The semi-autonomous world of corporate investigators

Modus vivendi, legality and control

Clarissa Annemarie Meerts

The semi-autonomous world of corporate investigators

Modus vivendi, legality and control

C.A. Meerts

Colofon

Cover design: Proefschrift-aio.nl
Layout: Proefschrift-aio.nl

Print: Proefschrift-aio.nl

The Semi-Autonomous World of Corporate Investigators
Modus vivendi, legality and control

De semiautonome wereld van corporate onderzoekers
Modus vivendi, legaliteit en controle

Proefschrift

ter verkrijging van de graad van doctor aan de
Erasmus Universiteit Rotterdam
op gezag van de
rector magnificus

Prof. dr. H.A.P. Pols

en volgens besluit van het College voor Promoties.
De openbare verdediging zal plaatsvinden op

vrijdag 23 februari 2018 om 13.30 uur

door
Clarissa Annemarie Meerts

geboren te 's-Gravenhage

Erasmus University Rotterdam

Promotiecommissie

Promotoren:	Prof. dr. R. van Swaaningen Prof. dr. N. Dorn
Overige leden:	Prof. dr. H.G. van de Bunt Prof. dr. W. Huisman Prof. dr. M. Levi

Book abstract

Corporate investigators provide investigative services to organisations faced with internal norm violations. Four main professional groups of corporate investigators can be identified in the Netherlands – private investigation firms, in-house security departments, forensic accountants and forensic legal investigators. These corporate investigators move in a semi-autonomous social field with a high level of discretion and autonomy. Extensive access to sources of information and settlement options, together with a context of highly fragmented legal frameworks, produce a corporate security sector that can provide its clients with a choice of solutions for norm violations. Corporate investigators are highly flexible in their investigatory work and in relation to the settlements that they recommend to their clients. Corporate investigators incorporate normative and reputational considerations, such as due process and fair play, into their day-to-day business. They largely work autonomously, engaging the criminal justice system only when this is considered desirable in the light of pragmatic or normative considerations. Other settlement options involve engaging civil and labour courts, arranging matters through out-of-court settlement agreements and making use of internal (labour) regulations of the organisation. Cooperation between law enforcement agencies and corporate investigators is fairly rare – public/private relationships are better conceptualised as coexistence, with public and private actors meeting only on an *ad hoc* basis. This means that the state has little insight into what happens in the corporate security sector. While this has the benefit for society that the criminal justice system is spared the trouble and costs of investigating and prosecuting these matters, it also means there is effectively no democratic control over the corporate security sector. For reasons of transparency and control, it may be wise to make the private investigation permit – now only obligatory for private investigation firms – a prerequisite for all corporate investigators, regardless of their professional or institutional background. As a result of the empirical work reported upon here, it is proposed that control over such a permit system should be placed with the Dutch Data Protection Authority, rather than the police.

Preface

From the moment that I was introduced to the subject, corporate security has intrigued me. From a criminological point of view, it remains largely obscured because of lack of attention. From a societal point of view, the same could be said. While police and (to a lesser extent) private security enjoy much consideration, both by society and criminology, the day-to-day business of corporate investigators remains relatively unknown. The field is shrouded in mystery. This may have been one of the attractions of the subject for me. The Research talent grant, awarded in 2012 by the Netherlands Organisation for Scientific Research (NWO), allowed me to pursue this subject. I am very grateful to NWO for funding my research and making my PhD project possible. In addition, I owe much gratitude to the anonymous professionals who were kind enough to participate in this research. By acting as respondents for the interviews and as gatekeepers for further recruitment of respondents they have proven to be essential. Without their expertise and support, the book that is before you would not have come into being. Additionally, I would like to take this opportunity to express special gratitude towards the two anonymous companies where the observations were executed. I have gained much insight into my research subject through the opportunity that was granted to me by the companies that have been so gracious in opening their doors to me. These experiences have been essential to my dissertation and have been both very educational and very engaging.

In the Netherlands, doctoral students are fortunate enough to be an employee instead of a student. I would like to thank the Erasmus School of Law for supporting my research and for adding to my development as a social scientist. I have thoroughly enjoyed my time as an employee of the Criminology department of the Erasmus School of Law of Erasmus University Rotterdam, both previous to and during my PhD research. In specific, I would like to thank my former colleagues from the Criminology department. You are a great group of people and I have been fortunate to work with you. In this light, I would also like to thank my students, with whom I have been very pleased to interact. Looking to the future, I want to thank my current employer, the Criminology department of the Vrije Universiteit Amsterdam (VU), in specific Prof. Dr. Wim Huisman and Prof. Dr. Edward Kleemans, for providing me with the opportunity to continue my work in academia. I very much look forward to continuing my research and teaching in Amsterdam.

Furthermore, I am very grateful to the members of the Doctorate Committee for commenting upon and assessing my dissertation. Specifically, I want to take the opportunity to thank my supervisors, Prof. Dr. René van Swaaningen en Prof. Dr. Nicholas Dorn. René, thank you for believing in the project and in me. Your critical outside perspective, as you tend to call it, has been essential to the substance of this

dissertation. I have enjoyed working with you and I am certain our paths will continue to cross. Nicholas, in many ways this book is a result of the fortunate circumstance that I was assigned to you as a student-assistant back in 2007. Back then I could not fathom that I would be captivated by the subject you had introduced to me in such a measure that I would write my dissertation about it. Your support, both personally and professionally, continues to be essential to my criminological career. Your sharp comments have improved my research – and my command of the English language – to a great extent. I feel very fortunate to have had the privilege of having you as my supervisor. I have not suffered from the often-voiced predicament of PhD students who are obliged to wait endlessly for a response from their supervisors. On the contrary, there might have been times when I would have preferred a day's rest in between submitting a chapter or paper and having to redraft it. I feel my dissertation is infinitely better as a result of your involvement. On a more personal note, I could not have wished for a more intelligent, inspirational, funny and warm supervisor than you. Our email conversations often make my day.

One of the added benefits of writing your dissertation is formed by the social ties you create during this time. When I first started working at the Erasmus University Rotterdam, I could often be found in L6-002, the office of Robby Roks and Joep Beckers. I have thoroughly enjoyed our conversations about academia, our respective research projects, students, football and life in general. I had fun working and not-working with you. Robby, I have always admired the dedication and the enthusiasm you combine with a healthy amount of cynicism with regard to our work as criminologists. To me, you are the prime example of the future of criminology. Joep, I am honoured to have you as my paranymph and as my friend. Although our professional paths have separated some time ago, I am glad we are keeping in touch. I believe there will always be a place for you in academia, should you decide to come back some day – you know the students would be thrilled. Lisa van Reemst, my other paranymph – the same goes for you. You have been my office mate for five years and during that time, I have come to know you as the sweetest, most genuine person. I have had so much fun working with you. I want to thank you for being there for me during the good and the bad times. I am proud to call you my friend and am so glad we are not losing sight of each other, even though we now work in different cities. It is my time to finish my PhD now; I am looking forward to celebrating once more as a result of the finalisation of your dissertation.

Finally, I would like to take this opportunity to thank the people who are closest to me and who have supported me during my PhD research (and, well, in 'life'). Many doctoral students express their relief after finishing their dissertation, having to be locked away in a room for a period of time. I have been lucky enough to be able to avoid that. My dissertation is a product of my hard work, combined with the support and understanding of my family and friends. First of all my parents, Leni Buisman and Paul Meerts. You have

both provided me with the implicit and explicit support necessary for such an endeavour, starting with the way in which you raised me. Thank you for giving me the freedom and confidence to pursue this path. I feel very fortunate to be your daughter. Thank you for your unconditional support and love. Mom, you have always been the pillar in my life and my inspiration. You have been a great role model, combining a flourishing career with raising a family. And specifically, thank you for getting me into the social sciences – and as a bonus, I ended up at Erasmus University, just like you. Dad, if anyone can relate to the motivation and effort necessary to finish (or even start) a dissertation, it is you. I have great respect for what you have accomplished, with your dissertation as icing on the cake. Your life in academia and your travels have inspired me to look beyond what is conventional. My brothers and sister, Fedor, Iris and Edo Meerts, you three are my safety net. Thank you for having my back. Fedor, you and I are headstrong to an equal amount and growing up together has sharpened my mind to a great extent. From growing up to growing old together, you continue to be my best friend. Barbara Huigsloot and Marlou Schellekens, my other best friends, thank you for your support and friendship. Barbara, I have trouble remembering the time when we were not yet friends and I could not imagine life without you. As your parents tend to say, you and me are like sisters. Thank you for being an ear to talk to, a shoulder to cry on and a friend to laugh with. For the both of us, a new chapter of our lives is about to unfold. I can't wait to see how the story continues. Marlou, studying criminology has long since rewarded me with your friendship, one that has evolved far beyond the lecture rooms. I am proud to see what you have accomplished in such a short period of time. Thank you for all those times studying, laughing and crying together. Let's keep up that great tradition until we are grey and old. Ilka and Elwin Burik, by entrusting me with the care of our beloved horse Blannish, you have afforded me with a daily moment of zen which has been essential to the process of writing my dissertation. I cannot thank you enough for that. And finally, I want to thank my dearest Kinsley Roosburg. I imagine being catapulted into this strange process we call a dissertation would have been difficult for anyone but you, especially at such a hectic time as the final year. Your cheerfulness and optimism in life is a big support and inspiration to me. Thank you for understanding the PhD process, thank you for unconditionally believing in me and thank you for always being there. You have been good to your word and have indeed made my life easier. And importantly, more fun. I cannot count the times we have said the words 'after the PhD…'. So now it's time for that holiday.

Contents

Figures

Tables

Chapter 1

Introduction

Research questions, theoretical notions and methodology

Introduction

A large-scale fraud in which the municipality of Rotterdam has been defrauded for millions of euros – the *Waterfront-affaire* (Gemeente Rotterdam, 2017). A large-scale real estate fraud in which a pension fund and others have been defrauded for millions of euros – the *Vastgoedfraude* (Van de Bunt, Holvast, Huisman, Meerts, Mein & Struik, 2011). The payment of multiple bribes and large-scale corruption in multiple countries by SBM Offshore (Functioneel Parket, 2014). These are all cases in which internal norm violations have led to considerable damage to both the organisations involved and Dutch society. Interestingly, the first line of investigation in these cases was not the criminal justice system – instead, internal investigations were done by corporate investigators. These are all examples of cases in which an official report has been made to the authorities. However, many cases that are investigated by corporate investigators never reach the criminal justice system (Williams, 2006a). Although traditional criminology is well aware of the issue of the dark number of crime – the fact that much criminal occurrences will not become known to the state (or to criminologists for that matter) – it is usually assumed that crimes in those instances remain un-investigated. The work of corporate investigators remains largely unknown to society and criminology alike.

The prevention and repression of crime is traditionally seen as a task exclusively reserved for governments (Boutellier, Van Steden, Bakker, Mein & Roeleveld, 2011). As Max Weber (1946) noted, the monopoly over legitimate use of force is the essential tool of governance of states. As a result, criminology has traditionally been mostly concerned with state activity in the reduction and management of crime. From a historical perspective, it has been argued by Garland (2001) and Wood and Shearing (2007: 7) that although "the governance of security has for some time been regarded as the primary responsibility, and indeed exclusive responsibility, of state governments [this] has not always been the case. From a historical perspective this way of doing is very new indeed – it constitutes no more than a hiccup in history". The argument is that the prevention and reduction of crime has historically been a shared responsibility and that we are in recent years moving back towards that 'normal' situation. In their discussion of an emerging plethora of public/private arrangements, Van de Bunt & Van Swaaningen (2005) argue that in this process, market rationales have permeated the criminal justice system as well.

A long list of publications over the years shows that the focus has been broadened to (critically assess the contribution of) regulatory agencies (see for example Mancini & Van Erp, 2014), civilians (see for example Van Steden, 2009) and private security firms (see for example South, 1988). As Jones and Newburn (2006) put it, there is a growing academic recognition for the pluralisation of policing. It is now

commonly recognised that police forces are not the only players in the security field. In the Dutch situation, multiple other actors are involved: regulatory agencies, special investigative units within ministries and the input of local government are just some examples (Van de Bunt & Van Swaaningen, 2005).[1] In addition to state-provided security services, there now is a substantial private security industry as well. In specific places, such as the Port of Rotterdam, public/private security-scapes emerge (Eski, 2016). Services provided by this private sector range from guarding and surveillance, to technical equipment services (Van Steden & Huberts, 2006). These are the types of activities that usually come to mind when one refers to 'private security'. A "very distinct sector within the security industry" is formed by private investigators (ibid.: 21). This book is concerned with private investigators, or more accurately *corporate* investigators. On the one hand, this means that the book focuses on a smaller group: i.e. only those investigators whose clientele consists of (public sector and commercial) organisations, excluding the detectives working for private citizens. On the other, as will be explained below when the research is outlined, my understanding of corporate investigators is wider than in most studies (including a range of different actors, see below).

Most research on private security focuses on the sector more generally, including private investigators as just another form of private security (see for example Shearing & Stenning, 1983). The rise of private forms of security provision is often seen as a (direct) result of increasing demands on public police in a time of neo-liberalisation of social policy (Jones & Newburn, 2006). Adding to that the growth of semi-public places, mass private property and risk awareness (Beck, 1992), one should not wonder that private security is booming. "Despite talk of public monopolies and the like most jurisdictions have generally housed a variety of policing bodies" (Jones & Newburn, 2006: 6). Public/private relationships in the field of security are often conceptualised along these lines. Theoretical concepts such as privatisation and responsibilisation are then used to indicate that the state either privatises some of its activities to private parties, or that the state mobilises private actors for the fight against crime (Garland, 2001). In that broad tradition, public law and public law enforcement bodies and strategies – police, prosecutors and criminal courts, and/or administrative agencies – are taken as conceptual starting points (see for example Janssen, 2011; Fijnaut, Muller, Rosenthal & Van der Torre, 2007). Relations between the public sector and private security are then posed in terms of cooperation by the latter with the former (Hoogenboom & Muller, 2002; Hoogenboom, 2009; Dorn & Levi, 2009; Cools, Davidovic, De Clerck & De Raedt, 2010). Whether or not this is the

1 See for example also Van Reemst (2016) on safety tasks of other first other first responders than the police.

right way to conceptualise private security more generally is not a question to be answered in this book. However, it is argued that for corporate security specifically, these notions fail to provide a correct conceptualisation.

The research reported on in this book was executed as a PhD-project at the Criminology department of Erasmus University Rotterdam. It is funded by the Netherlands Organisation for Scientific Research (NWO) through a Research Talent grant.[2] The research examines the rather under-researched field of corporate security (Walby & Lippert, 2014). Although interesting work has been done on different components of the corporate security sector (for example Hoogenboom, 1988; Gill & Hart, 1997; Van Wijk, Huisman, Feuth & Van de Bunt, 2002; Williams, 2005; Nalla & Morash, 2002), there exists a rather limited body of work on the corporate security sector as a sub-sector of the private security sector (Meerts, 2016). This research is therefore for a large part exploratory, mapping the sector and its legal frameworks (chapter 2), its activities (chapters 3 and 4) and its relationships with the criminal justice system (chapter 5). All of this has implications for the theoretical conceptualisation of corporate security as well.

Research focused on corporate investigators and corporate justice is highly relevant to criminology in multiple ways. First, the corporate security sector, like criminology, is highly interdisciplinary. Professionals with different backgrounds work as corporate investigators, all bringing their specific expertise with them. This means that the research subject and the analysis of that subject benefit to a great extent from an interdisciplinary approach, combining social sciences with law. Second, although the attention for social control originating from other sources than the police is growing, little research has been done as of yet on corporate investigators and corporate justice. It is, however, a booming sector which provides services that may affect both individuals and society. Creating a better understanding of this sector is therefore important. Third, the theoretical notions used for public/private relations may be in need of some adaptations with regard to their applicability to specific parts of the private security sector such as corporate security. In trying to fit everything into a state-centric discourse, criminology may be overlooking some important characteristics of private security.

2 https://www.nwo.nl/actueel/nieuws/2012/Gehonoreerde+voorstellen+MaGW+Onderzoekstalent.html.

To achieve a better understanding of the corporate security sector, the following research questions are used as a guide for the research:

Central research question
What is corporate security, how can its shifting relationship with law enforcement be conceptualised and what is its significance for the wider society?

In particular:

1. *What are the raison d'être and methods of corporate security in providing corporate justice?*
2. *How does this stay within – or breach – regulatory/legal frameworks?*
3. *How wide, in practice, is the sphere of discretion for corporate security, either to act alone, without informing public law agencies, or to inform and possibly to task them?*
4. *When, how and why does separate working change into case-sharing? How does this reflect the public and private interests at stake?*
5. *What are the consequences of the flexible relationship that corporate security has with law enforcement?*

The research questions as presented above, motivating the research, were defined in 2011 and have been subject to development during the research process. Therefore, the research questions are put into context in this first section. Research question 1 is used to explore the corporate security market and to determine the day-to-day business of corporate investigators. This question is answered in chapter 2 (with regard to the professionals who are active in the corporate investigations market), chapter 3 (with regard to the corporate investigative process) and chapter 4 (with regard to corporate settlement options). Research question 2 maps the legal frameworks that guide corporate investigators' activities and the extent to which corporate investigators seem to abide by these rules and regulations. This research question is answered in chapters 2 to 4 as well, chapter 2 providing the more general legal frameworks and chapters 3 and 4 relating the legal contexts of corporate investigations and corporate settlements more specifically.

Research question 3 reflects upon the question of autonomy of corporate investigators. The reasoning used in most literature, derived from the state-centric discourse (see below), is inversed here. The question is whether there is any room for corporate investigators to work autonomously and if there is, how far this freedom may reach. In addition, research question 3 refers to the situation in which

law enforcement agencies may be actively involved in corporate investigations by investigators and clients – either by informing them or using law enforcement agencies for their own (strategic) purposes. These questions are answered in chapter 4 (when discussing the corporate settlement options and the reasons (not) to report to the authorities) and chapter 5 (with regard to the public/private relations found in this research). The answer to this question is relevant to research question 4, which may be seen as a follow-up to research question 3. Central to the answers to research question 4 is the typology of public/private relations presented in chapter 5. The reasons for establishing contact with law enforcement authorities are related in chapter 4 and 5. Chapter 5 furthermore discuses formal and informal relationships between law enforcement and corporate investigators, presenting a typology for *ad hoc* contacts as well.

Research question 5, finally, turns to the consequences of both the existence of the market for corporate investigations and the relationships between it and the criminal justice system. This research question is answered throughout the book when themes such as investigator/client relations, the position of the involved person, the use of forum shopping and the relations between corporate investigators and law enforcement agencies are discussed. The 'consequences' mentioned in research question 5 are both practical (what are the consequences for the individuals and organisations involved and for society) and conceptual (what are the consequences for the applicability of commonly used theoretical notions).

