:12275.
[229] M.M. Koevoets,'Onrechtmatig verkregen bewijs in het arbeidsrecht', *ARA 2004/3,* p. 39-58 en 49 WPB.

the employer hired an extern agency following a suspicion of theft. This agency placed hidden cameras since the normal cameras were paused each time the thieves came into the shop. The hidden cameras showed that the employee was an accessory to theft. The evidence was held not to be obtained illegally since there was a concrete indication of organised thefts.[230]

Another measure that can be used by the employer is screening of the employee's emails. In 2014, the court had to decide in the following case: the employer took the laptop and mobile phone of the employee under false pretences (updating) and screened through the messages on the email account and messaging applications of the laptop of the employee. Entering the email account was easy since the password was stored in the laptop. The court ruled that the evidence was obtained illegally since the employer had no concrete suspicion that the employee had acted contrary to provisions of the contract. This did not mean that the evidence was held inadmissible. In fact, the employer could use the evidence but had to pay compensation in order to prevent the employee's right to privacy from being eroded.[231]

The employer can use recorded phone calls with the employee as well in dismissal procedures. Recorded calls fall within the scope of the Personal Data Protection Act 2000. This means that the criteria of proportionality and subsidiarity must be met. Evidence provided by recording phone calls that does not meet the criteria, is obtained illegally.[232] The Court rules that, despite the illegal nature of the obtained evidence, a recorded phone call could be used as evidence since establishing the truth weights more than (protecting) the privacy of the employee.[233] In this case, the employer did not have to pay compensation since the recorded phone call only contained information about wage payment and was therefore considered to be of a business nature.

6.4. Conclusion

In the Netherlands, it is legally possible to use materials that are obtained through illegal (covert) surveillance measures for dismissal, since the Dutch Court finds it more important to establish the truth than to protect the privacy of the employee. This does not mean that the employer can do whatever he pleases, since making use of this evidence requires payment of a certain compensation to the employee whose privacy has been compromised. The amount of compensation depends on the severity of the violation, the interest that the provision protects and the process of establishing the truth.

[230] Court of Amsterdam 08-09-2003, ECLI:NL:RBAMS:2003:AO0147.
[231] Court of Amsterdam 12-05-2014, ECLI:NL:RBAMS:2014:2751.
[232] C.V.E. Roeloff, 'De geluidsopname als bewijsmiddel in een arbeidsgeschil', Arbeidsrecht 2007/45.
[233] Court of Breda 15-02-2007, ECLI:NL:RBBRE:2007:AZ8381.

7. Whistleblowing

In which cases – if at all – are whistleblowers protected against dismissal in your country?

Whistleblowing is the disclosure by a person to the public or to those in authority of information about what is deemed illegal, not correct, or unethical within an organization.[234] For a long time, the legal status of a whistleblower was not regulated by the law in the Netherlands – especially in the private sector. Step by step the protection for whistleblowers has been better regulated in the Netherlands. In this section we will focus on the protection of whistleblowers in the Netherland. This section will start with the development of the protection of whistleblowers in the Netherlands. Subsequently, we will discuss the Dutch act for the protection for whistleblowers: The House for Whistleblowers Act.

7.1. The development of the protection for whistleblowers in the Netherlands

Whistleblowing in the Netherlands has received more attention since 2001 when Ad Bos, staff member of a construction company, went public with handwritten records documenting corruption that engulfed nearly the entire Dutch construction industry. The ensuing investigation into corruption and fraud spread to hundreds of companies and a number of officials of government. After a long trail that ended in 2005, construction firms agreed to pay a total fine of €230 million. In this case Ad Bos lost his job and his career and became destitute, but his disclosures immediately sparked discussions about implementing legal protection for whistleblowers.[235]

7.1.1. Whistleblowing: the principle of being good employee versus the right to freedom of expression

The first protection of whistleblowers in the Dutch private sector is based on Article 10 of the ECHR, which provides employees the right to freedom of expression. But this right is bounded by the provisions of Article 7:611 of the Dutch Civil Code which stipulates that an employee must behave as a reasonable and fair employee (the principle of being good employee). This Article implies that an employee, in principle, is obliged to discretion and loyalty towards its employer. This also applies if the employee believes that there is an abuse within the organization that must be addressed for public interest. In case of whistleblowing, there is a tension between those two provisions: being a good employee versus the right to freedom of expression. It is to the judge to make a weighing of interests between those two provisions.

