The Netherlands

Stibbe Jeroen Fleming & Michiel Coenraads

1. INTRODUCTION

In the past 10 years, more and more attention has been focused on corporate integrity. On a global scale, massive bankruptcies such as Enron have contributed to throwing the subject into the spotlight, while in the Netherlands, accountancy scandals such as Ahold have occurred. These events, and more occasional infringements of competition law, have had a significant impact on regulation and have lead to the development and implementation of legislation (eg the US Sarbanes-Oxley Act of 2002) and a general increased interest in corporate governance (eg in the Netherlands the development and implementation of the Corporate Governance Code).

As a knock-on effect, individual enterprises have themselves become more focused on their corporate integrity and as a consequence, the role of compliance offer has become increasingly important, *inter alia* because of the increasingly detailed legislation and supervision required. Following on from that, there has been an increase in internal or corporate investigations, which many companies see as a means of internal risk control. A corporate investigation will most likely be commenced if any trouble (or indication of it) arises and such investigation has the purpose of mapping the issue and making an assessment of the risks contained in it. The results of it can be instrumental for the determination of future strategy. In addition, the results of the investigation can be used to ensure adequate internal reporting, eg to the supervisory board.

When commencing a corporate investigation, or when designing and setting up procedures for such corporate investigation to be commenced later, one should keep in mind that the investigation itself must be incorruptible, both with regard to the design and the execution. Errors in these areas could lead to the results of the investigation being unusable, and could even damage the enterprise, for instance, if the impression arises that there is a cover-up being put in place. Below, we will explore a number of relevant issues of both a legal and practical nature and we will address what measures a company can take in the event that the investigation brings a fraud by (for example) employees to light.

The Dutch context: legal framework

First of all, it should be noted that Dutch labour law provides strong protection for employees. It speaks for itself that an employee does not have the same freedoms during working hours as outside them, but fundamental rights such as the right to privacy, and the right to confidentiality of mail and telephone conversations (in principle) also apply during working hours.

These rights are laid down in statute, but can also be vested in individual or collective labour agreements.

Further, it should be noted that employees also have a say in the development of policies within their company. This right also applies when the company seeks to implement a plan to install mechanisms that can be used for observing or controlling the presence, behaviour and performance of employees. Examples include the installation of cameras and the checking of email and the use of the internet. The works council must endorse such policies before they can be put in place (but only in general, not specific circumstances).

As a general rule, the following can be observed. The company may not infringe the employee's privacy any more than necessary. The measure taken must meet the requirements of proportionality (being in proportion to the envisaged goal) and subsidiarity (a lighter measure is not available). In addition, a reasonable expectation of privacy might play a role (see *EHRM* 25 June 1997, NJ 1998, 506 (Halford)). How these (relatively vague) standards should be applied, depends on the circumstances of the case. It is clear, however, that, for instance, permanent camera surveillance is not allowed, while camera surveillance in the event of concrete suspicions of fraud will be allowed. (See Court of Appeals – Hertogenbosch, 2 July 1986, NJ 1987, 451 (*Koma/Industriebond* FNV) and Dutch Supreme Court, 27 April 2001, NJ 2001, 421 (*Wennekes Lederwaren*).

Dutch law does not provide for statutory laws specifically regulating investigations. This does not mean, however, that the fundamental rights as described above have not sunk into almost every relevant aspect of the Dutch legal landscape. There is one statutory law that provides specific and concrete rules that are relevant for an internal investigation that requires a deeper exploration here. The Dutch Data Protection Act (DDPA), or *Wet bescherming persoonsgegevens* (WBP), which is based on a European directive, contains standards for sound and prudent processing of personal data. The most important points in the DDPA are:

- The scope of the DDPA is limited to the full or partial automated processing of personal data in the framework of the activities of a responsible superior (in this case, the employer). Both the term personal data and the term processing have broad definitions. Under 'personal data' falls not only written data or data contained in a database, but also visual material (such as video or photo images) and audio material (such as a recording of a telephone conversation).
- It is decisive whether the data relate to a person that is identified or can potentially be identified, as anonymous or encoded data do not fall within the scope of the DDPA.
- The term 'processing' comprises virtually all acting, as of the moment of acquiring the data up until the moment of destroying the data. This means that almost all a company's investigation methods will fall within the scope of the DDPA.
- If it is established that the DDPA applies, then the recording of the data must be registered with the board for the protection of personal data