The main research question is an amalgamation of the various more specific research questions. As will be apparent from the above description, the research questions are answered in different sections of the book. Chapter 6, then, concludes the book by drawing everything together and formulating an answer to the various research questions and drawing conclusions with regard the central research question.

This chapter continues with setting the stage for the research by defining some of its core concepts. Section 2 expands on this by discussing some of the more commonly used theoretical notions on private security and – most notably, the public/private relationship. These theoretical notions are critically assessed in the context of the research and a different approach is suggested. Section 3 delineates the methods used in the PhD research which is the basis for this book. Finally, a brief overview of the book is given to the reader.

1. Defining core concepts

This research explores the corporate security industry by focusing on private, corporate investigations into behaviour by organisations' staff, management, subsidiaries and sub-contractors, that is considered problematic by these organisations. Before this is possible however, a clear understanding of the core concepts must be obtained. In this book the terms 'corporate security' and 'corporate investigators' are used to emphasise the difference with the private security sector more generally (which contains a wide range of security services not discussed here – for example static guarding, surveillance or cash-in-transit transports) and private investigators specifically. The corporate security sector consists of professionals, providing specialised and tailor-made 'high-end' security services to their clients. The terms 'corporate security actors' and 'corporate investigators' are both used here to signify these professionals. Although corporate investigators may be involved in additional activities (such as pre-employment screenings and drafting and implementing integrity codes), this research focuses on the investigative activities of corporate investigators: mainly forensic accountancy, (private) investigations more generally, IT-investigations, asset tracing, and (assistance with) settlement and prevention tactics (Williams, 2005; Meerts, 2013).

There may be many actors involved in these kinds of activities. Important selection criteria for inclusion in the definition here are that the investigations should be (one of the) main professional activities of the investigator; that the investigations involve a person as a subject (person-oriented investigations)[3]; and that the investigations are done in a corporate setting (within an organisation).[4] This means that for example information bureaus gathering information in bulk without having a specific person in mind (Hoogenboom, 1994) and private investigators working for individuals (mainly divorce cases) are excluded from the research. Clients of corporate security may be both commercial and (semi-)public organisations. Respondents indicate that most of their clients are medium to large-scale companies, which they attribute to the costs of investigations. In this book, the term 'client' is used to indicate the consumers of corporate security services. In the case of an in-house corporate security department, the client is for example the company's management. In this research the following groups are considered to be part of the corporate security sector:

3 For a definition of person-oriented investigations, I refer to the guidelines for person-oriented investigations for accountants, which state: "[an investigation] of which the object consists of the actions or non-actions of a (legal) person, for the execution of which activities of a verifying nature will be done, for example the collection and analysis of (whether or not) financial records and the reporting on the outcomes" (NIVRA/NOvAA, 2010: 4).

4 To specify, the 'corporate setting' is not limited to commercial firms: (semi-)public organisations may also serve as a client to corporate investigators.

private investigation firms, in-house security departments, forensic accountants and forensic (departments of) law firms. Many corporate investigators have a background in law enforcement. Chapter 2 focuses more specifically on the different professional groups of corporate investigators.

In addition, the focus of the research is on (investigations into and settlements of) internal norm violations. The norm violation must occur in the context of an employee/employer relationship.[5] External threats, such as large-scale DDoS [Distributed Denial of Services] attacks by organised crime networks, are therefore excluded (unless they are executed by someone within the organisation). Anyone with a labour relationship with an organisation may be subject to corporate investigations. Moreover, it is important to note that corporate investigators have a distinct 'downwards gaze': most corporate investigations are focused on (lower level) management and employees, while the organisation itself, as a 'legal person' is often neglected (Williams, 2014).[6] 'Norm violations' is a broad-scope concept, which may be used for all types of employee behaviour that is deemed problematic by an organisation. As will be discussed below, one of the unique selling points of the corporate security sector is that investigations are not limited to criminal acts (Williams, 2005). The greater part of 'norm violations' (consisting of economic loss, misappropriation of assets, reputational issues and the like) occurring within organisations never reaches the criminal justice system (Dorn & Meerts, 2009). These norm violations may concern (alleged) criminal behaviour such as fraud, but they may just as well be about behaviour that is considered undesirable rather than criminal, for example behaviour that is non-compliant to internal regulations. All kinds of undesirable behaviour may be investigated by corporate investigators; however, most norm violations have an economic background (theft, fraud, favouritism in the granting of contracts, etc.). Many of the norm violations investigated by corporate security may be defined as white-collar crime in the sense of Sutherland as they often "consist principally of violation of delegated or implied trust" (1940: 3) – regardless of the question whether this violation is punishable by criminal law or not.

Corporate investigations are often followed by one of several corporate settlement options, discussed in chapter 4. Corporate settlements are solutions to norm violations, which may be derived from public law (criminal law), private law (contract law, tort or labour regulations) or internal regulations (of specific organisations). A key feature of corporate settlements is that they are a result of corporate decision

5 This is taken broadly though: it may also involve temporary workers (who have a labour contract with the temp agency instead of the organisation within which they actually work) and employees of subsidiaries.

6 However, most investigative reports also include a section on organisational issues which made the transgression possible – see chapter 4.

making within the context of organisations (as a reaction to internal norm violations) (as opposed to a decision taken by a state official such as a public prosecutor). The different corporate settlements may be argued to constitute a system of corporate justice. Within this system of corporate justice, corporate investigators and clients may be flexible, forum shopping in a way to get to the solution which is considered best suited in a certain case.

On the other side of the public/private divide is what is designated in this research as 'law enforcement'. Strictly speaking, this term only applies to police agencies. However, here the choice is made to include police, prosecution and special investigative agencies such as the investigative agency of the Dutch tax authority (the FIOD) in the definition. The reason for this is that although they certainly have different roles to play and different tasks to fulfil, these actors all contribute to the criminal investigations and the prosecution (or out-of-court settlements) of crimes. All of these actors are charged with the investigation of criminal offences according to the Dutch Code of Criminal Procedure (article 141 and 142 *Wetboek van Strafvordering*, hereafter WvSv). When specific public actors are meant in this book, they are mentioned by name. Regulatory agencies such as the Authority for Consumers & Markets (ACM), the Authority for the Financial Markets (AFM) and the Data Protection Authority (AP) are excluded from the term law enforcement as their primary focus is not on criminal prosecution but on administrative control and administering administrative measures.

'Public' and 'private' may be conceptualised in multiple ways. First of all, 'public' and 'private' may be used to signify the level of openness of for example investigations and solutions. The terms are used in this sense when the activities of corporate security within the private legal sphere are discussed. In addition, a 'sectoral approach' is used in this book, dividing the security sector along the lines of a governmental and a market sector (Jones & Newburn, 1993). This approach should be taken as an analytical tool – social reality, however, is much messier. As will become apparent in this book, public elements are introduced in the private sector and vice versa. It is important to note here that there is a high level of diversity within both the public and private sector. Many different opinions, interests and connections make for conflicts within the sectors as well as between them (Yar, 2011).

A public/private dichotomy may still be identified in terms of mode of service provision, the source and mode of financing (governmental funding or funding by a (private) organisation), and the status of investigators (whether they have powers of investigation) (Jones & Newburn, 1993). As such it is important to view corporate security in its own right and examine the activities within the sector autonomously and in relation to the public security sector. Below, sector 2 starts with an overview of

commonly used theoretical approaches.

2. Some theoretical notions on private security, corporate security and private/public relations

The use of concepts such as 'privatisation', 'responsibilisation' and 'security networks' implies a shift from the state as a main actor in the provision of security to a more diffused situation, in which both public and private actors have a central role. Although many scholars place the emphasis on the private side of crime control (see for example Shearing & Stenning, 1981), the implicit starting point remains the state. Arguments such as a hollowing out of the state, creating a control deficit in the face of growing demand for security, imply that it was originally the state who was the key actor. Historically, the state has had a limited task in the control of crime (Garland, 2001; Kerkmeester, 2005). Indeed, when it comes to *white-collar crime*, it is a well-researched fact that state intervention has traditionally been very limited (Sutherland, 1940). Only in recent years (2003), the Dutch government has instated the *Functioneel Parket* (FP), a special branch of the public prosecution office which focuses (for a large part) on fraud (for more on this, see Beckers, 2017). The issues of the state with regard to the dealing with white-collar crime do not constitute the main focus of this book; however, they are relevant to understand the popularity of the corporate security sector.

In this book, the key argument put forward by much of the literature – that the state is no longer able to provide society (here: organisations) with the security services it needs (here: a swift and efficient reaction to internal norm violations) – is put into question. As will be argued, investigations and prosecutions executed by public law enforcement agencies do (for the most part) not align with the needs of organisations. Private sector solutions, in the form of the corporate security industry, are better suited for this. This is not necessarily a historical shift, nor can it be put in terms of privatisation or responsibilisation: the historical absence of the state in the control over these matters makes such arguments untenable. Because of their importance with regard to the context in which this research has been done, some of the best-known theories about the relationships between private security and the state are discussed below. As will be apparent in the remainder of this book, these theories provide an uneasy fit with the realities of the corporate security market.

Theories explaining the growth of private security may be categorised in multiple ways. Here I choose to make a classification in terms of theories that claim that an inability of the state to meet demands for security services has led to private actors

filling the gap (section 2.1) and those that link the growth of private security to the growth of mass private property (section 2.2) (Button, 2004). These different approaches may be called by different names by different authors; however, most theories about public/private relationships fall within these broad categories. Section 2.3 reflects on the presented theory, followed by section 2.4, which provides some alternative views.

2.1 The over-burdened state – privatisation, responsibilisation and junior partner theory

Many theories on private security focus on a failure by the state to meet the growing demand for security. Different authors have termed this the 'fiscal constraint theories' (see e.g. Jones & Newburn, 1993). This term is used because the argument is that the public police organisation is subject to a restriction in its funding, leading to a situation in which the police are no longer able to cope with the demand for security. Concepts such as privatisation of security and responsibilisation of private actors are central here. By privatising some of its functions, the state tries to relieve some of the pressure. A shift from public to private is made in the provision of security (Williams, 2005). Responsibilisation is the process in which the state activates other actors to share responsibility for, in this case, crime control. In this way, the state may actually *extend* its reach instead of ceding it to the private sector.

Fiscal constraint theories may be divided into two categories. On the one hand there are the radical perspectives, posing that "the growth of private policing is an inevitable consequence of the capitalist crisis, where the state draws in the private sector to strengthen its legitimacy" (Button, 2002: 28). This is basically responsibilisation as discussed above. On the other hand, there are the liberal democratic perspectives, which state that the growth of private policing is an inevitable consequence of the increasing demands on the public police, which cannot be satisfied (Button, 2002: 29). This fits well with the idea of privatisation. The most established theory in this tradition is the junior partner theory, first introduced by Kakalik and Wildhorn. In short, this theory looks at private security actors as being junior partners to the state. Public actors may use private security actors to advance the goals of the state (Hoogenboom, 1988). The void that has been left by the police, because of an inability to meet security demands, is filled by private actors. For this to be feasible, private actors must thus be considered to be complementary to public actors: a division of labour may be discerned in which private security focuses on prevention and the police focus on repression. Private security is seen to deliver services that can be considered a preparation for the tasks held by the police and the prosecution office. For example, a security guard may detain a shoplifter who has been caught red-handed until the police arrive. The police may then continue with

criminal investigations, (ideally) leading to criminal prosecution. In such a scenario, the work of private security ends where police tasks start.

2.2 The growth of mass private property – nodal theory, anchored pluralism and loss prevention theory

In contrast to the ideas of (conscious) privatisation or responsibilisation policies, scholars such as Shearing and Stenning (e.g. 1981) see the development of private security as a result of a growth of mass private property. Because many (semi-)public spaces can now be found on private property, such as shopping malls and amusement parks, the domain of private security is growing along with it, simultaneously diminishing the domain of public police (Jones & Newburn, 1993). The main point is that power gets fragmented and divided among public and private actors alike. The growth of mass private property has in this view provided private and commercial actors with a sphere of independence, able to compete with that of the state. According to this strain of thought, complex networks combine to provide security.

One of the theories which may be seen to fit in the tradition of pluralistic models of security is the loss prevention theory which Hoogenboom (1990) termed the 'economic theory'. The theory derives its name from its emphasis on loss reduction instead of crime reduction. The economic relationships between private security and its clients are taken as a central point of departure. This theory furthermore suggests that the activities of law enforcement and private security are similar, contrasting with the views of junior partner theory about complementarity (Hoogenboom, 1990). Public and private security providers are seen as competitors in a market of security and as (partly) interchangeable (depending on the needs of the person or organisation affected) (Williams, 2005).

The ideas of nodal theorists such as Shearing, Stenning and Wood may also be viewed in this light. In short, nodal theory suggests that security is provided by a range of different providers, from which security consumers may choose. The state is seen as one of these providers but not as the primary one (Shearing, 1992). Although there is consideration for the issues connected to this type of "governing through crime" (Wood & Shearing, 2007: 5), security nodes are seen as more effective than state-provided security because they are able to utilise localised knowledge. In the words of Shearing and Stenning (1983): a new feudalism emerges. In addition to the nodal perspective on security, another pluralistic perspective is that of anchored pluralism (Loader & Walker, 2006). This perspective similarly holds that the security market is characterised by fragmentation and pluralism but contrary to the nodal standpoint, it does prioritise the state over other venues of security. The anchored pluralism stance is that the state still has a vital role to play as the main provider of justice, and as the legal 'anchor' of security provided by private actors. The reason for

this is that security is seen as a social good, which "severely precludes it being traded as a commodity and bought and sold freely on the market" (Loader, 199: 386). Loader goes on to argue that this does not imply that security ought only to be provided by the state (as this is not realistic); however, some democratic deliberation should be involved in one way or another.

Both the nodal and the anchored pluralism perspective assume that the field of security is highly fragmented, caused by the growth of mass private property, and that the state is no longer the only player when it comes to the provision of security. Additionally, though, the debate between nodal governance and anchored pluralism is partly a normative one – highly simplified it is about the role the state *should* have in the provision of security and the question whether or not security may be traded as a commodity.

2.3 An assessment of traditional private security theories

The above theories all (implicitly or explicitly) use the state as the theoretical point of departure. Whether it is a matter of privatisation and responsibilisation (conscious acts by the state) or a matter of (unintentional) growth of mass private property, the assumption remains that the state was present in a dominant way and that this presence is diminishing. As will be apparent from the following chapters, the role of the state is better conceptualised by its *absence*, when it comes to internal norm violations within organisations. It must be noted here that the presented theories do not focus specifically on private investigations but are created for the private security sector more generally. It might therefore very well be that they work better for traditional police duties such as foot patrol.[7] As noted above, the involvement of the state in the control of white-collar crime has historically been limited (Gill & Hart, 1997). In this sense, the investigation and settlement of internal norm violations can hardly be described as being privatised: for the most part, this has been a private matter anyway (Williams, 2005). A similar argument may be made with respect to responsibilisation (Garland, 2001). Junior partner theory lays emphasis on the role of private security as a subsidiary of the state, advancing state objectives in terms of governance. However, previous work has indicated that such an interpretation does not have much merit for corporate security (Williams, 2005; Meerts & Dorn, 2009). More may be expected from the pluralistic perspectives set out above, however these suffer from the same ailment: the reason for the retreat of the state may be sought elsewhere, there is still an implicit argument that private security's field of activity was once occupied by the state. In addition, the 'competition-argument' presented in the loss prevention theory must also be assessed critically (see chapter 5).

7 This has not been investigated in this research.

While the presented theories all allow for the existence of private forms of crime control, private crime control is usually seen to occur in either public spaces (such as a street) or public spaces within private property (such as shopping areas). They are thus located in specific geographical places which may be entered by the general public to one degree or another. The subject of this research does not fit this description in two important ways. First, corporate investigations and corporate justice are not limited to a specific location. Rather, the defining characteristic is the fact that there is a labour relation, providing the organisation authority over the person as an employee rather than over a specific location. Second, corporate investigations and corporate justice are not limited to *crimes*. This necessarily means that corporate investigators and the police are not interchangeable in general (although there may still be overlap between corporate security and police activities). It follows, thus, that although the above-mentioned theoretical notions have some value, they do not have a perfect fit with corporate security.

2.4 Juridification – the exploitation of the dark number of economic crime

A rare example of theorising which is specifically focused on corporate investigators may be found in the work of Williams (*inter alia* 2005). Williams (2005) claims that the growth of the market for corporate investigations is not rooted in either a failure of the state or an expansion of mass private property. Instead, the success of corporate security is a result of an "exploitation of the dark number of economic crime" (ibid.: 331). Crucially, Williams states that the traditional absence of the state in this area has led to the emergence and professionalisation of the corporate security market (see also Meerts, 2016). Through the marketing of a professional service which is directly responsive to clients' needs, instances of internal norm violations are commodified within the market for corporate security. For reasons to be discussed in chapter 3, many internal norm violations within organisations would not have ended up in the criminal justice system, regardless of the existence of a corporate investigations market (Williams, 2005). Thus, what corporate investigators do is the commodification and exploitation of a dark number of norm violations.

Three strategic resources are essential for this popularity of corporate investigative services: "(1) the framing of economic crime; (2) secrecy, discretion and control; and (3) legal flexibility and responsiveness to client needs" (Williams, 2005: 326). As mentioned, corporate investigations are not limited to criminal acts. This means that the category of behaviour that may be investigated is broader, also including for example non-criminal breaches of internal regulations. On the other hand, it also means that the focus of corporate investigators can be more narrowly defined: a corporate investigation may be limited to the behaviour the client would like to have

investigated (for example, focusing on a specific breach of contract but not on the role played by the organisation in this event). The fact that corporate investigators may work discretely, producing a report as a final product on the basis of which the client may decide on further action, is also highly valued: openness and loss of control are not standard ingredients of corporate investigations. Finally, because corporate investigators do not work within the limits of the criminal justice system, they are flexible in the solutions they may provide, taking the interests of clients into account. A criminal prosecution may not serve the private interests of the client for reasons presented in chapter 4. In these cases, another legal venue may be used (for example labour law).