Dutch case law on whistleblower protection – before the 1st of July 2016 – is largely determined by decisions at European level. Two major decisions of the ECHR with regard to

[234] W. Vandekerckhove, *Whistleblowing and Organizational Social Responsibility: A Global Assessment*, Ashgate Publishing 2006.
[235] DutchNews.nl, 'Bouwfraude' <accessible online: http://www.dutchnews.nl/dictionary/bouwfraude/> (accessed 17 February 2017); M. Worth, 'Whistleblowing in Europe legal protections for whistleblowers in the EU', *Transparency International* 2013, p. 67-77.

whistleblowers and reliance on Article 10 ECHR are ECtHR Guja v. Moldova[236] and ECtHR Heinisch v. Germany[237]. In these judgements, the court considers that whistleblowers should, in certain circumstances, have protection. The court applied a balancing test (with six weighing criteria) to assess if whistleblower can get protection pursuant to Article 10 ECHR. The six criteria are:

1. The public interest involved in the disclosed information;
2. The manner in which the information is disclosed;
3. The authenticity of the information disclosed;
4. The damage suffered by the employer as a result of the disclosure ;
5. The motive behind the actions of the reporting employee;
6. The intensity of the penalty imposed.

In 2012 the Dutch Supreme Court judged about whistleblowing for the first time since 1990.[238] In this judgement, the Dutch Supreme Court did not apply the criteria the European Court of Human Rights applies in whistleblower cases, but only refers to the duty of being a good employee (article 7:611of the Dutch Civil Code). However, the criteria applied by Dutch courts are essentially the same as the criteria that the ECHR applies, but the Dutch courts imposes more stringent requirements on the gravity of the public interest.

7.1.2. The first Whistleblowers Act in the Netherlands

On the 1st of July 2016, the House for Whistleblowers Act (Wet Huis voor klokkenluiders) has come into effect. The purpose of the Act is to improve the conditions to report a concern about wrongdoing within organizations and to provide better protection for those who do so. This legislation introduces statutory legal protection for whistleblowers and provides for the formation of a new authoritative body which consists of an Advice Department and a Research Department, the House for Whistleblowers

7.2. The House for Whistleblowers Act

7.2.1. The House for Whistleblowers

The House for Whistleblowers Act introduces the House for Whistleblowers (hereafter: "House"). The House, i.e. a Dutch public institution, consists of an (i) Advice Department and a (ii) Research Department.

- ***The Advice Department***
  The Advice Department provides information, advice and support on request to the employee about the steps that need to be taken if he or she is concerned about an illegal,

[236] ECtHR 12 February 2008, ECLI:NL:XX:2008:BD1054 (*Guja/Moldova*).
[237] ECtHR 21 July 2011, ECLI:NL:XX:2011:BT6201 (*Heinisch/Germany*).
[238] Dutch Supreme Court 26 October 2012, ECLI:NL:HR:2012:BW9244 (*Quirijns/TGB*).

unethical or incorrect situation. Besides that, The Advice Department will also refer the reporter to the relevant agencies or supervisory authorities in the case of an external report and providing general information on dealing with suspected abuse.

- ***The Research Department***
  The Research Department has the task to evaluate if an application of an employee who reports a wrongdoing in a company is admissible. If an application is admissible, research will follow. Furthermore, the Research Department is able to do research into the concern. Research can be done on its own initiative or on request. At last, the Research Department can formulate general recommendations with respect to how a report of a concern about wrongdoing should be handled.