(*College bescherming persoonsgegevens* or CPB). It must be noted that there is an exception in the event the data are collected for the purposes of legal proceedings against the relevant employee.
- From relevant case law about the use of investigation methods by the employer, it appears that employees only in exceptional cases invoke the DDPA or the violation of their privacy. In addition, courts only in exceptional cases apply the DDPA *ex officio*. This can, however, play a significant role when weighing the interests in employment litigation.
- The company can make the collection of personal data 'DDPA-proof' by compiling an internal code of conduct in which it is stipulated which kind of data will be processed and for what purpose.

2. MANAGING THE INTERNAL INVESTIGATION

Who should conduct the internal investigation?

From a legal point of view, very few directions can be given regarding the question of who should conduct the investigation. It will vary from case to case, since it will depend on the nature and complexity of the investigation. Potential candidates could be: the general counsel (perhaps in alignment with the company's audit committee); the compliance officer; or the company's internal fraud teams. They might be assisted by external advisers. Again, it depends on the nature and complexity of the investigation how the team should be staffed. In any case, external legal counsel, (forensic) accountants, and in some cases external detectives, can be engaged to form part of the team.

Most of the large law and accountancy firms in the Netherlands have set up specialised investigation teams with specific and detailed experience and knowledge in the field of asset tracing and recovery, corporate, and competition. Many investigations require profound and very specific knowledge, which the company probably will not have. This knowledge, in combination with the fact that they can generally set up teams very quickly, are the most common reasons for companies to staff their investigation teams with external advisers.

Other upsides of engaging such advisers include the following. First, in some cases it might be desirable to have the investigation conducted by people who do not have personal relationships with the subjects of the investigation. It will most likely benefit the credibility of an investigation if it is conducted by external advisers instead of the company's own people. In some cases it might be that the company's own people and the internal investigation team are too closely involved in the subject matter of the investigation. An advantage to engaging external legal counsel to conduct the investigation is that counsel in the Netherlands have legal privilege, which we will explore in more detail below.

As for the engagement of external detectives, the following remarks must be made. This type of investigator will most likely not be engaged for a corporate investigation dealing with (for instance) corporate integrity or potential competition law infringements. Detectives are more likely to come into play if the investigation concerns cases of fraud or theft by the

company's employees. Dutch case law has developed certain standards that must be observed when engaging a detective. One should take as a starting point that the company will not lightly be allowed to engage a detective to investigate its employees' conduct. The following concrete rules of thumb must be taken into account:

- Generally, the company itself must supervise its employees internally. Engaging an external detective – without the employees being aware of that engagement – is only allowed in exceptional cases, such as a concrete suspicion of severe wrongdoing. (Court of Appeals – Hertogenbosch, 16 January 1991, NJ 1991, 637. Court of Appeals – Hertogenbosch 2 December 1992, JAR 1992, 147. I.P. Asscher-Vonk, *private justice in het arbeidsrecht*, in: Asscher-Vonk, S.C.J.J. Kortmann, N.E.D. Faber, *Onderneming en werknemer*, page 22.)
- The detective's assignment must be concise and well delineated.
- The detective's assignment may only be brief.
- The investigation methods are relevant: the intensive use of technical means may lead to the inadmissibility of an investigation.
- The investigation must disregard the employee's private life as much as possible.
- The employee must have the opportunity to defend itself against the allegations resulting from the investigation.
- The report of the investigation must not be kept in the file for too long.