2.5 Recapitulation and beyond: a public/private continuum

Based on the above, it may be concluded that public/private relations are not easily conceptualised as close cooperation or tightly-knit (hybrid) networks.[8] The following chapters focus on the day-to-day business of corporate investigators. From this, it will become apparent that much of corporate investigators' activities remain in the private sphere. Previous empirical work by Williams (2005, 2006, 2014), Gill and Hart (1997, 1999), Van Wijk et. al (2002) and Meerts (2014b, 2016) supports this statement. However, corporate security does not operate in a vacuum, free from any public involvement. As indicated in chapter 4, there are reasons for law enforcement to be involved in corporate investigations. The question remains how the cooperation that follows may be conceptualised. This is discussed in chapter 5 and 6. At this point in the book, it suffices to take the following as a starting point for public/private relations. Public/private relations can be seen as a continuum, one end representing a complete separation between public and private, the other end a close cooperation between the two. Three ideal typical forms can be identified along such a continuum:

i. Separation. Corporate security has a high degree of autonomy from public authorities: it acts as an aspect of firms' management, keeping internal order within firms, by framing economic crime in terms of secrecy, discretion, control and legal flexibility (Williams, 2005). Here, corporate security is working separately from law enforcement. Typically, cases are investigated internally and handled through a corporate settlement; additionally the threat of criminal law may be deployed as an incentive to corporate settlement, however in most cases, the public agencies are not actually brought in.

8 In the broadest sense of the word, the term 'node' is sometimes used to signify (public or private) providers of security. In this sense, (corporate) security nodes indeed exist. However, traditional nodal theory implies there are networks between state and non-state nodes. Although corporate investigators certainly do not move in a vacuum and there are multiple interconnections, in most instances it would be too much to claim cooperation – rather, the field is characterised as coexistence (see chapter 5).

ii. *Ad hoc* coexistence. As a result of strategic or normative considerations, corporate security may call upon law enforcement to assist, transferring the evidence from the investigations to the police (Klerks & Eysink Smeets, 2005). The level of cooperation may differ widely, ranging from mere information transfer to coordination (see chapter 5).

iii. Obligatory tasks. Corporate security may be a servant to law enforcement: for example in compliance functions, such as implementation of anti-money laundering regulations (see e.g. Van Erp, Huisman, Van de Bunt & Ponsaers, 2008).

Figure 1. Schematic representation of ideal types in public/private relationships

Situation iii (obligatory tasks) is about compliance functions within organisations. The context of public/private relations is different in matters of compliance, as it is about "the organisation as a potential suspect I would say. We as corporate security focus on the organisation as potential victim" [Respondent 39 – corporate investigator]. As explained in section 1 of this chapter, the research focuses on corporate investigative services, which excludes situation iii from the scope of the research. This does not mean that corporate investigators are not involved in compliance matters or in investigations as a result of obligatory tasks.

Situations i and ii then, are central to this research. Much of corporate investigators' activities remain in the private legal sphere, in which a large measure of autonomy from law enforcement authorities may be claimed by corporate investigators. Much of what is discussed in chapters 3 and 4 is based on separation, rather than cooperation, and may be conceptualised as situation i (separation) above. However, this separation is not absolute. As a result of pragmatic and normative considerations, corporate investigators or clients may initiate law enforcement involvement (or, alternatively law enforcement may be involved through criminal justice investigations regardless of any conscious decision by corporate investigators or clients). It is argued in this book that 'cooperation' may be a misleading term for such relations, and 'coexistence' is used instead to signify public/private relations in situation ii. The words '*ad hoc*' are used to indicate that public/private relations generally are a result of a specific

case, rather than any form of long-term cooperation efforts. Chapter 5 further breaks down the concept of *ad hoc* coexistence, by presenting a typology ranging from (private to public) information transfer, through (minor) mutual information sharing, to coordination.

3. Methodology

The fieldwork data gathered for this research have been collected through triangulation of qualitative research methods (Noaks & Wincup, 2004). The research questions described in the introduction to this chapter are mainly descriptive and exploratory. Qualitative methods are best suited to get the rich information necessary to answer these types of research questions (Mortelmans, 2016). In addition to the main research methods, to be discussed below, supplementary information was gathered in multiple ways. To start with, previous research has been used in the form of literature, and the relevant legal frameworks and other legal information were assessed. During the course of the research multiple academic and practitioner seminars and workshops, as well as networking events, were attended. The observations made and informal conversations held at these different events proved useful as background information and, in addition, were very helpful with regard to entrance into the field. In March 2016 a seminar was organised in the context of this research, which was hosted by John Moores University Liverpool. The seminar served as a platform for discussion between the academics, corporate investigators and law enforcement professionals who participated, and myself. In addition, three corporate investigators were interviewed. The aim of the seminar and interviews was to receive input from UK experts, to check the research data gathered in the Netherlands against the British situation. Although very helpful in this sense, the information gathered in Liverpool is not sufficient to make a comparison between the UK and the Netherlands (see chapter 2 for more on this) – neither was this the intention of the seminar and UK interviews.

3.1 Interviews

The central research method is the semi-structured open interview. This type of interviewing is often used in qualitative research and is particularly helpful for exploratory research. In a semi-structured open interview a topic list is used to ensure relevant subjects are discussed (Beyens, Kennes & Tournel, 2016). Although the topic list contains a logical ordering, a key feature of an open interview is the flexibility of the interviewer and the interview process. As long as all relevant topics are discussed, many variations may occur in the order of subjects. In addition, topics may be added or deleted during the interview, according to the knowledge of the respondent (Baarda, De Goede & Van der Meer-Middelburg, 1996). In this research three different respondent groups were interviewed and three topic lists were used for these groups. Depending on the type of respondent, some questions were asked in a different way, some topics were added and others deleted. However, every interview discussed the following subjects: professional background of the respondent; types of cases in which corporate investigators are involved; reasons for corporate investigations/ settlements; process of the investigations; process of settlements; legal frameworks; public/private relations; and general opinion regarding the existence of corporate security. Every interview was concluded by the question whether the respondent felt any important subject had been neglected and whether he or she had suggestions for prospective respondents. The topics included in the topic lists served as conversation starters and reminders. In response to the information provided by the respondent, further probing was executed (Beyens et al., 2016).

The type of interview used for this research may be defined as an expert interview (Baarda et al., 1996). This type of interview poses its own unique issues, in addition to some benefits over a 'normal' interview. Expert interviews tend not be emotionally difficult for a respondent. The subject matter of interviews was such that it might be sensitive for the reputation of organisations, however, respondents were not personally emotionally involved. Another advantage of an expert interview is that respondents are generally well-informed, which means that much information may be gathered and the interview may be more efficient. On the other hand, experts, and especially those in management and higher positions are often pressed for time and hard to reach because they are shielded by administrative staff. Most respondents indeed indicated that they only had a limited timeframe available for the interview – however, as may be deduced from the average duration of interviews, most interviews were nevertheless of considerable length. Through the use of gatekeepers, access was granted quite easily (see below). Only one request was denied (the reason being that the respondent did not want to participate in any academic research) and one potential respondent failed to reply to repeated requests to reschedule a previously cancelled interview. Expert interviews call for a different approach than other

interviews because respondents are so well-informed. Repetition of questions and questions to which the answer seems obvious are not appreciated by respondents. Expert respondents may not feel they are taken seriously with this kind of questioning. The respondents in my research were eager to talk about their work (as they felt the research was a validation of the importance of their work).

A total of 59 expert interviews form the basis of this research.[9] The duration of interviews was on average one hour and eleven minutes, with outliers of twenty-three minutes (the shortest interview) and two hours and fifteen minutes (the longest interview). Most interviews (50) were audiotaped and transcribed, although some respondents (9) preferred not to be audiotaped. In these instances extensive notes were made and typed up directly after the interview was concluded. The sensitivity of the subject matter was the reason given by the respondents who did not want to be audiotaped. Some respondents requested a transcript of the interview and this was provided to them. All interviews were done face-to-face and most were done individually (51). For practical reasons four interviews were duo interviews. Most respondents were male (49), while ten respondents were female. Most respondents fall into the age group 40 to 60 years old. The *Randstad* was the central location of most professional activities of most respondents, which consists of the four biggest cities of the Netherlands (Amsterdam, Rotterdam, The Hague, Utrecht) and their surrounding areas; however respondents can be found all over the Netherlands. The average education level of respondents was high (academic education), although police respondents generally had a lower education level (being trained within the police organisation itself).

The three groups of respondents consisted of corporate investigators (33), law enforcement professionals (16) and clients (10). Among the corporate investigator-respondents a differentiation can be made in respondents working for private investigation firms (10), in-house security departments (18), forensic accounting departments (5) and forensic (departments of) legal firms (3). In this last group (forensic legal investigators), respondents had a double role as respondents could be both investigators in some cases and act as a client in other cases.[10] Law enforcement professionals consisted of professionals working for the police (8), prosecution (5) and FIOD (3). Respondents falling within the category of clients were HR personnel,

9 56 of these interviews were conducted in the Netherlands. An additional 3 interviews were done with corporate investigators in the UK (Liverpool).

10 Because they were approached and interviewed as clients, these respondents are counted in this category (which is why the numbers of investigators do not add up to 33 here). However, because these respondents also occasionally act as forensic legal investigators, they have provided useful insight. At the time of interviewing, the forensic legal investigator was a rather new phenomenon in the Dutch corporate security sector, which is why so few forensic legal investigators have been interviewed. Only during the research did this group emerge from the other interviews.

(labour) lawyers, or general management. As may be gathered from these numbers, not all respondent groups are represented to the same extent in this research. Because the research questions are for an important part focused on the activities of corporate investigators, and because of the wide variety of backgrounds within this group, the decision was made to focus on corporate investigators, which explains why this respondent group is relatively over-represented.

Table 1. Overview of interviews

Number of interviews	59[a]
Average duration interviews	1 hour 11 minutes
Corporate investigators	33[a]
Private security firms	10
In-house security	18
Forensic accountants	5
Forensic legal investigators	16
Law enforcement professionals	3[b]
Police	8
Prosecution	5
FIOD	3
Clients	10
HR, labour lawyers, management	7
Clients/forensic legal investigators	3[b]

[a] Three of these were conducted in the UK.
[b] These are the same respondents. They are only 'counted' in this table as clients.

3.2 Observations

In addition to the interviews, observations produced valuable data. Above, mention has been made of casual observation as part of participation in seminars and practitioner events. A more structured approach was taken in two observation periods with two different companies. Observations are often used in criminological research

and have the advantage over other methods of data collection that they can reveal information that is hard to obtain when for example directly asked (Bijleveld, 2009). The choice was made to do observations in this research to get more insight into the daily activities of corporate investigators and the (often subtle) relationships with (and frustrations about) the criminal justice system. The mere fact that the researcher 'is there' may provide valuable information (Zaitch, Mortelmans & Decorte, 2016). Meaning may be derived from situations, which cannot be asked through interviews. In this way, the observations were very useful. Because of the setting in which the observations took place, they can be defined as 'institutional ethnography': in this type of observation, the focus is on the institutional reality of the setting (ibid.).

Observation as a research method is a flexible technique (Zaitch et al., 2016). Therefore, the observations were not highly structured, although an observation schedule was used to ensure focus. The observation schedule contained the process of investigations, the types of settlements and public/private relations as the main topics. It was used as a guide but not as a strict tool for observation. Observations were recorded by a daily record sheet, in which detailed notes were recorded. Some parts of the observations were participant, although it was clear at all times what my role was (I was there as a researcher, not a corporate investigator) (ibid.). Most of the time spend during the observations was not participant in this sense: although I was present and did execute some minor tasks for the observation companies, my main role was that of *observant*, not participant.

The observations were executed in two separate observation periods. During the observation periods, a full-time position was obtained and full access to the systems of both observation companies was granted.[11] Both observation companies granted me an access card or key to allow me to enter the premises independently, an employee account and an email address to access the digital environment. During the observations, I have been present full-time during working hours, participated in meetings and have had multiple informal conversations. In addition, during both observations, I have been able to witness an investigative interview by investigators. In both observations, I have selected reports and other information relating to finalised corporate investigations. These were analysed using a topic list (see section 3.3 for more information). Other internal documents, such as codes of conducts, yearly reports and information published on the intranet were also used for analysis. During both observation periods, I was granted extensive access to all information necessary to me (after signing a confidentiality agreement). Investigators and other staff were very helpful, offering to help me gather information, explain matters to me and they were very willing to talk about their work and showed great interest in my research.

11 I cannot, of course state with a hundred percent certainty that no information was withheld. However, I had full access to the computer systems and any information requested by me was provided.

It must be noted that observation material is (maybe to a greater extent than information gathered through other methods) liable to interpretation bias, as the role of the researcher is larger in an observation setting. By entering the observation setting, the researcher necessarily influences the setting (Zaitch et al., 2016). This was most apparent during observation 2, when people started out somewhat cautiously towards me. This attitude changed rather quickly, however. In both observation settings there seemed to be a great passion for the profession. The workload for investigators was high in both observation companies, however employees indicated that there are also 'slow' periods during the year.

Observation 1 was executed at the very beginning of the research (mid-October to November 2012) and lasted seven weeks. The observation company (1) was a private investigation firm, with at the time five people involved in the investigations (including the two directors) and one secretary. The backgrounds of the investigators were diverse, ranging from a legal, criminological to an accounting background. Two of the five investigators had previously worked as a law enforcement professional. The clientele of this corporate security company was diverse as well, but assignments mostly originated from medium-sized businesses, (semi) public organisations and law firms. With some clients, framework agreements had been made, which ensured prospects to future assignments to a certain extent. This company is referred to in the remainder of this book as Observation Company 1.

Observation 2 was done near the end of the fieldwork period (beginning of February to March 2015) and lasted six weeks. The observation company (2) was a large Dutch company and the setting of the observations was the in-house security department of said company. The security department was at the time of observation headed by a manager, and divided in three parts (compliance, internal investigations and external investigations). All three sub-departments were headed by their own manager. The observations were done within the internal investigations department, which consisted at the time of observation of eleven employees (in addition to one manager and two secretaries). The internal process was structured in such a way that the department had three full-time investigators (all with a police background), three analysts (focusing on desk research) and five 'intake-employees' (forming a helpdesk where incidents might be reported by employees). This company is referred to in the remainder of this book as Observation Company 2.

3.3 Case studies

An additional purpose of the observations was to gather material for case studies, consisting of corporate investigations reports and additional information on these investigations. A case study may be defined as a detailed, rigorous study focusing on a certain case or object. As is common in case studies, multiple ways to gather information about the case were used (Leys, Zaitch & Decorte, 2016). In total, twenty-one reports were selected, ten of which were investigated by Observation Company 1 and eleven of which were investigated by Observation Company 2. Cases were selected based on the following criteria: they should provide enough information (an investigation report or other substantive information needs to be present) and the case should involve a labour relation (internal norm violation). In addition, the cases which were selected can be divided in those where no report to the authorities was made (14) and those that did involve a report to the authorities (7).

Cases were analysed using a topic list containing main topics such as the scope and content of the case, methods of investigation, the settlements chosen and the involvement of law enforcement actors. With the aid of this topic list, each case was analysed and recorded. The selected cases were all (but one) person-oriented and the number of involved persons ranged from one to entire organisational departments (consisting of a large multitude of employees). There was a variety of norm violations (both criminal and non-criminal) but in general the norm violations had a financial component (mostly embezzlement). The norm violations that were investigated in the cases ranged from small (petty theft or the leakage of minor information) to substantial (millions of euros in fraud). A broad-scope exploration of all the cases at file at both observation companies revealed a large variety of norm violations, ranging from financial issues such as fraud, theft, corruption to integrity issues more generally such as breach of privacy, breach of trust, sexual harassment and unauthorised ancillary activities. Although the presentational style differed between Observation Company 1 and Observation Company 2, the same components could be found in both the investigative process and the way of reporting about the investigations. Cases were not selected at random but purposively, so as to ensure enough information about each case would be available.

In addition to the investigative reports, which were the basis of the analysis of cases, other documents such as the (investigative) interview reports, the investigative journal, court rulings and media coverage were analysed. Furthermore, the investigators who had worked on the case were asked to answer certain questions and there were multiple informal conversations with investigators about the cases.

The information collected through the case studies was processed in Microsoft Word and coded and analysed with the aid of Atlas.ti, together with the interview and observation data. In addition, the collected information was contrasted with literature. This was an ongoing process and codes and topics were subject to improvement during this process (Decorte, 2016).

3.4 Some methodological reflections

As with any type of research, there are some specific methodological challenges which warrant some attention. First, the more general issues of validity and reliability are discussed. Following this, some more specific issues are highlighted. This section is concluded a reflection on my role as a researcher.

3.4.1 Internal and external validity

The term internal validity refers to the 'credibility of claims': can the information produced in the research be said to be 'true' (Maesschalk, 2016)? In interview settings, there always is the risk of socially desirable response tendencies (Beyens et al., 2016). One measure taken against this was not to react to questions from respondents about my opinion (see below). Although social desirability cannot be eliminated with certainty, there does not seem to be a very big risk regarding social desirability in this research for several reasons. First and foremost, the subject matter of this research is not sensitive to the respondents *personally* (although it might be to their organisation). Secondly, respondents were experts on the subjects at hand (and many were also experts on investigative interviewing).[12] As explained below, respondents readily assumed the role of expert, there to provide me as a researcher with insight into their social reality. Thirdly, respondents generally expressed well-formulated and strong opinions, which might be an indication that these were in fact their opinions. Some subjects, such as public/private relations appeared to reproduce a 'mantra' which is prevalent in the research field – i.e. that cooperation is desirable. However, further probing revealed that some respondents indeed held this opinion, while others produced a more nuanced view upon reflection. I have endeavoured to remain keenly aware of the possibility of social desirability or other answering tendencies and I have used further probing to check the validity and reliability of respondents'

12 This last circumstance had advantages and disadvantages. A considerable advantage was that most respondents had no objection to be interviewed or to be audiotaped, as they were familiar with both. A disadvantage that may be identified was that because of respondents' familiarity with the process of interviewing, many interview techniques did not have the desired effect. They either provoked (mild) irritation (for example in the case of repetition of questions in different terms) or they led respondents to fill out the course of the interview themselves by anticipating questions. This led me to change my strategy, treating the topic list as a more flexible guideline. In the end, all interviews provided the information they were intended to provide.

answers. Another measure taken to avoid reproducing possible socially desirable answers as 'facts' in my research, was the use of triangulation. Qualitative research methods produce rich data. The methods used here – interviews, observations and case studies – produce data with a high measure of internal validity because they give the researcher the opportunity to check the data (Zaitch et al., 2016). The fact that multiple research methods have been used, producing data from different sources and gathered in different ways (triangulation), also benefits the internal validity (Maesschalk, 2016).

When it comes to external validity, or the measure in which the results of this research may be generalised to the whole field of corporate security, more caution is warranted. In the strictest sense of the word, external validity may only be achieved when a sufficiently large sample has been used and the sample has been produced in a correct way (preferably at random). This is generally only the case in quantitative studies. Qualitative research data is richer in content than quantitative data, but the collection and analysis of qualitative data also takes more time. This makes it very difficult to get a sample which is large enough to be representative for all relevant actors within the research setting. In addition, as chapter 2 shows, there is no clear overview of the number of corporate investigators in the Netherlands. Finally, the covert nature of many of corporate investigators' activities makes access challenging (see below). Choosing respondents at random would most likely not produce much useful respondents within the respondent groups of clients and law enforcement professionals (even if a complete list of all possible respondents could be obtained) – and even if useful respondents would be found, access without a gatekeeper would be very challenging.