7.2.2. The scope of application of the House for Whistleblowers Act

The Act is applicable to (former) employees and (former) non-employees (for example: contractors, pay rollers, interns and volunteers, etc.).[239] Pursuant to the law, employers with at least 50 employees are obliged to adopt a whistleblowing policy on how notifications of suspected misconduct within the organization has to be dealt with. The internal whistleblowers' procedure contains at least:

- the manner in which the internal report will be handled;
- a definition of suspicion of abuse (as mentioned in the Act);
- the employees to whom concerns about wrongdoing can be reported internally;
- the obligation for the employer to treat the report in confidence if the employee requests to do so; and
- the possibility for the employee to consult with an advisor in confidence with respect to a suspicion of wrongdoing.

Besides that, the employer has to inform the employees about the situations in which a suspicion of abuse can be notified externally and the legal protection of a (potential) whistleblower.[240]

<u>The definition of suspicion of abuse</u>
It is important to have a clear definition of suspicion of abuse for the scope of application of the procedure. According to the Act, there is a "suspicion of abuse" if a perceived abuse is of structural nature and puts the general or public interest at stake (for example: breach of law, threat to public health, safety or environment and/or a danger for the public service or a company). The suspicion must be based on reasonable grounds.[241]

According to some lawyers, the definition of "suspicion of abuse" is defined too narrow in the Act. Because of the strict definition of "suspicion of wrongdoing" the House shall only have

[239] Article 1 section h of The House for Whistleblowers Act.
[240] Article 2 of The House for Whistleblowers Act.
[241] Article 1 section d of The House for Whistleblowers Act.

investigative power in exceptional cases. Furthermore, the narrow definition of "suspicion of wrongdoing" means that only a few workers can rely on the prohibition to prejudice[242].[243]

7.2.3. Procedure

The starting point for the Act is that any suspected abuse should be reported (orally or written) internally first to the responsible officer of the company, so that the organizations get the opportunity to resolve the abuses themselves. It is the organization's responsibility to adequately investigate a concern about wrongdoing that has been reported internally. If the complaint turns out to be well-founded, the organization is obligated to take measures to resolve the wrongdoing and to remedy its damaging consequences. But in the event that the (potential) whistleblower is of the opinion that the company does not take the complaint seriously, he can submit a report of the abuse to the House for Whistleblowers (with an application). Within six weeks, the Research Department will start a research about the suspected abuse and the consequences thereof (with the aim to complete the research within 12 months). The Research Department will not start a research, in case the request is unfounded, the public interest is insufficient or another body researches the matter. The law does not specify precisely when the public interest is sufficient, but in principle this concerns situations that go beyond the level of one instance or a few personal cases, for example due to the seriousness of the situation, its size or structural character.[244]

Under certain circumstances there can be a reason to skip the internal report and turn directly to the House. This will be the case, for example, if the situation is very serious and urgent, or if the highest management of the organization itself is involved in the suspected abuse.

7.2.4. Protection

One of the main goals of the Act is the protection of whistleblowers. Because of the fear of negative consequences for the personal consequences of a person, many people decided not to report a wrongdoing in a company in the past. To eliminate these fears, the legislature has chosen to provide legal protection of whistleblowers. The Dutch Civil Code states that it is prohibited to prejudice an employee who reports a suspicion of abuse – to his employer, the House or another organization – in good faith and in the proper manner.[245] The complaint must meet three requirements in order for the employee to make use of the employee protection of this new legislation:

- First of all, the employee must follow the procedure as described above with due care. In short, this implies that, in principle, the employee must report the suspected abuse internally first, and if he finds it necessary to report it externally, he must make sure that the facts are reported in a suitable and proportionate manner;

[242] See section 7.2.3.
[243] F.H.A. ter Huurne & A.J.C. Theunissen, 'Wet Huis voor klokkenluiders verbetert de positie van de klokkenluider niet', *TRA* 2016/104.
[244] Whistleblower Authority, *Integrity in practice. The reporting procedure*, February 2017, p. 9.
[245] Article 7:658c Dutch Civil Code.

- Secondly, the employee must have reasonable grounds for suspecting that the relevant facts are correct and that reporting them serves a public interest that prevails over the employer's interest in keeping them confidential. In many cases, reporting a concern about wrongdoing externally without prior notice will be deemed not to have been done with due care;
- At last, the notification must be done in good faith;

The prohibition to prejudice an employee means that an employer can not treat the person unfair. This can take many forms, such as dismissal or failure to extend a temporary contract, refusing to give a promotion or salary increase and/or transferring the employee. The prohibition pertains to the period of time during and after the investigation of the report.