Lastly, it must be noted that external detective firms are subject to the Private Detective Act (PDA) (*Wet Particuliere Beveiligingsorganisaties en Recherchebureaus* (WPBR)) and the Privacy Code (*Privacygedragscode*), under which a licensing system applies. In addition, these regulations provide for supervision of detectives. Detectives have a confidentiality obligation that is much less far reaching than the legal privilege of lawyers. This will be explored in more detail below. The Privacy Code provides for some basic procedural rules that apply to an investigation conducted by detectives. These standards do not apply to an investigation that is conducted by the company itself, but a certain consequential effect is assumed. (J.D.L. Nuis *et al.*, *particulier speurwerk verplicht*, 2006, page 78, 53.)

It must be noted that the results of the investigation (whether conducted by detectives or the company) generally fall within the scope of the DDPA (see above). As a consequence, if the company wishes to keep a copy of the report, it must notify the employee of it and provide it with a copy. In addition, the company must report it to CPB. The DDPA provides for an exception to these obligations if compliance with them would harm the preventing, tracing and prosecution of wrongdoings. A substantive explanation must be provided.

In short, from a legal perspective, only very few directions can be given as regards the staffing of an investigation team. It will depend on the nature and complexity of the envisaged investigation. It should be kept in mind that lawyers have a legal privilege. Engaging detectives may in some cases be necessary, but it must be clear that such investigations are bound to strict rules and cannot be too far reaching.

Retrieving reviewing and preserving of documents

The retrieving, reviewing and preserving of documents is crucial for investigations. Below we set out the applicable rules of Dutch law.

2.1 Hard copy documents

Generally, employment agreements and other regulations will contain clauses stipulating that all employee work products will be the company's property. So in principle, the company will be allowed to gather and review such documents, but this right is not unrestricted. In every case, the company must find the balance between ascertaining the truth and respecting the employee's privacy. In this respect, there is a large difference between the Dutch context and (for example) the US context.

2.2 Electronic documents

Recording telephone conversations

Under certain circumstances, the company will be allowed to listen in to or record an employee's telephone conversations. This will only be allowed if a number of conditions are met (see below). Further, a distinction must be made between business phone calls and phone calls of a personal nature. The company must realise that not all telephone conversations within the company will have a business nature. Personal phone calls fall under the employee's privacy and may not be checked by the company.

The recording of employee telephone conversations is only allowed if it is instrumental and necessary for achieving a legitimate objective of the company. The company will for instance have a reasonable interest if the recordings serve as evidence of fraud by an employee or as evidence of leaking of confidential information. Telephone conversations may only be recorded during a predetermined (short) period of time and must, as far as reasonably possible, be targeted. Therefore, taking note of corporate conversations continuously and without clear necessity may be unacceptable. Data may only be collected when there are indications of fraud. Continuously recording call detail records is not allowed. Collected data which retrospectively appears to be irrelevant must be deleted.

It must be taken into account that the PPDA may be applicable. Therefore a distinction must be made between analogue recordings and overhearing, or digital recordings and processing. The PPDA is not applicable to the analogue recording or overhearing of telephone conversations. However, if the data retrieved by analogue recording or overhearing is processed, eg by digitally or manually recording the conversations in a file, or if the call detail records are collected and the information can be traced to a single employee, the PPDA may be applicable.

In principle the employee concerned must be informed of the overhearing of telephone conversations, who can take note of the conversations and for what purposes. An exception applies to this rule if the collection of data relates to the investigation of a possible criminal offence.

Email (and internet)

In principle, the employer may check the use of email and the internet by employees. Based on the employer's power to give instructions to employees, the employer may restrict or prohibit the use of email in certain ways. If the employer intends to check the use of email or the internet, it must formulate the objectives in advance. The actions to be taken and the checks must be reasonable with respect to the interests of the employee since they may not use email solely for corporate purposes but also for private purposes. Besides that, an employee has certain independence in carrying out its work without the control of its employer. The Working Conditions Act provides that a qualitative or quantitative control mechanism on the use of email and the internet by employees is not allowed. The rule applies that the least burdensome means must be applied. Therefore, it is preferable to have an automatic content filter to read employee's emails.