However, in a more general sense, some measure of generalisation may be possible in qualitative research as well (Maesschalk, 2016). Although efforts have been made to gather information about the four groups of corporate investigators identified here, not all groups were interviewed to the same extent, with in-house investigators being best represented within the respondent group. The same goes for clients and law enforcement professionals. This approach was purposively used to gather data in the most efficient way. Within the group of respondents, saturation of data was reached at the end of the fieldwork: the general patterns identified here may therefore be considered to be a good representation of the views of respondents.

3.4.2 Internal and external reliability

Internal reliability refers to the reproducibility of the research by other researchers (Maesschalk, 2016). This may be realised by providing other researchers access to the data. However, in doing so the confidentiality of the data may be compromised and respondents would no longer be anonymous. This situation is highly undesirable.

As such, internal reliability is attained by making the manner in which information has been gathered and the mode in which this information is used in this research, transparent.

In light of the discoveries of scientific fraud in social sciences in the Netherlands and beyond, transparency seems to be more warranted than ever (Van de Bunt, 2015). The use of quotes serves a double purpose in this way: quotes may highlight and emphasise a certain finding by using an example given by respondents themselves. In addition, quotes may serve as an indication that data in fact has been gathered.

External reliability of a research is achieved when new research produces the same results (Maesschalk, 2016). Again, this is possible in an experimental setting but very hard to achieve in qualitative research. The best a qualitative researcher can do is being transparent about his or her own role in the research and collecting information. Section 3.4.4 focuses on my role in the research in more detail. First, the next section discusses the matter of establishing trust within the research setting.

3.4.3 Trust – access and confidentiality

Trust is hard to establish within an interview setting because an interview has a short time-span. It is therefore imperative that respondents trust that the information they share is treated as confidential. In this light, informed consent is essential. No parts of this research were covert and it has been clear to all respondents and other participants what my role was. Informed consent has been attained at every step (Vander Laenen & O'Gorman, 2016). For all methods used in this research (except open source data), confidentiality was guaranteed from the start. No information is presented in this book or in other publications based on this research, which may lead to the identity of respondents, specific organisations or specific cases. There is, of course a downside to this, as it makes the data gathering process less transparent and harder to duplicate. Protection of respondents is prioritised over transparency in this research. Anonymity is ensured for multiple reasons. First, the information gathered is sensitive information. Corporate investigators and law enforcement professionals deal with much sensitive information and it would be detrimental to the persons involved if this information would be openly discussed in detail in this book. Ensuring anonymity therefore has, secondly, the additional benefit that access to information is granted more readily. Third, much of the specifics which would be detrimental to anonymity are not relevant to the questions posed in this research. In this way, the content of the research is not affected by this choice.

The way in which respondents are approached is also relevant with regard to trust. Respondents were contacted through email or telephone contact, based on contact information received through gatekeepers and other respondents. Through contacts established in previous research in the field (Dorn & Meerts 2009; Meerts & Dorn 2009;

Meerts 2013), gatekeepers were approached. Gatekeepers are key contacts who are in a position to make introductions and grant access (Noaks & Wincup, 2004). This mode of entry is especially useful for difficult-to-reach groups, such as experts (Baarda et al., 1996). For this research, gatekeepers proved essential in gaining access. Experts are generally hard to access and in the corporate security market, which is largely reliant on discretion, it is even more difficult. Adding to that the fragmentation of the field, the small amount of cases that are reported to the authorities and the fact that clients hardly ever publicise that they have ordered internal investigations to be done, getting access without a gatekeeper would have been very difficult indeed.

Three different gatekeepers were used in this research. Once interviews were conducted, each respondent was asked to suggest new respondents. In this way, every respondent acted as an additional gatekeeper as well. This method of gaining access is called snowballing. Through snowballing, one may reach valuable respondents in an efficient manner (Mortelmans, 2016). Especially in the case of clients (who are difficult to identify because much of corporate security's work is not publicised in the media) and law enforcement professionals with experience with corporate investigators (who are difficult to identify because many corporate investigations are not reported to the authorities), the snowball method proved effective. However, a sample achieved through gatekeepers and snowballing is also a selective one, as it depends on the network of previous respondents. To mitigate this, multiple gatekeepers were used. In addition, at a certain point in the research, saturation of respondents occurred: the same names (who had already been interviewed) kept reoccurring, independently of the gatekeeper through which the respondent had been approached (ibid.). The observation companies were approached after contact had already been established through interviews.

3.4.4 Getting captivated – a reflection on the role of the researcher

A reflection on the role of the researcher is essential to any type of research: researcher bias may occur because of the methods used, the choices made and the interpretations the researcher produces. As mentioned, observations (and to a lesser extent interviews and case studies) are liable to this as well. During the interviews, my role as researcher now and then became apparent as some respondents tried to 'test' me: by asking some questions they tried to find out whether I had sufficient knowledge with regard to the subject matter. Depending on the situation, I reacted by either showing my knowledge or assuming ignorance. The strategy I chose depended on my assessment whether or not showing knowledge would steer the respondent in any way. For example, when I was asked what I thought were the reasons not to report to the authorities, I refrained from answering the question. In this example, revealing the reasons mentioned in literature and previous interviews might have directed the

respondents in a certain direction.[13] However, I did present basic knowledge of the law when questioned: this is factual information and in this context (in which the respondent was keenly aware of the law because of his professional background) it would not steer the respondent in a certain direction. I was careful not to display any opinions during the interviews but was less hesitant to do so after the interview had been finalised and informal conversation ensued. Assuming either ignorance or knowledge had the added benefit of respondents opening up more. Respondents were experts on the subjects at hand and it was important to acknowledge this in the interviews (Beyens et al., 2016). The fact that I am a young woman may have been beneficial as well. Most of corporate security and law enforcement is "dominated by old men" as one manager during observation 2 stated.

During the observations, most people reacted in a positive and curious manner, although it took some time to establish trust (Zaitch et al., 2016). After trust was established, more information became available and employees of the observation companies displayed much effort to share information with me and explain certain mechanisms. This is a good example of what Roks (2016) means when he writes about the changing role of the researcher over time. As the relationship with the research setting changes, so does the measure of access. The immersion in the field was not of such nature that capture was a real danger. Capture (also known as 'going native' or 'over-rapport') refers to the situation in which a researcher identifies with his or her research field in too great a measure, leading the researcher to miss information and results and interpretation of information to be affected (Zaitch et al., 2016). My relationship to my field of research and my research subject is not to be defined in the sense of capture, but it can be aptly described as *captivation*. Captivation in this context has a more positive meaning than capture: being captivated by the research subject may facilitate a more in-depth investigation and discussion. My captivation with (or fascination for) the corporate security market has promoted a critical stance towards existing private security theories, the fieldwork of this research and the conclusions arising from the fieldwork (as opposed to being captured, which may promote tunnel vision).

13 For example, literature places much emphasis on the role of reputational damage when it comes to reasons not to report a norm violation to the authorities. In contrast, respondents attach much less importance to reputation.

Book structure

In the following chapters, the research questions presented in the introduction to this chapter are answered, using the data collected in this research. The legal context within which corporate investigations and settlements occur is first discussed in chapter 2. This chapter also identifies the four groups of corporate investigators which are central to this research and discusses some notable differences between them. An important conclusion of chapter 2 is that the corporate security sector is fragmented in multiple ways. The four main professional groups of corporate security providers – private investigation firms, in-house security departments, forensic accountants and forensic legal firms – all have their own specific selling points and, importantly, their own legal frameworks. This leaves room for clients to actively search for the investigator who is best suited to investigate the norm violation the client is faced with (forum shopping). While legal frameworks may differ widely among different corporate investigators, activities are largely similar (partly as a result of diversification of the field). Because many corporate investigators follow similar norms (such as an emphasis on due process), corporate investigators of different backgrounds tend to adhere to similar rules in practice.

Chapter 3 goes on to describe the investigative process and the methods that may be used to gather information in the context of corporate investigations. The process is discussed from the assignment confirmation to the report that follows from the investigations. Corporate investigators are not charged with the investigation of criminal offences according to the Dutch Code of Criminal Procedure (article 141 and 142 WvSv) and as such do not have formal powers of investigation. In addition, corporate investigators tend to avoid terminology used in criminal justice proceedings. This sets them apart (symbolically) from law enforcement agencies. However, they have extensive access to information through the rights the organisation has as an employer. As such, corporate investigators have extensive possibilities of investigation within the limits of what they are allowed to do.

Chapter 4 follows the investigative process further, by describing what happens next: the settlements which may follow corporate investigations. Four categories of solutions are presented, originating from different legal venues: criminal law, the Civil Code (including private contract regulations and labour law) and internal regulations of organisations. Corporate justice achieved through corporate settlements is a good example of forum shopping: the solution which is most beneficial to the client is chosen. Chapter 4 also discusses reasons organisations may have to either avoid a report to law enforcement authorities or actively involve the authorities through a report. In general terms these may be divided into strategic and normative considerations.

Chapters 3 and 4 largely represent situation i (separation) presented in Figure 1 above. In chapter 5, the focus shifts to situation ii (*ad hoc* coexistence). Public/private relations in the field of corporate security are explored, focusing on a typology ranging from (private to public) information transfer (A), to (minor) mutual information sharing (B) to coordination (C). Some formalised attempts to cooperation, aimed at establishing a longer-term relationship, are discussed but these are yet to be successful. Public/private relationship seem to be likely to remain based on *ad hoc* occurrences because of the nature of corporate investigations, corporate justice and the types of norm violations that are usually the object of corporate investigation processes. Strategic use of different legal venues and forum shopping make relationships fluid and *ad hoc*. In this chapter, material derived from the case studies is explicitly used to clarify public/private relationships in the context of coexistence.

Chapter 6, finally, concludes the book by providing an answer to the research questions and discussing the major concepts arising from the research: the concepts of forum shopping, the autonomy of corporate investigators within the private legal sphere, coexistence and non-contractual moral agency are used to discuss the unique nature of the corporate security market within the field of (crime) control. The role of private and public interests is furthermore discussed and attention is paid to the issue of the governance of the corporate security field. Some suggestions are given with respect to the regulation of and control over the corporate security market. Chapter 6 furthermore provides a discussion and reflection on the research. It concludes this book by looking ahead to future research.

Chapter 2

Legal frameworks

The legal context for private investigation firms, in-house security, forensic accountants and forensic legal investigators

Introduction

There are multiple actors with different backgrounds active in the corporate investigations field (Williams, 2014: 59). These different actors have their own laws and regulations to adhere to, which are described in this chapter. Some rules are specific to the professional group, while others apply to all. In addition to the specific rules applicable to them, corporate investigators with different backgrounds seem to adhere to a similar set of general principles of law (most notably fairness, proportionality and subsidiarity). These general principles of law are codified for some but not for others (NVb, 2014; NIVRA/NOvAA, 2010). The differences in legal frameworks provide some corporate investigators with strategic advantages compared to others. As this chapter will show, all four groups have their specific selling points (which may or may not be directly related to the legal frameworks): in-house security departments are internal to an organisation, therefore providing a unique level of specialised knowledge about the organisation. In-house investigators and investigators working for a private investigation firm often also have a police background and are skilled interviewers. Private investigation firms are furthermore permit-holders and are external to the client, bringing with them an air of objectivity. This latter circumstance also applies to forensic accountants, who furthermore may be seen as financial experts. Investigators with a legal background finally, are experts in the legal interpretation of the findings and they may assist with settlements. In addition, forensic legal investigators may make use of their legal privilege to protect the outcomes of the investigations.

The fact that there are different rules for different players makes for a rather scattered field, in which it is not altogether clear for those involved which rules they have to adhere to. The way in which the topic is handled by legislators does not really do much in clearing up this confusion. The issue of legislation pops up every once in a while in Parliament, however this has not lead to systematic, uniform legislation (Klerks, 2008: 17). An interesting point made by White (2014) in this regard is that legislators tend to regulate the kind of private security activity that is most visible, and thus, threatening to the legitimate position of the police. White focuses on the difference in regulation of in-house and external security (guards) in the UK more generally, however his argument could be extended to corporate investigations. The legal framework provide by the Dutch Law on Private Security Companies and Private Investigation Firms (hereafter: Wpbr) is mainly focused on the more traditional security activities. There are many specific rules in this law about security guards, cash-in-transit and private alarm companies but on private investigations the law is very general. The legal framework seems indeed focused on the most visible parts of the private security industry, as it mostly regulates such things as uniforms. The

inclusion of a requirement for private security firms to notify the police about security activities is interesting in the absence of such an obligation for private investigators. As this chapter shows, within the already limited mention of private investigations in the Wpbr, the law seems even more narrow as it specifically focuses on the most visible corporate investigators: the private investigation firms. The other types of investigators discussed in this chapter are excluded from the Wpbr.

While it is certainly not the case that the sector is *unregulated*, one might suggest that the consequence of the dispersed nature of regulation is that many opportunities for forum shopping are created. Forum shopping is the process in which parties pick and choose from certain 'forums' to suit their specific interests. In international business relations, parties will for example choose a jurisdiction for the settlement of a dispute that will produce the most favourable outcome (Whytock, 2010). In the context of this chapter, it means that both clients and (to a certain extent) corporate investigators may choose from different legal frameworks. As this chapter illustrates, in the Netherlands, different actors are liable to different legal frameworks. The diversity in the legal frameworks applicable to corporate investigations is a prime example of the interdisciplinary nature of the sector and the remarkable position of corporate security. Corporate security constitutes a commercial sector (regulated by private law), offering a product that may have an outcome either relating to public law (criminal proceedings), private law (contract or tort), labour law (labour relations) or internal regulations. Chapter 4 of this book focuses specifically on these different outcomes in the form of corporate settlements.

While there are also other players active in the field of (corporate) investigations,[14] the focus in this chapter (and this book) is on four main groups: private investigation firms, in-house security departments, forensic accountants and forensic legal investigators. The different rules and regulations applicable to these four groups, and their respective advantages for clients compared to other investigators, are discussed. Some particular legal requirements are left to be discussed in more detail in following chapters, as they for example apply specifically to certain investigative methods.

Although the four professional groups of corporate investigators have their own specific legal framework, some general rules apply to all. Section 1 starts by focusing on these general legal frameworks. Sections 2 to 5 go on to discuss the specific legal frameworks applicable to different corporate investigators. All of this leads to

14 For example, information-companies, debt collection agencies, IT specialists and companies specialising in employee absence might also be involved in investigative activities. Many of these actors do not have (or need) a permit as discussed in section 2 of this chapter because they are not investigating individuals ('natural persons'). The focus in this research is on those professional investigators who investigate (persons) as their core professional activity.

differences between corporate investigators, leaving room for clients to choose the corporate investigator who is most suited for their present situation (forum shopping). Section 6 looks into the respective selling propositions of each group compared to others, through a focus on the themes: professional background and knowledge, and legal frameworks and position with respect to the client. A discussion concludes the chapter, reflecting on the legal context of different corporate investigators.

1. General rules and legal frameworks for investigations

One of the defining characteristics of criminal investigations is their far-reaching nature. In legal terms, 'investigating' is defined in the Dutch Code of Criminal Procedure as 'the investigations into criminal acts under auspices of the public prosecutor, aimed at a decision in criminal proceedings' (article 132a). 'Investigating' in this sense is limited to the actions of law enforcement officers (article 141 & 142). Powers of investigation are exclusively granted to law enforcement agencies and since a large scandal in the 1990's, the more intrusive of these are explicitly regulated in the Dutch Code of Criminal Procedure as special powers of investigation ['BOB'] (Title IVa and Title IV). Corporate investigators do not have powers of investigation (see also chapter 3) so these laws do not apply to their work. A corporate investigator is, however, bound to adhere to the Criminal Code, as are all natural and legal persons. This means, for example, that they cannot detain someone or use force against him and that they have to respect other people's rights to privacy.

1.1 The Data Protection Act (WBP)

With respect to privacy, there is specific legislation which is relevant to corporate investigators, the WBP [Dutch law safeguarding the protection of personal privacy].[15] This law applies not merely to corporate investigations, however the WBP serves as an important guide for these as well. Although the WBP restricts the gathering and use of personal data, it simultaneously leaves room for this. For example, article 23 under 1b, states that personal data that have been made public by the involved person may be used. In a time when many people are actively using social media and hereby exposing much personal information, this means that corporate investigators may gather and use personal data quite easily (see also chapter 3).

15 Chapter 3 discusses some specific parts of the WBP more in-depth, when it comes to the details of investigative activities.

Many rights and possibilities of corporate investigators are derived from the rights the client has as an employer (Williams, 2014: 68). In general terms, employers are allowed to exercise control over their employees, however they should take certain restrictions into account (CBP, 2015a). Firstly, there should be a legitimate reason for such control, which may be constituted by suspicions of criminal or other undesirable behaviour. Furthermore, less intrusive ways to gather the necessary information should have proven ineffective (in accordance with the principle of subsidiarity). The control should also be reported to the Data Protection Authority (AP – previously called CBP) and the Works Council of the organisation will have to grant approval. Employees should furthermore be made aware of the rules, the possibility of control and the manner of control (e.g. through a code of conduct). Finally, the employer should respect the right to confidential communication of his employees. This does not exclude the possibility of control over for example telephone or email communications, however the employer should distinguish between professional and personal communications. In case of suspicion of a crime, the employer is allowed to record telephone conversations. If the control that is to be exercised is covert, there should be a reasonable suspicion of a crime committed by one or more employee(s). The AP should approve this type of control in advance and the employee(s) should be made aware of the covert control after it has been completed (ibid.).

With regard to some specific types of control the AP has issued guidelines, for example in case of camera usage (CBP, 2015b). The principles of law of subsidiarity and proportionality are important here. Because the breach of privacy is substantial, employers should weigh the necessity and the interests being served with the use of cameras against the interests of the involved person (in accordance with the principle of proportionality). If the goal that is to be reached by the use of cameras may be reached through less intrusive means, these should be applied (subsidiarity). In addition, the use of cameras should be reported to the AP and the Works Council will have to grant approval. Hidden cameras are allowed in special circumstances, one of which is (the investigation of) suspicions of theft or fraud. This type of camera usage may only be of temporary nature (ibid.).