8. Posting on social media

Are the (legal) consequences of postings over social media about the employer, superiors, colleagues, workplace conditions and so on an issue in your country? If yes, can such postings lead to a dismissal and / or slander claims?

8.1. Social media and dismissal in The Netherlands: a hot item

A (negative) social media post: does this fall within the power of the employer to sanction (e.g. by dismissal) or does this post fall within the freedom of speech and the right to private life? The right to private life and the freedom of speech are fundamental rights that protect the employee. These rights are, however, not unlimited since both the Dutch constitution and the European Convention on Human Rights (ECHR) have restrictive clauses. How far these restrictions may go, is a hot item. There are mainly two movements: one side finds that the freedom of speech should prevail while the other states that the interests of the employer should be protected. This is why there have been many litigations about dismissal due to social media posts: over more than ten times in the past five years.

A very recent example is the so called "Blokker-case" that caused quite some turmoil.[246] In this case, the employee called the employer a "faggot" and a "gigolo" and said that the company was a "business for cunts and whores" because the employer refused to give him an advance payment. The court terminated the employment contract since the employee exceeded the principle of being a good employee which is laid down in article 7:611 DCC (the counterpart of the obligation for employers to be a good employer).

8.2. Legal framework for dismissal due to social media postings

According to Dutch law –that recently has been changed substantially-, an employment contract can end *ex lege*, by consent, by approval of the Employee Insurance Agency, by dissolution of the contract by the court at the request of the employer and by summary dismissal. In the Netherlands, it is not common to take other disciplinary measures. Therefore, this will not be discussed here.
In order to answer question 8, in particular the summary dismissal and dissolution by the court are relevant in case of unaccepted social media postings. Therefore, these two methods will be further discussed there.[247]

Since July 2015 dismissal law allows eight exhaustive grounds for dismissal, which are:

a) Redundancy and business economic reasons;
b) Occupational disability which has persisted more than two years;
c) Frequent absence that has unacceptable consequences;
d) Incompetence and failing to work properly;

[246] Court of Arnhem 19 March 2012, ECLI:NL:RBARN:2012:BV9483.
[247] In the Netherlands, a petition to set aside summary dismissal and a petition for dissolution of the employment contract due to social media postings will be handled by the (subdistrict) court. See article 7:681 Dutch Civil Code.

e) Culpable behaviour and omission by the employee;
f) Refusal to perform (part of) a job which cannot be adjusted, due to conscientious objection;
g) Disturbed employment relations;
h) Other grounds (of bases) that are of such nature and severity that continuation of the employment cannot be expected (residual category).

A petition for permission for dismissal (from the employee insurance agency) or dissolution by the Court has to be based on one of the above bases. It is not possible to combine legal basis or accumulate circumstances from various bases.[248] Furthermore, the employer is obligated by law to investigate a suitable reassignment into another job. The only suitable legal bases for dissolution of the contract by the court due to social media posts are the "e-basis" and "g-basis" (apart from summary dismissal, see below, or a mutual agreement for terminating the contract).

8.2.1. Dissolution by the court

The "e-basis" gives the possibility to ask for dissolution of the contract if the employee acted culpably or was negligent in such a way that it is not reasonable to require from the employer to continue the employment contract.[249] If the employee has acted in such a way, suitable reassignment will not be required.[250] An example of culpable behaviour is given by the Action-case. It involved an employee who was a shop manager. The employee often wielded foul language to her subordinates such as "look that negro, I hate him", "you dirty Moroccan, you're late!", "dirty, whore, cunt, get off my parking space". The court ruled that the Action-shop did not have to tolerate the used language especially since the employer had an exemplary function as shop manager. A contributory factor was that the shop manager had been warned several times before. Therefore, the court terminated the employment contract.[251] Generally, the burden of proof for the "e-basis" is quite heavy and is on the employer, which makes it hard to the employer to dismiss the employee on this basis.[252]