Camera surveillance

Camera surveillance by the employer is only allowed in certain circumstances. If camera surveillance is used in order to collect information relating to unlawful acts by the employee, the employer may install cameras without informing the employee. However, it is not allowed to install cameras for the sole purpose of observing employees (Court of Appeals – Hertogenbosch, 3 July 1086, NJ 1987, 451). It is legitimate to install cameras to improve the safety of employees (eg for prevention of robbery).

The Dutch Supreme Court, on 27 April 2001, ruled that an employer may install cameras without informing its employees if the following three criteria are met:

- there must be a clear suspicion that one of the employees is committing a criminal offence;
- the only way to record the clear suspicion is by using concealed cameras (principle of subsidiarity); and
- the use of concealed cameras is limited to a specific area of the employer's premises (proportionality).

The PPDA provides that the employer must inform the CBP of camera surveillance. It must be explicitly reported if concealed cameras are used. In that case the DDPA will start an investigation first.

Please note that in most cases the works council must approve camera surveillance. Also in this case an exception applies in cases of suspicion of unlawful acts. Procedures can be agreed upon with the works council in advance.

2.3 Obtaining oral evidence from employees

Interviews will be an important source of information in an investigation. An employer is permitted to interview its employees (or to have its employees interviewed) but such interviews can only be held on a voluntary basis. The basic principles of an investigation also apply to the interviews: the right to hear and be heard; the employee must be provided with the relevant documents; and the employee must be informed of the purpose

of the interview. It is not permitted to invite the employee for an informal conversation, when in fact it is an interview designed to obtain information from him. Certain standards of a criminal investigation also apply to these kinds of interviews by the employer: the prohibition to put pressure on someone; caution; and the right to assistance.

If an external detective interviews the employees, special rules apply which must be observed by the detective. The Privacy Code (see above) provides that prior to each hearing, the employee must be informed that its cooperation is voluntary. Furthermore, detectives may not put pressure the employee. (J.D.L. Nuis *et.al.*, *Particulier speurwerk verplicht*, The Hague: SDU publisher 2004, p. 52 and M.M. Koevoets, *Wangedrag van werknemers* (diss. Rotterdam) Boom legal publisher 2006, pages 53 and 78.)

The Rules of Conduct of the Dutch Bar Association prescribe that a lawyer must identify itself as such and must take away any misconception in that respect.

Illegally obtained evidence

If an employer disregards the abovementioned rules in an investigation, they act unlawfully and any evidence will be considered illegally obtained. There are different thoughts on whether or not an employer can use such illegally obtained evidence in civil proceedings. Such evidence may not be allowed in proceedings relating to labour law, nor can it be of influence in determining a severance payment. A judge will assess any illegally obtained evidence on a case-by-case basis. In doing so, the following factors must be considered:

(i) the seriousness of the violation of exercising due care;
(ii) that it is very difficult or even impossible to deliver rebutting evidence as a result of the unlawful act; and
(iii) the seriousness of the misbehaviour of the employee.

(H.H. de Vries, *'opsporingstechnieken in de onderneming en het recht op privacy'* in: E. Verhulp en W.A. Zondag (red.), *Disfunctioneren en wangedrag van werknemers*, Deventer: Kluwer 2003, p. 244).

2.4 Legal privilege

Lawyers (and doctors, civil law notaries and clergymen) in the Netherlands have a statutory duty of secrecy and a corresponding right of attorney-client privilege. This duty of secrecy is more extensive than a contractual non-disclosure agreement since lawyers may refuse to testify in court based on their attorney-client privilege. Confidential correspondence between a client and its lawyer also falls under this duty of secrecy. This rule only applies to lawyers and not to in-house counsel.

This right of attorney-client privilege belongs to the lawyer, not to the client. Therefore it is up to the lawyer to assess what information is covered by the attorney-client privilege and what is not.

It must also be noted that the right of attorney-client privilege only applies to information a lawyer receives in its capacity as a lawyer. Although this term is interpreted extensively, it is advisable to keep this in mind when forming a research team.

3. DISCLOSURE FROM THIRD PARTIES

It may be of added value for an employer to obtain information from third parties and as such, the following must be borne in mind.