The above possibilities for employers and, by extension, corporate investigators, leave ample room for information gathering in the context of corporate investigations (see also chapter 3). Article 27 WBP states that the Data Protection Authority should be notified of automated use of personal data. The use of certain personal data is restricted though: article 16 of the WBP prohibits use of personal data regarding religion, health, criminal past, etc. unless the law has granted an exception. One of the exceptions with regard to data regarding someone's criminal past is made in article 22 WBP, which for example states that one may use the data to protect ones interests. This means that employers (and by extension in-house investigators) are allowed to

use and process data about (prospective or former) employees. Interestingly, article 22 (under 4) of the WBP explicitly frees parties that have a permit based on the Law on Private Security Companies and Private Investigation Firms from the prohibition to work with (gather/process) criminal data. Not all corporate investigators have such a permit though (see below). Those who do not have a permit might still be able to use this kinds of data, as sub c states that this is possible when 'proper measures' are taken and the Data Protection Authority has done prior investigations on its permissibility.[16]

1.2 The Civil Code (BW) and anti-money laundering legislation (Wwft)

Another general set of rules relevant to corporate investigators, in addition to criminal law and data protection legislation, is the system of the Civil Code (BW). The Civil Code is important when it comes to settlement of internal norm violations (see chapter 4), but it is also a more general guidance. The Civil Code captures the relations between civilians and private entities and article 6:162 BW states that anyone who commits a wrongful act towards another may be held liable to repay damages. On the basis of this article, corporate investigators may be held accountable for any wrongful and unlawful actions during their investigations. Chapter 7 section 10 BW furthermore concerns the labour relations between employer and employee and provides the employer with certain rights, for example to set rules and control the compliance of said rules (article 7:660 BW). This gives the employer (and by extension, a corporate investigator) room to control his employees, investigate when necessary and take (disciplinary) action (Schaap, 2013).

Finally, the Law Preventing Money Laundering and the Funding of Terrorism (Wwft) may compel corporate investigators to notify the authorities of 'irregular transactions'.[17] This type of regulation relates more to the compliance functions of corporate security, however it may be relevant to investigative activities as well. This may for example be the case when corporate investigators find a fraudulent transaction which benefited the client – every further action with the money would be money laundering. Corporate investigators have explicitly been made subject to the Wwft in 2013 (Minister of security and justice, 2013). The Wwft compels

16 In addition to national privacy laws, international and EU privacy regulations are relevant to corporate investigations as well. Corporate investigations may cross national borders and so may personal data. The Dutch privacy law is in accordance with the EU directive on privacy, dating from 1995. However, as of May 2018 new EU privacy regulation will come into force (see http://ec.europa.eu/justice/data-protection/). Were relevant, specific international and EU regulations are mentioned throughout the book.

17 This is not a report to law enforcement authorities in the sense of a victim trying to spark criminal investigations, but a notification of 'unusual transactions'. It could, however, lead to a criminal justice procedure or investigations by the relevant regulatory agency in their own right.

investigators to inform authorities about irregular transactions and prohibits them to notify the client about this. Failure to comply is an (economic) offence, punishable by criminal law. In this way, internal investigations may prove a liability for clients.

> But – we still have obligations, for example in connection to the reporting of unusual transactions. The client knows this because he is made aware of it in the confirmation document for the assignment. We will not communicate to him that we make a Wwft notification, but we will notify authorities when required. This may be a risk in an investigation. Clients might think that if they hire a forensic accountant, he has to notify. So sometimes we recommend to the client to make the assignment run through a law firm, to protect the client's interests. [Respondent 40 – corporate investigator]

Some concern has been voiced about the use of (derived) legal privilege by lawyers to circumvent the applicability of the WBP and Wwft. However, the current interpretation of this question is that both laws are applicable in general but legal privilege may protect investigations from scrutiny based on these laws (Minister of security and justice, 2015).

This section has set the stage with regard to general legal frameworks, applicable to all corporate investigators. In addition to these, other (general) laws and regulations may apply, depending on the context within which the investigations take place. For example, if the investigations are within a financial institution such as a bank, financial regulation applies as well. Taking into consideration that corporate investigations take place within all sectors of economic activity (but also within the sphere of public administration), it would be impossible to map all these different legal contexts here. However, it is wise to keep in mind that in addition to what is discussed in this chapter, further regulations may apply in different contexts.

The rules and regulations discussed in the sections below are specific to the type of investigator. However, on a more 'normative level', there are commonalities between the four groups discussed. All corporate investigators interviewed for this research mention the importance of certain principles of law to guide them in their investigations. For some, these principles have been codified in a code of conduct, while for others they may just be an 'internal compass'. Leading principles of law which are often mentioned are fairness (treating the subject with respect and keeping his interests in mind)[18], proportionality (the method used should be proportional to the goal) and subsidiarity (when a less intrusive method is available, this should be used). Another widely-used principle is that investigations should have a reasonable

18 The adversarial principle plays an important role here – the right of a subject to be heard and informed.

foundation: investigators should refrain from accepting an assignment without merit, for example when an employer merely wants to get rid of a difficult employee.

2. Private investigation firms – those with a Wpbr-permit

> The Wpbr is the only Act of Parliament that is specific to us. And then there is the code of conduct, made generally binding by the minister [of security and justice] and approved by the Data Protection Authority. That's about the investigative activities. But that's all there is really. Ok we're not allowed to commit crimes or to act wrongfully; that would make us liable. And general principles of law are important but they are in the code of conduct. And we try to keep up with case law and adapt our own code of conduct if necessary. [Respondent 1 – corporate investigator]

For a long time, private investigators have been regulated as a 'by product', falling under the law prohibiting militia until 1999 (*Wet op de Weerkorpsen*). The law against (politically oriented) militia was created in 1936 (Fijnaut, 2002). Although the law was created to prohibit the formation of militia belonging to the NSB, a Nazi-oriented political party, the definitions used were broad enough to also include private security companies. The minister of justice issued a decree in 1939 to exempt private security companies from the interdiction, simultaneously creating some rules for private security companies to comply with.[19] Interestingly, in the *Wet op de Weerkorpsen* there is no mention of private *investigation* companies, the focus is on private security as such. Because of the growth of the private security sector after the Second World War, it was deemed desirable to regulate private security in a separate law. A working group (1974) and later an advisory committee (1979) were formed, both indicating that a separate law was necessary. However, because of the urgency of the matter, as a transitional stage, the *Wet op de Weerkorpsen* was amended (and renamed to explicitly include private security *and* private investigations) to provide a better fit with the private security industry (*Wet op de Weerkorpsen en Particuliere beveiligingsorganisaties en recherchebureaus*) (ibid.).[20] This was the first (explicit) mention of private investigations in Dutch law.

In 1999, a specific law regulating private security organisations and private investigation firms was implemented (*Wet Particuliere Beveiligingsorganisaties en Recherchebureaus* – hereafter: Wpbr). The Wpbr does not provide much guidance for corporate investigators.

19 See *Staatscourant, 6 juli 2000*.

20 There have been multiple other intermediary changes in the law but these are not relevant at this point (Fijnaut, 2002).

The law is fairly general and mostly focused on regulating permits, rather than regulating the actual activities of investigators. It does, however, provide some definitions of what a private investigation firm is. Firstly, article 1, under 1 (e) of the Wpbr defines investigative activities as: 'the collection and analysis of data'. This is a pretty broad definition. The law continues to define a private investigation firm as:

> A person or legal entity, who, in the performance of a profession or [as a] company for profit, does investigative work in as far as these activities are carried out at the request of a third party in connection with a private interest of that third party and in as far as they relate to one or more specific individuals (article 1 under 1 (f) Wpbr).

This definition has some consequences. First of all, as the law is applicable to private investigation firms, others who are not included by this definition are not subject to the Wpbr. This means that in-house security departments are excluded from the legal framework provided by in the Wpbr. In-house departments do not perform services *for a third party* as they are part of their 'client' (State secretary of justice & minister of the interior, 2009). Additionally, most forensic accountants are exempt from the Wpbr because they are investigating as part of their legally defined task (article 1 under 3 Wpbr). Forensic accountants who are chartered accountants are by that definition no private investigators in the sense of the Wpbr.

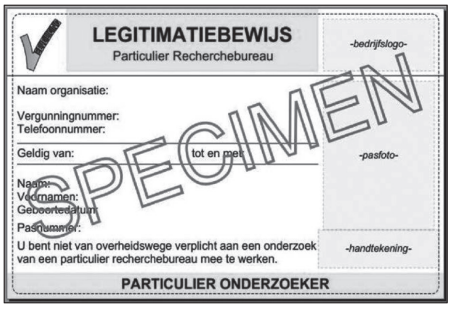
The Wpbr is fairly broad scope, however there are more specific rules laid down in the ministerial ordinance on private security organisations and investigation firms (*Regeling Particuliere beveiligingsorganisaties en Recherchebureaus* – hereafter Rpbr). This ordinance regulates some practical matters, such as permits and education. It is illegal to maintain a private investigation firm without a permit (article 2 under 1 Wpbr), which is criminalised as an economic crime in the Law on Economic Crimes (article 1 under 4 Wed). Those who fall under the Wpbr and Rpbr need to have a permit from the Ministry of Security and Justice (for the organisation: article 2 Wpbr; for management: article 7 under 1 Wpbr) or the chief of police (for employees/individual investigators: article 7 under 2 Wpbr). Permits are granted to people who are 'competent and reliable' (article 7 under 4 Wpbr). As proof of competence, private investigators should possess a certificate of an accredited course on private investigations.[21] Reliability means that a permit will be refused when someone has either been convicted for a crime resulting in a fine, a penal order or a transaction within the last four years; when (s)he has been sentenced to imprisonment or community

21 This requirement does not apply to people born prior to April 1944 and working as a private investigator prior to the Wpbr came into force (article 26 Rpbr). With this, the legislator seems to accommodate the former police officers who have been working as private investigators for a long time. The Wpbr was late to occur and before it came into force, there already was a substantial private investigations sector in the Netherlands.

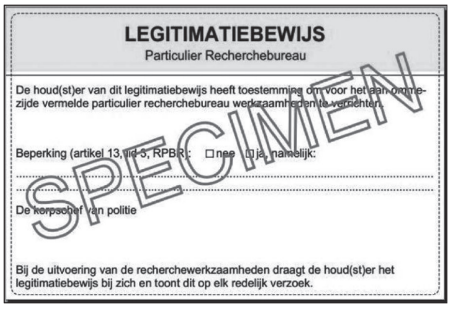
service within the last eight years; or in case of 'other known and relevant facts'. These other facts may for example be grave suspicions of (involvement in) crimes or known criminal associates.[22]

Figure 2 displays the official identification card for private investigators in the Netherlands (also known as the 'yellow pass'). It contains a photograph and some personal details (name, date of birth and registration number) of the investigator and of the company the investigator belongs to (name, registration number and phone number). A card is valid for a maximum of five years and the expiration date is displayed. Interestingly, the front of the ID card states that 'you [the person to whom the card is shown] are not obliged by the government to cooperate with an investigation of a private investigation firm'. As we shall see in chapter 3, this 'voluntary' cooperation with investigations is very important for corporate investigators. The back of the card portrays the signature of the chief of police, the statement that the card holder is allowed to execute investigative activities and – if applicable – some restrictions.

Figure 2. Private investigator identification card



Front identification card private investigators



Back identification card private investigators

The Wpbr states that employees of private investigation firms have an obligation to be discrete about the information they gather during their work, unless they are legally required to divulge the information (article 13 Wpbr). It should be noted that the circumstance that a criminal act is discovered *may* mean that confidentiality does not apply. However, there is no such thing as a duty to report for private investigators. Whether or not a crime is reported to the authorities is up to the client (and partly the investigators) (more on this in chapter 4). The Rpbr furthermore dictates that investigation companies make sure that personal and other confidential data are stored securely (article 4 Rpbr). The aforementioned WBP handles these matters in more detail.

22 See *Staatscourant, 1 april 2014, nr. 9654*.

The actual regulation of specifics of investigative work was left to the industry itself. It is, however mandatory for private investigation firms to have a complaints procedure (article 18 Rpbr). The specific rules that apply to investigative activities of private investigation firms have been articulated by a representative organisation of the Dutch security sector (NVb). This code of conduct is not merely binding to members of the NVb, because of article 23a of the Rpbr it applies to all private investigation firms. This code of conduct has been approved by the Data Protection Authority and is added to the Rpbr as attachment.[23] All private investigation firms are obliged to have a code of conduct in place that is in accordance with the Privacy code of conduct as approved by the AP.

In 2015 there were some 300 licensed investigation firms in the Netherlands that had about 700 licensed investigators working for them (Inspectie Veiligheid en Justitie, 2015). The corporate security market is however much bigger than merely those who are licensed under the Wpbr. Below, we will first focus on in-house security departments, after which our attention will turn to forensic accountants and investigators with a legal background.

3. In-house security departments

> I take it you know the Wpbr, that law puts certain demands to investigation firms. Well, we are an investigation firm, it's just that we investigate internally and not for externals, for others. It has pros and cons. The biggest pro is that we are not required to have a permit. [Respondent 39 – corporate investigator]

As mentioned above, Dutch law does not regard in-house security departments as private investigation firms and as such they are excluded from the Wpbr and Rpbr. The question of whether or not in-house departments should fall within the reach of the law has been discussed in Parliament. The idea behind the exclusion is that because a security department is part of a larger organisation, there will be internal checks and balances in place that should suffice. Making the Wpbr and other legal frameworks applicable to in-house departments would 'lead to a substantial administrative burden for these organisations. This, when compared to the way the public (privacy) interest is protected, leads to the conclusion that extension of the reach of the law is not within reason' (State secretary of justice & minister of the interior, 2009). However, there are still many voices that suggest that the law should apply to in-house departments as well, by making the *nature of the activities* the criterion

23 The Privacy code of conduct has been updated in 2015 and was again approved by the Data Protection Authority.

for applicability of the law (see for example Klerks & Eysink Smeets, 2005). Although many respondents from in-house departments appreciate that they do not have to comply with (the mostly) administrative demands of the Wpbr, at the same time, they feel it is based on an arbitrary distinction. As the above quote shows, many in-house investigators see themselves as being an investigator in the sense of the Wpbr because their work is largely similar to that of private investigation firms. In practice, many in-house departments follow the Wpbr regardless of their exclusion from it.

Because of their exclusion from the Wpbr and Rpbr, in-house departments aren't legally bound by the Privacy code of conduct as defined by the representative organisation of private security either. However, many in-house departments seem to follow the Privacy code of conduct by defining their own guidelines for their investigations, based on this code of conduct.

> What we did is, we made a privacy code of conduct for our investigations, which is more or less the same as the one that investigation firms use. Because we don't want to act differently from them. So we work within the same limitations. We have published these documents on the intranet, so everybody in the company knows what the rules are we play by. Also to make sure that no deviations occur and you don't get in trouble in court. We can show that we work the way the market works, just like the rest. So the official one may not apply to us but we made our own anyway and we agreed that this is the way we do our job. [Respondent 19 – corporate investigator]

All respondents working at an in-house security department indicate that they have their own internal regulations, mostly very similar to the Privacy code of conduct for private investigation firms, comparable to the statement of the respondent quoted above. Similarly, article 18 of the Rpbr is followed as all respondents from an in-house department indicate they have a complaints procedure regarding their activities. In addition, many in-house investigators have completed training in one form or another with regard to their investigative activities (even though they are not required to do so by law). However, a police background may prove to be sufficient for organisations with regard to relevant training and experience.

> Of course you also receive some education internally for specifics related to the job. But the basic skills, knowledge of criminal law, that's important. If they want to report in the end you need to know what kind of information the police need to prove theft etc. What I see in our line of business is that most investigators working for organisations, security managers, they have followed some course on this. And there are registers for security experts, with the right credentials. [Respondent 15 – corporate investigator]

In addition to internal regulations and more generally applicable legislation such as WBP and the Criminal Code, the laws regulating specific branches of industry mentioned above are especially relevant for in-house investigators. Banks for example have to adhere to the Law on Financial Institutions (Wft), telecommunications companies to the Telecommunications law, and so on. It goes too far to discuss all these specific regulations here but it should be noted that this does affect the day-to-day business of the company and as such, of the in-house security department to a greater extent than it does for other investigators. In-house investigators work for one client – the organisation they are a part of. The legal context of this organisation thus constitutes the background for all their investigations.

4. Forensic accountants

> *We have always advocated the opinion that the rules for accountants are more strict than those for private investigators. Some of our colleagues have filed for a permit just in case, but we think: look, the rules we use are more stringent than the Wpbr so it is nonsense to get a permit. So we won't. And the minister has agreed with that standpoint. [Respondent 27 – corporate investigator]*

Many accountancy firms now have their own specialised forensic departments, those of the 'Big Four' (Deloitte, Ernst & Young, KPMG, PwC) being the most well-known. The first to establish a forensic department in the Netherlands was KPMG in 1993 (Van Almelo & Schimmel, 2014). Although the 'forensic accountant' has positioned himself as a leading actor in the field of private (financial) investigations, the Dutch legislator does not differentiate between forensic accountants and normal accountants (De Graaff, 2007). There is no legal definition of forensic accountancy and there are no specific laws for the forensic branch.[24] There are, however, more general laws that also apply to the forensic accountant (as he still is an accountant), most notably the law regulating the profession of accountant (*Wet op het accountantsberoep*; hereafter Wab) and the law regulating the control over accountants (*Wet toezicht accountantsorganisaties*; hereafter Wta). In the Netherlands, there are two kinds of accountants: the chartered accountant (RA) and the accountant-administration consultant (AA). The RA and AA are different only with regard to their types of clients and their educational background, with the RA being educated on university level and the AA on college level. While the RA caters mostly to large and multinational companies and 'organisations with

24 Neither is there a specific education, leading to a title 'forensic accountant'. There are, however, some courses within other academic studies, such as criminology (Leiden University) and the Big Four have their own internal courses.

a public interest element', the AA finds his clientele in small to medium businesses. They have the same tasks and responsibilities and both are mandatory members of the association of accountants (NBA).[25] The different laws regarding the RA and AA have been combined in 2012 in one law (the Wab).[26]

To be allowed to use an accountancy title, it is obligatory to be listed in the register (article 41 Wab). Those who are legally allowed to call themselves accountant are subject to disciplinary proceedings (article 42 Wab). Since 2012, when the Wab came into force, the disciplinary proceedings are dealt with by the Accountancy chamber of the court in Zwolle, which consists of a mixture of judges and accountants. The appeals are dealt with by the Court for trade and industry. The five disciplinary measures which may be administered are a warning, a reprimand, a fine, a temporary removal from the register and a permanent removal from the register (article 2 *Wet tuchtrechtspraak accountants*; hereafter Wtra).