On ground of the "g-basis" a disturbed employment relation can lead to dismissal. This basis requires that the relationship between the employer and the employee is disrupted.[253] In order to meet the conditions of this basis, a proper motivation is required. The existence of a disrupted relationship is therefore not enough: the employer has to prove that is it not reasonable to require from him to continue the employment contract,[254] and the employer must have tried to solve the problems.[255] This basis does, contrary to the e-basis, still require from the employer to reassign the employee (if possible), if necessary even with the aid of training. The size of the

[248] A.J. Swelheim, "Draait de redelijke grond de ontbindingsprocedure op slot?", *Arbeidsrecht*, 2014/51, p.22; O. van der Kind, "Ontslag op staande voet onder de Wwz", *Arbeidsrecht*, 2014/50, p. 57.
[249] J.M. Van Slooten, I. Zaal, J.P.H. Zwemmer, *Handboek nieuw ontslagrecht*, Deventer: Kluwer 2015, p. 116.
[250] Article 7:669 paragraph 1 DCC.
[251] Court of Amsterdam 8 December 2015, ECLI:NL:RBAMS:2015:8949.
[252] A. Roukema and D.J.Rutgers, "Kroniek Wet Werk en Zekerheid 2015", Bb 2016/14.
[253] J.M. Van Slooten, I. Zaal, J.P.H. Zwemmer, *Handboek nieuw ontslagrecht*, Deventer: Kluwer 2015, p, 137; Court of Nijmegen 12 January 2016, ECLI:NL:RBGEL:2016:86.
[254] Court of Leeuwarden 23 September 2015, ECLI:NL:RBNNE:2015:4491. See also A. Roukema en D.J.Rutgers, "Kroniek Wet Werk en Zekerheid 2015", Bb 2016/14.
[255] Court of Assen 24 September 2015, ECLI:NL:RBNNE:2015:4508; Court of Maastricht 16 September 2015, ECLI:NL:RBLIM:2015:8010.

company does matter when the court assesses weather this condition has been fulfilled.[256] Therefore, the burden of proof of this dismissal-ground is quite hard too.

8.2.2. Summary dismissal

Article 7:677 of the Dutch Civil Code creates the legal framework for summary dismissal. This is a heavy remedy and is seen as a last resort.[257] Therefore, the article sets strict conditions for a summary dismissal in order to be lawful.

- *Urgent cause*
  There must be an urgent cause in order to terminate the contract. Examples of urgent causes are mentioned in article 7:678 of the Dutch Civil Code, including that the employee batters, crudely insults or seriously threatens the employer, his family members or other employees.[258] According to the Dutch Supreme Court an urgent cause contains "deeds, characteristics or behaviour of the employee, reasonably allowing the employer to terminate the employment contact with the employee".[259] The urge of the cause has be both subjective and objective. A cause is subjectively urgent if it is beyond reason to the employer to terminate the employment contract with proper prior notice. The objectivity means that every reasonable person experiences the cause as being urgent.[260] Examples of urgent causes are theft, drunkenness, refusal to work and gross insulation.
  The circumstances of the case are also important to the court when determining whether a cause is urgent or not. Such circumstances are the severity of the cause, the personal circumstances of the employee, length of the employment history, the employer's policy (does he have a social media code or not?), prior warnings and the effects of the dismissal for the employee.[261]

- *Notice without delay*
  The employee has to give notice of the dismissal quite soon after its conduct. This does not mean that notice should be given immediately after the conduct. The employer does have reasonable time to consult a lawyer, to consult or to investigate the case.[262]