Data kept in third party files may fall under the scope of the PPDA. If this is the case, such third parties may not without reason provide information that falls under the scope of the PPDA. The purpose of providing the information from third parties to the employer must be in line with the purpose of keeping such information. Article 8 of the PPDA provides for six grounds on which providing information from third parties is allowed:

(i) unambiguous consent from the employee;
(ii) to carry out an agreement to which the company is a party;
(iii) a statutory obligation;
(iv) a vital interest of the company;
(v) fulfilment of a public responsibility; and
(vi) a justified interest.

Dutch law does not provide for a disclosure obligation or discovery before or during a trial. However, Dutch law provides for three ways to request information.

- The Dutch Code of Civil Procedure provides for means to obtain information from third parties. Article 843a DCCP states that someone with a justified interest can, at its own cost, request for perusal of a copy or an extract of determined records relating to a legal relation to which it is a party. Data on a data carrier are also considered to be records within the meaning of Article 843a DCCP. The scope of this provision is limited by the term 'relating to a legal relation'. It must also concern determined records, fishing expeditions are not allowed.
- Article 21 DCCP provides that parties in a trial are obliged to state facts accurately and completely. Article 22 DCCP provides for the possibility that a judge will order the parties to provide determined records or to clarify certain statements. Although this is a discretionary power, this can lead to evidence becoming available.
- The DCCP also provides for the possibility of a provisional examination of a witness to preserve evidence. This creates the possibility for a possible claimant to assess the existence of a potential claim and to obtain evidence for a potential trial.

4. PRESERVATION OF ASSETS/DOCUMENTS

Dutch law provides for extensive possibilities of conservatory attachment. These possibilities are more extensive than in other countries. Each party that can summarily substantiate its claim, can obtain permission from a judge to levy conservatory attachment on the opposing party's assets. Such assets can be in the possession of the opposing party, but may also be in the possession of third parties. In the latter case, conservatory attachment can be levied on assets of the opposing party in the possession of third parties. The purpose of a conservatory attachment is to preserve the possibility of recovery of a claim on the assets of the opposing party. It is

commonly accepted that conservatory attachment is also levied as a form of pressure on the opposing party.

If the opposing party disagrees with the attachment, it can start interlocutory proceedings to claim the lift of the attachment. The judge will lift the attachment if the opposite party can summarily prove the non-existence of the claim or if the opposing party provides security for the claim (eg by issuance of a bank guarantee). The person making an attachment is liable for damages resulting from the attachment if the judge rules that the attachment was levied unjustifiably. It must be taken into consideration that such damages are potentially major (eg in the case the attachment leads to obstructions in industrial processes).

A judge who gives permission for the attachment will stipulate that proceedings in the principal action must be started within a certain (short) period of time. If the proceedings have not been commenced within that time, the attachment will end. In the principal proceedings the claimant must be able to prove its claim. If the claimant succeeds, it will get an entitlement to enforcement so it can levy execution. If it does not succeed in proving its claim the attachment will end and it can be held liable for damages resulting from it.

5. CIVIL PROCEEDINGS

The company can start civil proceedings to claim damages if, following an investigation, it is clear that the company is the victim of fraud and the responsible persons have been pointed out. The company may also report the criminal acts of the persons to the Public Prosecution Service. Dutch criminal proceedings provide for a civil claim within the criminal proceedings. In this way the aggrieved party can also obtain an entitlement to enforcement. The advantage of such a procedure is that the aggrieved party may benefit from the evidence provided by the Public Prosecution Service.

6. ANTI-BRIBERY/ANTI-CORRUPTION LEGISLATION

Introduction

The Dutch Criminal Code (DCC) prohibits bribery of both civil servants (public sector bribery) as well as individuals working in the private sector (commercial bribery). The giver and the receiver of a bribe are punishable under the DCC. A broad variety of behavior can fall within the scope of the DCC.

In general, every gift, promise or service (advantage) offered can fall within the scope of the criminal provisions. The DCC does not provide for minimum rules about the value or nature of the advantage.