Some respondents indicate they have been removed from the register at their own request. One reason mentioned for this is that the mandatory 'permanent education' hours (NBA, 2016) are superfluous and expensive for accountants who are not active as a traditional accountant. For accountants working as corporate investigators, being registered doesn't have much added value. Without registration, they are not allowed to use the title RA or AA, however, they do not need this title when working for a private investigation firm (or in-house security department). "I have requested to be removed from the register but I am still perfectly able to look at the books and when they want me to report what's in the administration and how much money went to account A, B or C, I can do that" [Respondent 13 – corporate investigator]. No longer an accountant in the official sense, these investigators are no longer subject to the rule of the disciplinary court. This is mentioned as another reason for removing oneself from the register (Van Almelo & Schimmel, 2014). That would, of course, be a perverse effect of the regulations, however it does not necessarily mean that the investigator in question is now 'unregulated'. Depending on the position of this investigator, he or she then falls within the regime of the Wpbr (when working for an investigation firm) or the internal regulations of the company (when part of an in-house security department).

Because of the lack of a *specific* legal framework, respondents feel that the rules regulating accountancy do not align well with the activities of the forensic accountant. There are some guidelines designed by the NBA, however they should not be regarded as having a binding nature (NIVRA/NOvAA, 2010). The Accountancy chamber does take these guidelines as a point of reference in disciplinary proceedings

25 Before, there were two organisations, the NIVRA (for RA's) and the NOvAA (for AA's).

26 For an overview of legal developments around accountancy in the Netherlands until 2007, see De Graaff (2007).

though, and deviation from the guidelines requires explanation (see for example ECLI:NL:TACAKN:2016:49). Within the profession, there have been voices claiming that the forensic activities of a forensic accountant do not align with his legally determined duties and the investigations should be left to private investigators (Van Almelo, 2007).

The circumstance that the law does not provide specific rules for the forensic activities of accountants makes the aforementioned view of the state secretary of security and justice – that the Wpbr does not apply to forensic accountants because they are investigating as part of their legally defined task – a bit problematic in my view. Seeing that neither the law nor the disciplinary proceedings are specifically created for the forensic activities of accountants, it is not surprising that there is some debate among accountants (and other corporate investigators) about the applicable rules. For example, some forensic accountants have a Wpbr-permit, while others do not. There is a difference of opinion within the accountancy sector whether or not a permit is necessary and whether or not a forensic accountant should follow the rules laid down in the Wpbr. The corporate investigator quoted below is a forensic accountant himself.

> It is odd though – some minister has said that [the Wpbr is not binding to accountants] as a reaction to questions from Parliament, based on the lobby of the big accountancy firms. But it's strange if you think about it – those accountancy firms who are doing person-oriented investigations should fall under the Wpbr. [Respondent 40 – corporate investigator]

It may be argued that the rules binding forensic accountants are more based on principles of law than on actual hard and fast laws (Van Wijk et al., 2002). These principles of law have been codified in the rules of professional conduct for accountants, as issued by the NBA (NBA, 2014). As 'fundamental principles' have been noted: competence and diligence, integrity, objectivity, professional conduct and discretion.[27] Other important principles of law identified by the NBA are proportionality and subsidiarity, the adversarial principle, the principle of fair play, the principle that results need to be verified, the principle that the accountant should refrain from giving a judgment and that he should be independent and impartial.[28] Although these general principles of law may be of guidance in many situations,

27 Interestingly, the law indicates that accountants are bound to discretion about the information they gather during their legally mandated control tasks, unless they come across a fraud of material importance to the financial accountability of the client. In such a case, he should report this to law enforcement (article 26 Wta). 'Fraud of material importance' is fraud of such a nature or size that it may for example influence investment decisions of others. However, when the client acts directly upon this information by ordering an internal investigation and making a plan about the steps to be taken, this obligation to report does not apply (article 37 Bta [*Besluit toezicht accountantsorganisaties*]).

28 Chapter 3 will discuss this more in-depth.

they may not be of much help in some circumstances more specific to investigative activities (Van Wijk et al., 2002). Van Wijk et al. conclude that forensic accountants do not always have enough rules to guide them and that they should be subject to the Wpbr (which was under construction at the time of their research). This suggestion was not implemented by legislators though and as shown above, the recent change in accountancy legislation and regulations has not brought specific (written) rules for forensic accountants either. The fact that accountancy regulation does not include rules for forensic work results from the fact that 'these situations [in which there are no adequate rules] are connected to the detective part of the job, not to the use of accounting methods' (Van Wijk et al., 2002: 229).

Taking into account that forensic accountants seem to view themselves (and be viewed by others) *and the regulations they have to comply with* as top of the crop, this lacuna in the legal framework could be considered remarkable. The code of conduct for person-oriented investigations (which does not possess the legal status of professional regulation), expressly refers to the Privacy code of conduct for private investigators who are licensed under de Wpbr, to be used as a guideline (NIVRA/NOvAA, 2010) and forensic accountant respondents indicate that they indeed use the Privacy code of conduct in their investigations. As the Wpbr is not legally binding to accountants, this should be regarded as a suggestion rather than a strict rule.

> It's rather odd that for example the forensic departments of the Big Four don't have to have a permit, while we do. I think that's quite extraordinary. Because, just because they are part of an accountancy firm, they don't have to meet that requirement. We, as private investigators, have to pass an exam, not that that's very difficult but at least it is some kind of check. And they don't have to do that. It's as if when you're part of an accountancy firm they think that you know everything. [Respondent 5 – corporate investigator (forensic accountant working for an investigation firm)]

However, among respondents, the view is prevalent that the code of conduct that has been made by the NBA is the most stringent of all regulations regarding private investigations. While the nature of accountancy regulations may be argued to be 'morally strict' as a result of the emphasis on (legal) principles, the codification of these principles of law into legally binding laws is largely absent. As many commentators have stated, there is still no clear-cut framework for forensic accountants to work in (e.g. Van Campen & Van Hulten, 2015). The Privacy code of conduct for private investigation firms has integrated many principles identified by the NBA within its guidelines, and, as mentioned above, the NBA itself encourages its members to follow the Privacy code of conduct. However, there are some disagreements about the practical use of some of the principles of law which are incorporated in the

Privacy code of conduct and the NBA-guidelines. For example, many accountants argue that a forensic accountant should refrain from making a judgment. As the NBA code of conduct states, an accountant should limit himself to 'reporting the facts and the circumstances and regulations that are relevant to these facts' (NIVRA/NOvAA, 2010: 15).

> We are contracted-in to do fact finding, assigning value or giving meaning is not an accountant's job. At the most you may describe the rules and describe the act. These are then laid side by side but a report should not state that the act has therefore been improper. [Respondent 36 – corporate investigator]

It seems though, that it is not the mere fact that a conclusion is drawn from the findings but rather the way in which this is done that is problematic. Accountants should refrain from giving a legal interpretation and from using normative language (such as 'right' or 'wrong') but it seems nearly impossible to avoid drawing any type of conclusion whatsoever (Van Almelo & Schimmel, 2014: 50). A recent decision by the Court for trade and industry seems to suggest that the crucial point here is not the interpretation of facts as such, but rather the way these conclusions are supported by the report (ECLI:NL:CBB:2016:118). This resonates well with the requirement from the accountancy code of conduct, that all conclusions made by an accountant should have a sound basis. "According to accountancy rules we should have a reasonable foundation for our findings. Which means that if you say, 'this is red', you should have the facts to substantiate that conclusion" [Respondent 41 – corporate investigator].

The accountancy profession has suffered considerable reputational damage since the start of the economic crisis of 2008. The role of the accountant in the years leading up to the crisis, and the (often sideways) share accountants have had in scandals, have led to substantial criticism. These criticisms focus primarily on the control task of accountants. In 2014 (and the years before that), the Authority for the Financial Markets (AFM) published a report in which it concluded that there were structural deficiencies in the major audit firms (the Big Four) and that fundamental reforms of the sector were necessary (AFM, 2014). Since then, the NBA has made several attempts to reform the sector and improve its reputation (*Werkgroep toekomst accountantsberoep*, 2014).[29] One of the ways this is to be done is the oath accountants are required to take as of June 2016 (from May 2017 onwards, every accountant should have taken the oath) (*Verordening op de beroepseed voor accountants*).

29 The AFM fined all Big Four firms in March 2016 for failure to comply with their legal duty of care (AFM, 2016). However, these fines are based on the infractions found in the 2014 report. Recent AFM publications indicate that the sector is making serious improvements (AFM, 2015).

5. Investigators with a legal background – forensic legal investigators

> In those cases in which we are hired as an independent advisor there are no fast and hard rules, you have to formulate that together with the client. But I don't think that this is causing many issues. I believe that you need to make rules when they're needed, not before. And I'm not using any investigative powers, I ask people would you come over to answer some questions, you may bring a lawyer, you don't have to, that's it. It's a developing profession, seven years ago it didn't even exist and now there are many large firms who are getting into the market. So there is probably going to be some kind of regulation in future, to set standards for our investigations. [Respondent 30 – forensic legal investigator/client]

The most recent player added to the field of corporate investigations is the lawyer (Jennen & Biemond, 2009). Lawyers have long been involved in corporate investigations, however, before they were mostly clients. As clients, lawyers are often also partly involved in the investigations, for example because there are some (simple) actions they may do themselves, or they may be involved in the role of expert on the legal aspects of the investigations (e.g. whether or not the behaviour might (or should) be framed as criminal or as a private law matter) (Van Almelo & Schimmel, 2014). At the conclusion of the investigations, when decisions are to be made about the steps that are to be taken, (labour) lawyers are often involved in the processes of advising and decision-making. More and more (large) legal practices have now developed their own investigative branch and smaller legal firms have also emerged that specialise in private investigations.

Much like the legal framework in place for accountants, there are no rules for lawyers that specifically focus on investigations. There are, however, more general laws regulating 'traditional' activities of lawyers, the *Advocatenwet* [the law on the legal profession] being the most important. Lawyers need to be registered to be able to act as a lawyer (article 1 *Advocatenwet*) and only those who are registered may call themselves lawyer (article 9a *Advocatenwet*). Like accountants, lawyers have a system of permanent education, with which they must comply (article 4.4 *Verordening op de advocatuur*).[30] The basic education is university (or college) level. An oath is required for lawyers (article 3 *Advocatenwet*). All lawyers are required to be a member of the Dutch order of lawyers (*Nederlandse orde van advocaten;* NOvA).

30 There is no official education for investigative lawyers. However, there are some new initiatives targeting accountants and lawyers. These (academic) courses may be used for the permanent education points-system. For example the course 'financial forensic expert' of the Erasmus University Rotterdam aims at both accountants and lawyers.

This is a public body and its ordinances are legally binding (article 29 *Advocatenwet*). Disciplinary proceedings are held by Councils of discipline (presided over by a judge with two (or four) lawyer members and assisted by a clerk) in the district in which the lawyer operates and appeals may be made to the Court of discipline (presided over by a judge with one (or two) (judge) members and one (or two) lawyer members and assisted by a clerk). Disciplinary measures that may be taken are a warning, a reprimand, a fine, a one year suspension and a removal from the Bar register (article 48 *Advocatenwet*). It is also possible to take no disciplinary action.

The law dictates that a lawyer is responsible for the protection of his client. He does this in a way that is independent (from e.g. government), yet partial to his client and he should be competent, act with integrity and be a confidant to his client (article 10a *Advocatenwet*). In this sense, there is a difference between the other types of investigators, as this partiality is only for lawyers explicitly regulated by law. As the law is designed to regulate more traditional types of legal assistance and not investigations, this is not surprising. In the moderately inquisitorial judicial system of the Netherlands, lawyers have an important obligation to protect the interests of the suspect, who is more the object of investigations than an equal party to the proceedings (Cleiren, 2001).

The code of conduct, issued by the Dutch society for lawyers (NOvA) is an elaboration of the general principles as laid down in the *Advocatenwet* but remains focused on the lawyer's 'core business' (NOvA, 1992). The code of conduct is not legally binding, rather it is meant as a guideline for practitioners and disciplinary proceedings. Some specific parts of the guidelines can be used by lawyers when doing investigative work as well. Rule 29 of the code of conduct for example, states that the role of the lawyer should be clear in all communications with third parties. In disciplinary proceedings, this rule has been used to claim that the roles of the (fundamentally partisan) lawyer and the (independent and objective) fact finder should not be blurred (ECLI:NL:TADRSHE:2012:YA2502). In the ruling referred to here, the court decided that the complaint that was launched had no merit, arguing that a lawyer always is a partial service provider because of his profession, even in the capacity of investigator (which ruling has been confirmed by the court of appeal) (ECLI:NL:TAHVD:2013:33). In the same way, rule 30 of the code of conduct may also apply to corporate investigations. This rule states that a lawyer should refrain from providing false information. This could apply to for example an interview situation, in which it would be considered wrong to provide the person who is interviewed with false information. Similarly, rule 36 may apply as it states that a lawyer is not allowed to make a recording of a conversation without the prior consent of the person. Still, there is no specific legal framework available for investigative activities by lawyers, either by law or in the form of self-regulation.

Lawyers have a special position in the Dutch legal system, insofar as they not only have an obligation to discretion (article 11a *Advocatenwet*) but they also have legal privilege (*inter alia* article 218 WvSv[31]). This means that – with few exceptions – they are not obliged to give authorities information about clients. There is some debate among investigators (and clients) whether the use of this legal privilege in investigations is an asset or should be considered as stretching the law. One of the risks of private investigations is that the report may be subpoenaed by investigative agencies and notwithstanding their obligation to discretion, investigators must comply with this, unless they have legal privilege. If the use of legal privilege is deemed necessary in investigations a lawyer will be involved, either as the investigator, or as the client to other investigators.

> In case study 1, Observation Company 1 was hired by a legal firm to do the investigations. This course of action was chosen over a direct relationship with the organisation in which the norm violation had taken place for several reasons, but the most important one was the derived legal privilege that may protect the outcomes of the investigations. All reports and communications with the law firm are protected by a derived legal privilege. This means that the reports do not need to become public. Since a public organisation was involved in this case, and legislation provides any citizen with the right to ask for inspection of documents of public authorities (*Wet Openbaarheid Bestuur*), without the protection of legal privilege, privacy sensitive information might have become public before the investigations were concluded. [Case study 1]

Many investigators and clients feel that the use of (derived) legal privilege is a safe way to proceed. However, others see some downsides to the use of legal privilege in corporate investigations.

> We as forensic accountants have no legal privilege but lawyers do. If we're involved by a lawyer we get derived legal privilege. But the thing is, if you do your internal investigations under the protection of legal privilege, a prosecutor or a supervisory authority will not accept the outcomes of the investigations. Because lawyers are really careful about what is written down in the end and everything that may harm a client will be left out. But if you don't use legal privilege they might use your report and might not investigate fully themselves as well. You can use legal privilege, that's the choice an organisation will have to make. But just know that your report will be judged differently if you choose to report to the authorities in the end. [Respondent 27 – corporate investigator]

31 Code of Criminal Procedure.

When the lawyer acts as a client, the investigators who are hired may appeal to a 'derived' or 'secondary' legal privilege.

> It is not inconceivable that we act as legal representative to defend the position of our client in a legal procedure – well in such a case it is perfectly legitimate to do this in your capacity as legal privilege holder. And all the auxiliaries you use – whether that is your secretary or a translator, another expert or accountant – all act under the banner of your privilege. [Respondent 28 – forensic legal investigator/client]

There is some debate about whether or not this derived privilege is something that will hold up in court. In a 2015 ruling, the Dutch Supreme court has decided that investigators who have derived legal privilege are not exempt from complying with a subpoena; they should provide the documents to the examining magistrate, who then decides whether or not the documents are protected by (derived) legal privilege (ECLI:NL:HR:2015:3714). As such, it is not entirely clear whether or not derived privilege protects an investigation, even when the investigations are done under auspices of a lawyer. There is, however, consensus that when derived privilege is used, the lawyer should actually be involved in some way and not merely be recruited when a precarious situation arises, in order to use legal privilege (Keupink & Tillema, 2013). The minister of security and justice has expressed the same opinion in response to questions from Parliament (Minister of security and justice, 2013).

> What you should not allow to happen is misuse of your privilege. Say, for example, that a forensic accountant is investigating and that he finds something which he thinks is disagreeably sensitive. Without legal privilege, such a report is very convenient for the prosecution office, prosecutors could say 'great we don't have to investigate it further, thank you very much'. That's the danger. Doing internal investigations without someone who has legal privilege to protect it, well, all the prosecution office has to do is ask for the report. But as a lawyer you shouldn't allow your privilege to get abused. A lawyer shouldn't just do some trivial things for show so that legal privilege will be applicable. No, that can't be. [Respondent 28 – forensic legal investigator/client]

In a ruling in a civil court case between the housing association Vestia and its managers, the court of The Hague has decided that the report following internal investigations by a law firm is not protected by legal privilege if the investigations are purely intended as fact finding (no juridical findings, qualifications or conclusion being presented). The court sentence states that 'according to its assignment the investigation's purpose was to acquire an independent and objective image of the facts. (...) This makes the claim that the report falls within the (functional) legal

privilege of the (lawyers of) De Brauw void' (ECLI:NL:RBDHA:2015:248). For legal privilege to be applicable, it should be relevant for the (traditional) position of the lawyer as partisan representation of the client in legal proceedings.

Many voices have suggested that the lack of regulation applicable to lawyers who operate as corporate investigators is problematic. As it is popular opinion that the code of conduct for lawyers needs to be updated, it has been suggested that the new version should include specific rules on investigative activities and the use of legal privilege (see e.g. Mr. Online, 2016). Others feel that the corrective effects of 'the market' and the judicial system ensure the quality of investigations (see e.g. Van Almelo, 2013). This argument, however, could also be applied to the other investigators (with the possible exception of in-house investigators) who *are* regulated. In addition, as we will see in chapter 4, many corporate investigations never end up in court. It would therefore be very difficult for the judicial system to correct misbehaviour by investigators in these cases.

Now the legal frameworks regulating the activities of the different investigators have been discussed, the next section focuses on the way the differences between investigators are exploited by the different groups – and valued by their clients.

6. The selling propositions of the different types of investigators

Although the backgrounds of and rules for investigators differ, their actions are for a large part similar. The question then remains, what are the selling points of the different investigators – in other words why do clients choose them over others? This section discusses the different strengths and weaknesses of the four groups discussed above, based on the research data.

6.1 Background and specialist knowledge

All professional investigators feel they have an advantage over other types of investigators – and they do. The strength of one type of investigator is the weakness of the other – which is something that each type of investigator exploits as part of its own niche within the niche. When it comes to in-house departments, the great advantage for the 'client' organisation is their familiarity with the organisation in which the investigations take place. Although all types of corporate investigators have more access and find their way within organisations more easily than law enforcement investigators, it is inevitable that external investigators have less

knowledge with regard to the particular organisation than those who belong to it. In-house investigators are the specialists with regard to that particular organisation, they know how the processes work and have multiple contacts within the organisation. This makes for easy access.