- *Notice of the cause*

[256] Court of Amsterdam 4 November 2015, ECLI:NL:RBAMS:2015:7802.
[257] Court of Appeal of 's Hertogenbosch 11 June 2013, ECLI:NL:GHSHE:2013:CA3072.
[258] Article 7:678 section 2 sub e DCC.
[259] Dutch Supreme Court 12 December 1986, *NJ* 1987, 905.
[260] H. Nieuwenhuis, *Commentary on article 7:678 DCC* 2011, paragraph 2; E. Verhulp, W.A. Zondag, *Disfunctioneren en wangedrag van werknemers*, Deventer: Kluwer 2008, p. 78.
[261] H. Nieuwenhuis, *Commentary on article 7:678 DCC* 2011, paragraph 2; Court of Leeuwarden 6 April 2011, ECLI:NL:RBLEE:2011:BQ0356.
[262] O. van der Kind, "Ontslag op staande voet onder de Wwz", *Arbeidsrecht,* 2014/50, p. 54-58; *Parliamentary paper II* 2013/14, 33818, nr.3 p. 115; See also Dutch Supreme Court 19 February 2016, ECLI:NL:HR:2016:290 Dutch Supreme Court 21 January 2000, ECLI:NL:HR:2000:AA4436; Dutch Supreme Court 18 September 1987, ECLI:NL:HR:1987:AC9961.

The employee should be informed about the urgent case. This will enable the employee to consult a lawyer about the lawfulness of the dismissal.[263]

8.2.3. Conventional method

Research shows that there were 188 proceedings about the validity of summary dismissal during the first year of the new Dutch labour law.[264] As shown in the above subsection, summary dismissal is subject to strict procedural and substantive requirements which makes it hard to employers to dismiss employees legally via this method. That is why many (in 102 out of the 188 cases) employers submitted a request for dissolution to the court in order to increase the chance that the employment agreement ends.[265] Of all these dissolution requests that were based on the e-basis or g-basis 50% of the requests were granted.[266]

8.3. Where to draw the line

All cases are different. It therefore differs from case to case what postings on social media are tolerated and which are not. There are mainly 2 different subjects that can be derived from Dutch case law when it comes to dismissal cases: criticism on management and gross insult.

According to Dutch case law, the employer has to tolerate a certain amount of criticism.[267] Generally, criticism will not often lead to dismissal because of the freedom of expression of the employee. For example, an internal memorandum or an open letter to the board should be accepted.[268] It is however important whether it concerns non-confidential or confidential information: if it concerns confidential information, the employee is held to raise awareness internally first before seeking publicity.[269]

The unclear area is even bigger when it comes to insult since the employee has the freedom of expression. This freedom is mitigated by the principle of being a good employee.[270] Which social media posts are permissible – and which are not – depends on the circumstances of the case.
One of these factors is the usual way of interaction within a company. In general, the way parties deal with each other during working time is decisive for the consequences of the (possible) insult.[271] For example, the repeated use of words like "gasbag" and "that crap of you" did not lead to dismissal in 1975 due to the social developments in language and is deemed

[263] Dutch Supreme Court 23 April 1993, ECLI:NL:HR:1993:ZC0939; E. Verhulp & W.A. Zondag, *Disfunctioneren en wangedrag van werknemers*, Deventer: Kluwer 2008, p. 69-70.
[264] M.L Beukhof en R.D Rietveld, "Het ontslag op staande voet in cijfers", *TvO* 2017(1), par. 4.
[265] M.L Beukhof en R.D Rietveld, "Het ontslag op staande voet in cijfers", *TvO* 2017(1), para. 4 and 6.
[266] M.L Beukhof en R.D Rietveld, "Het ontslag op staande voet in cijfers", *TvO* 2017(1), par. 4.
[267] Court of Maastricht 21 Februari 1991, ECLI:NL:KTGMAA:1991:AI8415; Court of Groenlo 2 January 1989, ECLI:NL:KTGGNL:1989:AI8197.
[268] E. Verhulp, *Vrijheid van meningsuiting van werknemers en ambtenaren*, Den Haag: Sdu 1996, p. 121.
[269] Court of Alkmaar 28 February 2002, ECLI:NL:RBALK:2002:AD9687.
[270] Article 7:611 DCC.
[271] E. Verhulp, *Vrijheid van meningsuiting van werknemers en ambtenaren*, Den Haag: Sdu 1996, p. 130.