Public sector bribery

Articles 177 and 177a DCC prohibit making, promising, rendering or offering an advantage to a civil servant, such as a gift or a promise, or rendering or offering a service to an official (including foreign officials, see Article 178a DCC) in order to induce this official civil servant to do

something or to refrain from doing something in the execution of his duties.

Articles 362 and 363 DCC prohibit civil servants from requesting or accepting an advantage while knowing or reasonably expecting that this advantage is offered to induce him to do something or to refrain from doing something in the execution of his duties.

Commercial bribery

Article 328ter DCC prohibits commercial bribery. Article 328ter paragraph 1 DCC prohibits any individual working in the private sector from requesting for or accepting an advantage with reference to something he did or refrained from doing or will do or will refrain from doing in the execution of his duties while – contrary to good faith – concealing the receipt of the corresponding advantage from his principal. Article 328ter paragraph 2 DCC prohibits the giving or promising of an advantage to an individual working in the private sector while reasonably suspecting that the individual – contrary to good faith – will conceal the receipt of the corresponding advantage or promise from his principal. Both the receiving and the giving of a bribe to an individual working in the private sector is punishable under Article 328ter DCC.

Corporate entities

Under Dutch criminal law (Article 51 DCC) offences can be committed by individuals or by corporate entities (and, in addition, by a number of other entities put on a par with corporations by the relevant legislation). Corporate criminal responsibility presupposes a criminal act committed by an individual such as an employee. This individual act or omission can lead to corporate criminal liability, if the Court concludes that it is reasonable to attribute the behavior of the individual to a corporate entity. The Dutch Supreme Court (*Hoge Raad der Nederlanden*) has ruled that, generally, an act that has been committed 'within arm's length' of a company or within a corporate setting (*in de sfeer van de onderneming*) may, within reason, be attributed to the company. According to the Dutch Supreme Court, a company could be said to have accepted certain behavior if it did not take precautions which might reasonably be expected of the corporation in order to avoid the behavior in question.

Cross-border corruption

The Dutch courts have jurisdiction over any person suspected of committing corrupt acts within the Netherlands. Furthermore, the Dutch courts have jurisdiction over certain corrupt acts which take place outside the Netherlands. With regard to cross-border corruption, the following persons can be prosecuted in the Netherlands:

- any person or corporate entity, regardless of its nationality, bribing a Dutch person or a Dutch civil servant outside the Netherlands. The person or corporate entity can be prosecuted where the act is also punishable in the state where the act has been committed;
- any Dutch person or corporate entity bribing a (foreign) civil servant

or (foreign) individual working in the private sector outside the Netherlands. The person or corporate entity can be prosecuted where the act is also punishable in the state where the act has been committed;
- any Dutch civil servant or any person in public service of an international institution situated in the Netherlands bribing a civil servant outside the Netherlands. The person or corporate entity can be prosecuted where the act is also punishable in the state where the act has been committed;
- any Dutch individual working in the private sector who has been bribed outside the Netherlands, where the act is also punishable in the state where the act has been committed (article 5 lid 1 sub 2 DCC); and
- any Dutch civil servant or any person in public service of an international institution situated in the Netherlands who has been bribed outside the Netherlands.

Possible sanctions

In the case of public sector bribery, individuals can be punished with imprisonment for a maximum term of four years or a maximum fine of EUR 81,000. Corporate entities can be punished with a maximum fine of EUR 810,000.

In the case of commercial bribery, individuals can be punished with imprisonment for a maximum term of two years or a maximum fine of EUR 81,000. Corporate entities can be punished with a maximum fine of EUR 810,000.

Apart from the imposition of a fine, a legal person convicted of a crime can be faced with a consecutive separate court procedure leading to the confiscation of illegally obtained profits (Article 36e DCC).

Depending on the specific line of business, civil and/or administrative penalties can be imposed as well.

Furthermore, as a result of EU directives that are implemented in the Dutch Public Procurement Act 2012, parties convicted of bribery must be excluded from public procurement processes. A suspicion or conviction with regard to corrupt practices can also result in a suspension from participation in private procurement processes.