> One of the reasons why we are so good at this, is that we understand the company better than an investigation firm would. Look, if you want to find deviations, you're going to have to know normalcy first. And once you understand the normal process, then you may start to see deviations. We know this company, we know our way around and we understand its culture. [Respondent 39 – corporate investigator]

Not only do in-house investigators know the organisation subject to the investigations well, they also know the organisation's (commercial) background. Details of investigations may differ between a bank, a telecommunications company or an industrial plant. External investigators usually have so many different clients, with different commercial backgrounds, that it would be impossible for them to know all of these in-depth. Often, people working in in-house departments have been formerly employed by law enforcement agencies (however, some are 'regular' employees of the organisation who have been placed with the security department because of personal interests etc.). This means that they usually have experience with police-like investigations and investigative methods such as interviewing, but much less so when it comes to administrative investigations, IT-investigations (although usually the IT-department of the organisation can help out with this) or the legal implications of the investigations (for which the HR and/or legal department may step in).

> Observation Company 2 is the security department of a large Dutch company. The security department doing the investigations consists of eleven people who had some role in the investigations, with three full-time investigators and three desk researchers. Throughout the larger organisation there are also security officers located, one for every specific field in which the company is active. These security officers may assist in investigations when their segment is involved. In addition, specific IT questions (for example, when electronic data is needed) are asked from the IT department, which will then provide support. Compliance matters are left to the compliance department and Legal and HR may assist as well. In this way, the security department is the specialist on the investigations and has easy access to additional expertise from inside the company. As the manager said: 'You see what kind of specialist knowledge is necessary, my guys have this knowledge about the specific electronics we as a company use and all of that. It's useless to get someone from the outside to look into it, it's impossible for him to understand all our systems and have the specialist

> knowledge necessary to investigate these matters. [If you don't understand the way this company operates and the systems and tools needed for that you will draw the wrong conclusion]' [Excerpt from observation 2]

Because of their background in law enforcement most in-house investigators have experience with making a report to law enforcement authorities, which they often handle when the company decides on this course of action. Their law enforcement background is very helpful as it enhances the chance that a reported norm violation will be investigated by the authorities.

> If I report to the authorities and I have made my own case [the private investigative report], my chances of the report being taken up are much larger because it saves them some trouble but also because they know that it's something serious. My advantage is that I know what they need. It's just faster that way. A normal citizen who doesn't have much experience with reporting to the police will find it difficult to find his way into the organisation. [Respondent 15 – corporate investigator]

This advantage of having many people with a police background is not unique to in-house departments. Just like in-house departments, private investigation firms often also have many former police officers (or prosecutors) working for them. All the advantages of having experienced interviewers who are accustomed to the process of investigations are therefore present within private investigation firms. This police-like image may be useful and it is often advertised as an asset on the websites of commercial investigation firms but it may also work against a firm. Competitors with an accounting or legal background tend to depreciate the police background of many investigation firms, claiming they are under-qualified 'rent-a-cops'.

> The camera aimed at the cashier, doing a little stake-out and taking some pictures… They [private investigation firms] are not equipped to do quality work when it comes to fraud of course. Fraud, that's being done by people at the top of the tree, it's about a lot of money and they are being advised by expensive lawyers and tax experts from fancy firms. There is a lot of intellect hidden in a fraud. You're not going to solve that with a camera and someone with a police background. [Respondent 32 – forensic legal investigator/client]

Especially forensic accountant-respondents seem to want to distance themselves from the image of being a private detective. An often-heard remark is that private investigation firms, seen as dominated by former police officers, are good for the more straightforward investigations but fall short when it comes to complicated fraud schemes.

> What we often hear is 'oh so you are private detectives'. I wouldn't say is a derogatory term but... it's a different category of work. They are often very perpetrator-oriented. That's not really our focus, who is 'guilty'. It is the conclusion to our investigations but not our main focus. We focus on analysing facts. And usually these facts are complex and require intelligent background research, complex accounting, to get the full picture. [Respondent 40 – corporate investigator]

This view of corporate investigators working for private investigation firms as being incapable of complex investigations into fraud comes in part from the general opinion in the sector that police officers are not skilled enough for this type of work. Former police officers in this view would then also lack the skills and knowledge. Furthermore, the (many) courses given about private investigations (some of which are accredited) are below academic level (Klerks, Van Meurs & Scholtes, 2001). Many respondents feel the educational standards for private investigators are too low. "I would suggest that the educational standards and the representative organisation should focus more on the specialised work. Now my investigators have had to follow a course which is practically useless to them" [Respondent 13 – corporate investigator].

Private investigations do indeed require more than merely a police background and private investigators are 'not just a private form of public police', as many private investigation firms themselves acknowledge. Consequently, private investigation firms tend to also hire forensic accountants, IT-specialists and other useful specialists to fill the gap in experience with administrative or IT-investigations and other specific skills. The combination of these people from different backgrounds makes that investigation firms are often able to cater to many investigative needs of clients.

> You know, an investigation has different dimensions, you have a financial part, a technical part, an operational part. And sometimes you need one investigator because he is better at that particular part than others because of his background and experience. [Respondent 13 – corporate investigator]

As chapter 3 shows, respondents tend to stay clear of 'law enforcement language'. Respondents from investigation firms (just as other respondents) tend to distance themselves from an image of being private police and market their firm as being the best of both worlds: the advantages of private investigations more generally apply (see chapters 1 and 3) but in addition, they have inside knowledge of the workings of the criminal justice process. Private investigation firms tend to be generalists compared to other corporate investigators (or, conversely focus on one specific niche of investigations).

> Observation Company 1 is a small investigation company, known for specialised knowledge on different subjects. As one of the owners stated: 'We're trying to deliver a high quality product'. Because of the law enforcement background of one of the owners and another investigator, the company has a large network in both law enforcement and the commercial sector. Many assignments originate from this network or are based on positive word of mouth among organisations. The private investigation firm prides itself on its reputation of being a high-end and independent investigation firm. [Excerpt from observation 1]

Depending on the client's wishes, private investigation firms may thus give advice about how to settle the matter at hand. This advice may or may not be included in the report (see also chapter 3). When the client wants to report the norm violation to the authorities, private investigation firms often provide help with this process.

> When our assignment comes directly from the organisation, with no lawyers involved, we will also take on an advisory role for the client and we may then also report to the authorities for the client. The question is then, how will you go about this. You could go to the local police station but our experience is that that's a dead end. It might help to go directly to the chief public prosecutor, send him a letter with appendices – meaning our investigative report. [Respondent 2 – corporate investigator]

Not having a police background, forensic accountants conversely, have the reputation of being the experts on investigations into financial administration.[32] They have been academically trained to produce and audit financial administration but the 'forensic' part is more learning on the job. Many forensic accountants who have years of work experience are also skilled interviewers. However, according to many respondents this is not their strong suit. "What we see is that forensic accountants are very good at forensic accounting but that doesn't mean they are good at thinking about systems of fraud or what makes people tick." [Respondent 32 – forensic legal investigator/ client]

> When it comes to interviewing people, you might not want to leave that up the financial investigator who has looked into the administration. It might be best to let someone with a police background do the interview, because he might not have the know-how with regard to the content but he knows how to interview. He can assess how someone behaves, he understands that kind of stuff much better than the competent accountant who knows very well what the administration says but is

32 However, some forensic accountants have worked for either police, prosecution or specialised investigative services such as the FIOD (the investigative service of the Dutch revenue authority) in the past.

> much less equipped to respond to the involved person and read his body language. [Respondent 13 – corporate investigator]

Even though forensic departments of big accountancy firms tend to diversify their services, for example by creating tools for the analysis of big data collections, their expertise lies with the investigation of 'the books'. Just like private investigation firms try to employ 'other experts', forensic accountancy firms or departments also employ former police officers, legal experts and IT-specialists. The service provided does remain centred around forensic accountancy though, and they follow the (rules and) guidelines that apply to accountancy work. One of the implications of this is that forensic accountants tend not to draw conclusions based on their report. It is considered 'not done' for an accountant to assign blame because this is considered a subjective qualification and an accountant needs to remain objective.[33] "We don't even have an advisory role in this. I have my opinions but it's not my decision, the organisation needs to decide for itself whether they [feel this is a crime and] want to report or not" [Respondent 27 – corporate investigator]. This is considered a drawback by clients, who often want to hear the professional opinion of the accountant about how to qualify the incident. "And after all that [a long and expensive investigation] you get a report filled with facts but just having the facts is of no use of course. Because these facts need a social and legal interpretation. Without a legal reading, facts are useless" [Respondent 32 – forensic legal investigator/client]. When a client does decide to report a norm violation to the authorities, most forensic accountants provide some assistance with this.

> I can give you examples of investigations which have cost a small fortune but looking at it, you think 'What on earth did these guys do?' So you have high rates but also – if you would get a second opinion on what they actually did, it makes no sense from an investigations-perspective. For example the Big Four [accountants], they are reproached now and then for their investigations, that they don't yield much results and basically just map what the client already knows. That it costs a lot of money but actually yields no results. That they for example won't find the money that has been defrauded or get it back. [Respondent 13 – corporate investigator]

The 'weakness' of forensic accountants is, conversely, the strength of investigators with a legal background. It is exactly the ability to provide a client with a legal qualification of the norm violation which gives forensic legal investigators their advantage over other investigators. Some forensic legal investigators provide a full investigative

33 As discussed, there is some discussion about this though, some accountants feel they are allowed to draw conclusions as long as these are based on the factual results of the investigations.

service, others specialise in the validation of investigations done by others. In the latter case, forensic legal investigators mainly look at whether the investigations are 'correct' in procedural terms, but also with reference to the facts that are presented (are the facts, which are necessary to take further steps, clear) and with regard to the legal interpretation of these facts (what does it mean from a legal point of view). Forensic legal investigators have no specific background in either financial administration or police investigations, however many forensic legal investigators have a prosecution background. In this way they are often familiar with the investigation process. The most important forte of forensic legal investigators is their extensive knowledge of the law. They are much better equipped than other investigators to draw conclusions from investigations and give specific advice to the client on how to proceed.

> When it comes to an investigation in need of a decent analysis with regard to the facts and the law, and when there is need for an advice regarding corporate governance – I would use a law firm for that. Other investigators say they can do it but in reality they deliver a poor result. [Respondent 28 – forensic legal investigator/client]

Although not specialised in the investigations *per se*, forensic legal investigators in this sense provide a more encompassing service. Often, other investigators are contracted-in to do specific parts of the investigations resonating with their area of expertise. In this way, a forensic legal investigator may provide its clients with a report spanning both the investigative 'facts' and the legal implications that follow from that. And – when the client has chosen a particular settlement – the involved lawyer, or a specialised colleague from his firm may assist with that too.

> We assist our clients when incidents occur within their organisation, we will investigate for them, we advise them on what kinds of measures are to be taken and in the event that a regulator or the justice department is to be involved, we will advise them about how to deal with these agencies. [Respondent 30 – forensic legal investigator/client]

6.2 Rules and ethics and position regarding the client

As we have seen in this chapter, the different types of investigators have different rules to follow. This has some implications for the choices made by clients. In-house departments, which, it goes without saying, can only be used when an organisation has such a department, are subject to (often quite strict) internal regulations. The fact that the regulation is mainly internal to the organisation (apart from more generally applicable legislation such as the WBP) may not be a 'problem', however it does put much responsibility on the organisation itself. The rules are constructed inside the organisation and the control over the application of these rules is also largely

organised within the organisation (although a civil claim against the organisation remains a possibility). The general control by the Works Council of the organisation (approving the rules) and the specific control of higher management on the actual investigations in case of a complaint, both keep things close to the organisation. This has value for the organisation, as there is less danger of matters becoming public knowledge. However, sometimes an organisation needs an independent outsider to investigate because of the issues at stake. In those cases, internal investigations by the in-house department are not deemed sufficient and another corporate investigator is contracted to either execute or validate the investigations. "Sometimes they have done their own investigations and fraud has been found but they feel they need an independent third party to as it were validate the investigations or come to that conclusion independently" [Respondent 27 – corporate investigator].

While their position within an organisation may suggest that in-house investigators cannot be considered independent, the fieldwork suggests that in-house investigators often clash with 'the organisation'. Comparing my observations within an internal security department to those within a private investigation firm, my conclusion is that there is less of a difference between the two in this regard than I had expected beforehand. The in-house security department seemed to function as quite an independent unit within the organisation, while also being part of it.

> We are independent from others in our investigations. When we have by-catch we will investigate that in principle as well. The by-catch can be pretty big, for example a case that we're still working on was initially by-catch. The organisation was also investigated, apparently it was possible for these things to happen without the processes noticing it. In these cases, we need some extra pairs of hands so we use some external investigators. But there can be tension between us and HR. We have a separation of powers, we are in charge of the investigations, HR decides on the sanctions. When we hear that a sanction is much lower than we would have liked and than what we find reasonable based on previous cases, that can generate friction. Especially [investigator] can go to extremes to make his point, he can be very fierce. In principle, we decide on content and scope of the investigations, there's no influence from others on that. But of course, when it comes to the higher echelons the top has its opinions on it. That's the way it goes isn't it. The higher up the tree, the more interests are involved. [Excerpt from observation 2 – informal conversation]

Because of the different points of reference between managers and investigators – profit versus security/integrity – the in-house department is not always regarded straightforwardly as being a service provider to the rest of the company. In this sense, some disputes might occur within an organisation between management and in-

house investigators. Interviews with in-house investigators and their internal clients seem to support this finding. Although very much aware of company interests, investigators often take a different approach to this than for example 'normal managers' do.

> I'm considered to be the paranoid one, who sees fraud everywhere. We have to convince them all every time around, that's how we all feel. Because it clashes with the business of making money. When we investigate and one of our stores is affected or we lose a business partner, that looks like it costs a lot of money but in the end, you're not making any money on the fraudulent behaviour you know. All of that is fictitious. You actually lose money over it as you are unjustly paying bonuses and commissions. [Respondent 48 – corporate investigator]

In most organisations, in-house security departments report directly to the Board of the company, thus granting them a semi-independent position within the organisation. "We report to the board of managers, there's only my manager in between. That independent position is a crucial principle" [Respondent 39 – corporate investigator]. Because there is no commercially driven connection between the investigators and their clients, in-house investigators often have more freedom in their investigations. There is no formal contract in which an investigative assignment is delimited and respondents suggest that this leaves more room to make independent decisions that lead to the expansion of the investigations. The respondent quoted above goes on to say "it is really nice to be able to work without the costs for your investigation being an issue. I have worked for a commercial investigation firm before and there you have to work on a commercial basis for a third party" [Respondent 48 – corporate investigator]. For a client who pays external investigators by the hour, an expansion of the investigations may mean significantly higher costs. Internal investigators are paid by the organisation anyway so in this sense the scope of the investigations matters less. However, a larger scope of investigations may mean that a particular part of the organisation is being hampered in its day-to-day business and the time an investigator spends on one case will have effect on the time he can spend on another. In addition, big cases may call for more manpower than is available in the in-house department and external investigators may have to be contracted then, as indicated in the excerpt of observation 2 above. These and other consequences make that costs also are a factor for in-house departments.

> You have to weigh everything during your investigations: am I going to continue, do I have all the information I need, is it useful to keep investigating? The question always is, what do you want to achieve and what do you need to achieve it? If you want to fire someone, you don't need to prove he's committed fraud a hundred times, a couple of

> times is enough. It might be relevant with regard to retrieving the money. And for the processes inside the organisation. It is so hard to set limits, but it is important. You have to prioritise, the more time I spend on case X, the longer cases Y, Z and others have to wait. We're only a small department for a lot of cases after all. [Respondent 43 – corporate investigator]

In-house respondents also indicate that they 'sell' their product to management by indicating the cost reduction they may achieve:

> I am going to get more staff next year, we have shown that doing something about fraud can generate money by multiple business cases. If you lose one credit of 500.000 euro, that means you will have to get say 400 new ones to compensate for it. That is a lot of new business you will need if you have 10 of these cases. And the same goes for internal fraud. [Respondent 31 – corporate investigator]

During observation 2, it became clear that contrary to investigations done by other investigators, not every in-house investigation culminates in a report. There is a bulk of (often minor) cases reported to in-house investigators and when it comes to minor or easy cases, sometimes the interview report or investigations log is deemed a sufficient record. In these cases, it is more cost effective not to write a full report (however, there still needs to be some record of the investigations and settlement). A report is necessary when sanctions will be taken bringing the matter outside the company (e.g. dismissal, a civil suit or a report to the authorities).

> In principle we make a report for every investigation. I say *in principle*, because *in fact* this is not necessarily the case. Some cases are slam-dunks, we're not writing an entire report for that. Often things are handled by HR or the manager and that's it then, some milder, internal sanction. Look, when it's clear what the facts are, when he has stated yes I did that, stupid, it won't happen again – we don't really need to make a report. We have his statement, we store that and record the sanction in our systems and that's it. [Respondent 19 – corporate investigator]

Private investigation firms are commercial entities in their own right, external to the clients who hire them. The relationship to clients is therefore somewhat different from that of in-house departments. The fact that they are *external* to the organisation gives an investigation done by a private investigation firm an air of objectivity, although the commercial relationship between client and investigator somewhat dilutes the independence of investigators. While they are more expensive than in-house investigators, many (especially smaller sized) organisations do not have their

own in-house security department and are as such reliant on external investigators. The hourly rates of private investigation firms are often lower than those of forensic accountants and investigators with a legal background. Their clientele consists of small and medium size companies and (semi) government organisations but larger companies may also call upon private investigation firms for investigative services.

The fact that private investigation firms need a permit, based on the Wpbr, may provide them with some legitimacy. In practice, the control over the permit, exercised by the police, is very limited (Batelaan & Bos, 2003; Inspectie Openbare Orde en Veiligheid, 2009: 8). Supervision is mainly focused on formal safeguards up-front (regarding the decision to grant a permit) but there is no real control once a permit has been granted (Kolthoff, 2015). In addition, respondents indicate that the administration of permits is incomplete.

> If you try to gather information on how many private investigation firms have a permit you will find that the numbers known to the justice department and those known to the police do not match. And some have no identification card, which means that they have a permit but are not eligible for an identification card... And also that they might not be known to the police. So the supervision, that's just really bad. And the police do not give it any priority either, it's a purely administrative process for them. [Respondent 41 – corporate investigator]

Before the revision of the Wpbr in 2006, private investigation firms had to report on a yearly basis to the police about their activities, a requirement that has since been lifted (Klerks, 2008: 16). This mandatory report was not very informative and many private investigation firms did not see its point. "We had to report every year about the number of cases we did, but that's just a checklist. It does not contain any information whatsoever on nature, size etc. Nothing about the type of client, it's useless. But we report because that's the law" [Respondent 1 – corporate investigator]. According to the official announcement in which the change in legislation has been made, the government felt that the costs connected to this obligation for the private sector outweighed the benefits for the state in receiving them.[34] Hence, the requirement to file a yearly report was removed from the Wpbr.