acceptable.[272] This means that the way people usually express themselves in a particular context must be taken into account.
Another factor is the comprehensibility of the statement. For example, the employment contract of an employee who called his employer a thief because the latter did not fulfil commitments about the amount of wages and allowances, was not terminated by the Dutch Court of Appeal since the Court found this statement comprehensible.[273] On the other hand, the employee who called his employer repeatedly a "racist" was dismissed since it was not proven that the employer did systematically discriminate migrant workers.[274]
The third factor is the degree of culpability of the employer. This can be demonstrated by a case in which the employee called to his employer: "fat pig, don't shout!". This was tolerated by the court since it was the employer who began the fight and created the escalation.[275]
Lastly, the form of the way the insult is communicated is a factor. A written insult can lead more quickly to consequences than a verbal insult since a written insult (and therefore a post on social media) is not a whim but a deliberate utterance.[276]

These factors are the "basic factors". Dutch case law concerning dismissal due to social media posts shows that there are two more elements that play an important role. The first element is the presence of a social media code. An employer who has a code of conduct or even a social media code has a stronger legal position than the employer who does not have such a code. The second element are warnings. Although warnings are not a codified requirement, it has become a requirement created by Dutch case law.[277]

Overview of requirements:
- Usual way of interaction within the company;
- Comprehensibility of the statement;
- Culpability of the employer;
- Appearance of the insult;
- Presence of a social media code;
- Prior warnings.

De jure, it is quite hard for the employer to dismiss the employee due to social media posts. However, in practice employees are often fired due to insulting social media posts. A recent example is the dismissal of a Dutch postman who said on Facebook that he was sorry that only 44 people got killed by the attacks in Istanbul last December. His employer, PostNL, announced to terminate the cooperation with the postman.[278] It is not very likely that PostNL fulfilled all

[272] Court of Amsterdam 5 April 1975, ECLI:NL:KTGAMS:1975:AI6527.
[273] E. Verhulp, *Vrijheid van meningsuiting van werknemers en ambtenaren*, Den Haag: Sdu 1996, p. 133; Court of Appeal of 's-Hertogenbosch 29 May 2007, ECLI:NL:GHSHE:2007:BE6837.
[274] Court of Almelo 12 May 2011, ECLI:NL:RBALM:2011:BQ4333.
[275] Court of Appeal of 's-Hertogenbosch 11 June 2013, ECLI:NL:GHSHE:2013:CA3072.
[276] E. Verhulp, *Vrijheid van meningsuiting van werknemers en ambtenaren*, Den Haag: Sdu 1996, p. 130.
[277] Court of Limburg 31 March 2015, ECLI:NL:RBLIM:2015:2660; Court of Arnhem 11 April 2012, ECLI:NL:RBARN:2012:BW2006; E. Verhulp, *Vrijheid van meningsuiting van werknemers en ambtenaren*, Den Haag: Sdu 1996, p. 129.
[278] E. Meijer, "Chauffeur PostNL ontslagen na opmerking op Facebook", *Algemeen Dagblad* 12 December 2016 <accessible online: http://www.ad.nl/digitaal/chauffeur-postnl-ontslagen-na-opmerking-op-facebook~a4b9a2f9/> (last accessed: 30-12-2016).

requirements (prior warning, social media code etc.) to fire the employee lawfully but most of the times employees are not aware of these requirements that do protect them.

8.4. Slander claims by the employer

Slander claims due to social media posts are not very common in The Netherlands. Dutch labour law does not provide a special basis for slander claims due to social media posts. In order to claim damages, the employer has to use the general basis for claims which the Dutch Civil Code lays down in article 6:162. This is the so called wrongful act.

The court needs to answer the question whether posting a message on social media is a wrongful act. In order to do this, the court needs to balance the interests of the employee (freedom of speech) and the interests of the employer (protecting the company). In general, employees do have the freedom of speech. This freedom will be limited in case the employer's (or company's) honour and reputation will be damaged by the social media posts. In assessing whether this is the case, the court looks at all the circumstances of the case.

In practice, e.g. in a 2013 ruling, the court often rules that the employee is obliged to delete the social media post in order not the be imposed a fine.[279]

[279] Court of Amsterdam 12 August 2013, ECLI:NL:RBAMS:2013:5386.