In addition to the permit, some private investigation firms have a quality certification issued by the representative organisation NVb. However, not every private investigation firm is a member of this organisation and some respondents even indicate they have discontinued their membership as they did not feel represented by the organisation. "We have debated whether or not to be a member

34 See *Staatscourant, 2 oktober 2006, nr.191*.

but we decided not to. Their focus is on the lower tier of the market, those whose clientele consists of private persons and smaller companies, the simple cases" [Respondent 13 – corporate investigator]. To complicate matters further, there are also other representative organisations available, such as the Association for private investigation firms (Bpob) or (the Dutch chapter of) the American Society for Industrial Security (ASIS) or the European Corporate Security Association (ECSA). As such, there is not one representative organisation exercising control over all private investigation firms.

Control over private investigation firms in reality comes down to the client or a judge (when a judge is involved in the settlement of the matter).[35] This may be considered a bit problematic as investigators have a relationship of commercial dependence with their clients. The question could be asked whether the client would indeed interfere when his interests are served by some illegal activity of investigators. The dependence on their clients has led to a reputation of "the fired ex-cop who started his own little investigation firm. You know, the guy with the hat and the raincoat, hiding in the bushes. I'm not saying that they aren't there as well, but that the minority" [Respondent 41 – corporate investigator]. Despite this image, most private investigation firms are professional organisations, focusing on corporate clients and bound by the Wpbr and the Privacy code of conduct for private investigation firms. This Privacy code of conduct is quite clear and provided some detailed guidelines, however it is largely up to the firm itself to control compliance (also by putting mandatory complaints mechanisms in place). One of the complicating factors with regard to control is the emphasis and importance investigation firms place on their independence. Private investigation firms rely heavily on their individual reputation of being an independent and objective party, even when they are bound to their client for commercial reasons. Many respondents stress that when they feel they are being used by a client, they will terminate the investigation (see also chapter 3).

> During the inventory of cases for the case studies I came across some records of cases which were turned down or handed back to the client. When asked about this [investigator] explained that, in principle, all cases within the field of expertise are accepted. Observation Company 1 is a commercial entity and needs clients. However, there are cases in which there are conflicts of interests or in which there does not seem to be a just cause for investigating, or the assignment the client wants performed is not just. 'I have had a situation in which the chair of the board of directors wanted us to look into the expenses of one of the other board members. But then you continue your conversation and then it becomes clear that there is no cause for that. That it's just a conflict within the

35 See chapter 3 and 4 for more detail. Neither in civil nor in criminal court are judges eager to expel evidence which is considered to be illegally obtained by private investigators.

> board of directors and that this director thinks it is very convenient if that person could be removed. That's no just cause for an investigation.' [Excerpt from observation 1]

One of the ways of procuring independence and preventing clients from interfering with the contents or outcomes of the investigations, is not to provide them with preliminary findings while the investigations are still in progress. Thus, this situation makes it difficult for a client to unjustly steer the investigation, however it makes it equally challenging for a client to exert some kind of control over the investigations. Respondents indicate they inform clients about progress of the investigations, so some general control is possible.

> Once you get started you should remain in contact with the client because when an organisation is confronted with fraud this will have a lot of impact on that organisation. Tensions will occur so you need to be aware of that. But it is also important to keep them informed about your actions of course, what are you doing, what do they think you are doing. You can and sometimes should consult with the client about the course of your investigations but in the end it is our decision. Because we are investigating independently. Our investigations are concluded by a report and that report may be used as the basis for criminal procedures or a civil suit so you need to make sure it is done properly and will hold up in court. [Respondent 5 – corporate investigator]

Private investigation firms need to balance their independence and objectivity with the commercial relationship they have with clients. This is of course easier to do in a time where there are many assignments available than in a time of economic austerity. While it was impossible to make such a comparison in the context of this research, it would be interesting to focus on this subject in further research.

Just like private investigation firms, forensic accountants are external to the client and have a commercial relationship with said client. While private investigators are sometimes still regarded as the dodgy rent-a-cop who is going through the garbage, forensic accountants have quite a different reputation. The reputation of forensic accountants has long been that they are impartial, objective investigators and many (especially large) organisations tend to hire them 'for the name'.[36] The oath that has recently been made mandatory for accountants may help to sustain this image.

> I wouldn't hire a forensic accountant. For the simple reason that you don't really get value for money. They do the same as investigation firms but their prices are sky high. I wonder why a company would hire them; I guess because of the Big Four logo. 'Look,

36 Whether this is changing in the aftermath of the reputational damage the accountancy profession has suffered in the economic crisis remains an open question at the moment.

> we have hired a big company and spend a lot of money so it should be ok'. But in my opinion there's not much to separate them from a private investigations bureau. [Respondent 31 – corporate investigator]

In spite of the scepticism of this (in-house security) respondent, many large clients feel that it is safer to go for the big name than to hire a smaller investigation firm. Big Four (and other large) accountancy firms are well-known and are largely considered to be experts on corporate investigations. In addition, forensic accountants have an image to be more strictly regulated than other investigators. This would provide them with more legitimacy than the other investigators, who are sometimes referred to as 'cowboys'. As we have seen in this chapter, this is not the case in the strictly legal sense. The legal framework applicable to accountants is put in place for their more traditional core tasks and they are not specifically adapted (or very helpful) to investigative activities. The (not legally binding) guidelines for person-oriented investigations and the more general rules of professional conduct for accountants, issued by the NBA, are not very specific either. They are focused on general normative considerations and principles of law and as such respondents seem to regard these guidelines and rules as normatively restrictive and stringent. As related above, these guidelines and rules are used in disciplinary proceedings and as such there is a reasonable measure of control.[37] The case law provided by the accountancy chamber is effectively used as regulation by forensic accountants. Still, the fact that disciplinary proceedings are quite regularly launched against forensic accountants may be an indication that the rules to follow are not quite clear as of yet.

The main selling point of forensic accountants, their good name and reputation as impartial, does warrant some critical reflection though. The commercial relationship with the clients is also relevant for forensic accountants and even though it may be easier for a large accounting firm to reject an assignment when this is deemed morally correct, the fact remains that to do so does create a loss of business. Furthermore, forensic accountants from large accounting firms might find themselves in the position where their firm is also the auditing accountant of the client. Although this situation is convenient for the client, it may not be desirable with regard to impartiality. Not only does the client represent a large commercial interest for the accounting firm, it may also be the case that the auditing accountant has made mistakes. Although not necessarily problematic, this does harbour the potential for conflicts of interest. Van Almelo (2016), in his collection of accountancy 'slips', shows that this is not merely a theoretical danger.

37 This control is of course dependent on someone complaining about the accountant and making a disciplinary case against him.

> Our disadvantage compared to large accountancy firms is that our services are limited to forensics. [But that is also] an advantage because we will not get in the conflict of interest situation, we can take any job and we can be firm in our report, we never have to be afraid that what we report has negative effects for colleagues who are doing the auditing services because we don't have those. But on the other hand, it also means we don't have our own steady customer base. [Respondent 2 – corporate investigator]

The same goes for investigators within large legal firms who do investigative work. In an investigation for the Dutch Railway company, legal firm De Brauw Blackstone Westbroek was criticised for being the investigators in the case, while also representing Dutch Railway in a procedure with the Authority for the Financial Markets in the same case (NRC, 2015). Although the results of the internal investigations have been validated by two second opinions, the double-role of the law firm remains contested (advocatie.nl, 2015). As mentioned above, lawyers are by law partial to their clients' interests. However, when they are hired for investigations, this partiality is problematic as corporate investigators strive to be impartial.

> There are now more and more lawyers who focus on the corporate side. They pretend to do independent investigations, which is obviously not true. Because they are lawyers, and they do not confirm by contract that their investigations are independent. If I was an accountant, I would be very critical about that. Ok so you have a report and it states many findings but whether it represents that which should have been investigated, you can't tell. Nor whether they have written down everything that should have been written down. [Respondent 32 – forensic legal investigator/client]

This respondent, a lawyer himself, is quite critical about a lawyer's ability to act as an independent and objective investigator. This situation is not improved by the possibility of the use of legal privilege by lawyers. The legal privilege may be problematic from the point of view of control and independence, it is at the same time a major benefit for clients. As mentioned, corporate investigations carry the risk of their findings being used in a criminal proceeding against the client. (Derived) legal privilege may protect against this risk and for this reason lawyers are often involved in one way or another in investigations. However, as mentioned above, when an investigations report does not contain legal qualifications and is purely about fact finding, the court has ruled that this is not protected by the legal privilege.

One circumstance which might be valued by clients is that legal firms have a good reputation – just like forensic accountancy firms – and are considered as 'morally sound', while they do not have any specific rules to follow when it comes to corporate

investigations. As is the case with accountants, the brand the firm's name represents is important here.

> For me, as a lawyer, I don't have to do anything. I'm not bound to rules. So I can do it [investigate] any way I see fit. On the other hand, accountants are regulated. They have a stamp of approval – I'm not sure anyone would believe in accountants anymore but if they do, the rules surrounding accountancy make for a sort of quality hallmark. A lawyer doesn't have that, he only has his own name and reputation. [Respondent 32 – forensic legal investigator/client]

The laws on the profession of lawyer are not specifically applicable to investigative activities and there are as of yet no specific guidelines for investigators with a legal background. There is a system of disciplinary proceedings but contrary to the case of forensic accountants, there have scarcely been any proceedings aimed at investigative activities as of yet. This all culminates to very little effective control. There is much discussion about whether or not this should be considered problematic. Many respondents with a legal background feel it is not – they feel that the legal obligation to be a good lawyer is enough.

> Accountants have a set of guidelines for [investigations] which are actually quite inconvenient. When they interview people, their rules for person-oriented investigations may work against you. They are not completely illogical safe-guards but they can be very annoying because you have to for example give information to some person who might be a suspect, while you have to keep you client in the dark. So sometimes we work without the accountants. They are only detrimental to your investigations then. [Respondent 28 – forensic legal investigator/client]

Though understandable from a strictly efficiency-oriented view, the fact that certain investigators are used or not used because of the legal framework that applies to them could be considered as a downside to the fragmented nature of corporate investigations regulation. This situation invites forum shopping by clients, not only on merit but also on applicable legal frameworks. Even though there are few examples known in which corporate investigators actually do break laws and more general normative guidelines, the possibility to do so exists and a client with 'bad intentions' may quite easily abuse this situation. Control is largely left to clients and corporate investigators themselves. In those cases in which a judge is involved in the settlement of the matter, respondents suggest that (regardless of the type of investigator) evidence is only rarely excluded.

So if there's no effective control and everything is pushed back – you would have to admit that the control over the use of the material that has been collected by a judge is very limited as well. That is, if it happens at all. There is a great ruling about a case in which the adversarial principle has been broken. And the judge just doesn't care. He just accepted the report. If this is the way we treat this issue, you can make all the rules you want but if there's no-one connecting consequences to the infringement of the rules… And the same goes internationally, most of the cases never reach a court in which control could be exerted over the ways in which information is collected. And if it does happen, there's no hard and fast legal framework to compare the behaviour to. [Respondent 41 – corporate investigator]

Table 2. Overview of four different groups of corporate investigators

Type of investigator / *Aspects*	In-house department	Private investigation firm	Forensic accountant	Forensic legal investigator
Specialist knowledge	Own organisation Interviewing	General Interviewing Often also expert knowledge on other areas (niche)	Administrative/financial Often also IT-tools for big data	Legal implications of investigations
Service provided	Investigations Report (not in every case) Report to law enforcement authorities if necessary	Investigations Report Advice and help with settlement	Investigations Report Report to law enforcement authorities if necessary but no advice on how to proceed	Investigations Report Legal advice Help with settlement
Rules and ethics	Internal regulations Normative guidelines	Wpbr-permit Normative guidelines	Accountancy legislation Normative guidelines	Lawyer legislation Legal privilege Normative guidelines
Control	Internal control Judicial control (if the case reaches court)	Control by police Judicial control (if the case reaches court) Control by client	Disciplinary proceedings Judicial control (if the case reaches court) Control by client	Disciplinary proceedings Judicial control (if the case reaches court) Control by client
Costs	Relatively low	Medium	High	High
Position regarding client	Part of client	'Independent' Commercially dependent on client	'Independent' Commercially dependent on client Possible conflicts of interests	Partial to client Commercially dependent on client Possible conflicts of interests
Reputation	Reputation as being partial	Reputation as being client-centred Well-known as either generalists or niche	Reputation as being impartial Big name: 'You pay for the name'	Reputation of high morality Big name: 'You pay for the name'

Discussion

This chapter has delineated the different legal frameworks surrounding corporate investigations in the Netherlands. Although one conclusion may be that there are many differences between the various investigators, it is important to note that while this may be the case, there are more similarities still. In their 'pure form' there are substantial differences between in-house departments, private investigation firms, forensic accountants and investigators with a legal background. However, there are very little corporate investigation units in this pure form. In-house departments and investigation firms predominantly staffed with former police officers recruit accountants, lawyers and IT-specialists, forensic accountancy (departments of) firms employ former police officers, lawyers and IT-specialists and investigative (departments of) law firms also hire people with an IT or public-sector background (in their case, mostly former prosecutors). Should some expertise be required that is not available to the corporate investigators, specialists are contracted-in for that part of the investigations. While the field is thus simultaneously specialising and generalising, the legal frameworks in which corporate investigators operate remain dispersed and unclear to most of the people involved.

The overview presented in this chapter is not exhaustive. Specific laws are applicable to specific fields of industry, which for example may render disclosure to a supervisory agency necessary. It would be overly complicated and confusing to the reader to go into detail regarding all these regulations. However, this circumstance makes for a quite fragmented context of legal frameworks and many respondents are not up-to-date on all the rules they need to comply with (even when they think they are). One case in point is the controversy over the (non-)necessity for forensic accountants to have a Wpbr-permit. As stated in this chapter, forensic accountants are explicitly exempt from the permit obligation. The fact that there remains confusion about this point is an indication that this is considered peculiar by many of the investigators involved. Even more peculiar may be the relative silence in this regard about whether or not corporate investigators with a legal background should have a Wpbr-permit. In my opinion, it would be beneficial to the sector to have one set of rules, applicable to all involved. The fact that the different types of investigators try to incorporate each other's strengths makes the fragmentation within the legal frameworks problematic, both from a level playing field point of view, and from the perspective of rights of the people involved.

While it proves difficult for investigators to be sure of the legal frameworks that apply to them, it is even more difficult for clients and maybe more importantly, for involved persons. Not being a suspect in the sense of a criminal justice procedure places the subject of investigations in a precarious position. Cooperation with investigations by

individuals might be voluntary, there may still be a lot of pressure from one's employer to cooperate. The fact that rules differ between investigators makes it more difficult to ensure fair play. Many respondents feel this and commit themselves to the rules they deem most stringent, usually a mixture between the Privacy code of conduct for private investigation firms and the more general principles of law guiding forensic accountants and lawyers (which are in part already incorporated in the Privacy code of conduct). However, as a result of the voluntary nature of this, and the lack of control over their application, these rules and principles of law are vulnerable to deviation. Respondents stress their own reputation and their commitment to rules and principles of law and my research does not give strong indications of widespread problems. However, as chapter 3 illustrates, even when following the rules, investigators may for example place involved persons under duress. And, additionally, chapter 4 shows the profound impact which corporate investigations may have on individuals.

The corporate investigations industry thrives on the basis of the marketing of discretion and trust. This means that the sector is not very visible, neither to the public eye, nor to the state. White (2014: 44) has argued that "because of the distinctly 'un-police-like' way they perform these functions" and the fact that they "also undertake functions which are not usually performed by police officers" (e.g. forensic accountancy), corporate investigators tend not to be associated with the police, which "equates to near zero visibility through the state-centric lens".[38] The lack of transparency has been problematised before, however the (political) discussion remains largely focused on private security more generally (see for example State secretary of justice and minister of the interior, 2009). Even when private investigations are mentioned, the discussion usually remains centred on private investigation firms instead of the entire corporate investigations industry (see for example State secretary of security and justice, 2016). As a consequence, all those investigators without a permit remain out of the (regulatory) gaze of the state (White, 2014). By abolishing the obligation to provide the chief of police with a yearly report on investigative activities (again, for those with a permit) the state could be said to actually further diminish its information position (although the yearly report was not very informative). One suggestion to enhance the state's information position on investigative activities, made by *inter alia* Fijnaut (2002), is to institute a duty to report every crime to the police. Even leaving aside for the moment other issues such as capacity and expertise problems within the police and prosecution, such an obligation would prove counter-productive in my view. The flexibility in the legal venues chosen for the settlements of internal norm violations, as well as the use of discretion in investigations and settlements and the trust clients place in investigators are highly important to the success of the sector (Williams, 2005).

38 Although, as we have seen, *within* the sector there is a view of private investigation firms being the most police-like. This would substantiate White's claims that these are the ones being regulated (as the Wpbr excludes all others from its framework).

As Van Wijk et al. (2007: 226) rightly state, such a duty would furthermore lead to a kind of 'junior partnership', with corporate investigators working as the junior in a field defined by the priorities of the senior (the state). As mentioned in the previous chapter, such a view of the corporate investigations industry does not align well with its practical reality. In addition, a duty to report would require a (legal) interpretation of the facts by the investigators, something which forensic accountants tend to stay clear of. Van Wijk et al. (2007) suggest that if such a duty would be considered desirable, it should be applied to the client, not to the investigator. Investigators are bound to discretion; this is one of the selling points of corporate investigation services. A duty to report would therefore put the investigator in a difficult position towards his client.[39] Furthermore, corporate investigations are not restricted to the investigation of criminal behaviour, other unwanted behaviour being included as well – in these cases, there would remain a lacuna in control even when there would be a duty to report every crime to the police.

A less drastic measure, which is more in line with the abovementioned practice in the corporate investigations field as well, would be to include all those who investigate professionally in the permit system of the Wpbr. As related in this chapter, respondents do not think highly of this system – there is very little actual control and educational and other demands on permit holders are regarded to be quite low. It would therefore be constructive to upgrade these in the process. One benefit of having a comprehensive permit system is that it would render control possible (at least in theory – in practice this also depends on prioritising of the supervising authority). Another is that the Privacy code of conduct, used already by most corporate investigators in practice, would be applicable to all corporate investigators. As suggested before by *inter alia* Klerks & Eysink Smeets (2005) and CBP (2007), the nature of the activities would then be the primary concern in the decision whether or not a permit is necessary, instead of the current situation in which the permit obligation is connected to an investigator's professional background and relationship to the client. This would also make those who define themselves as for example 'mediator' or 'information broker' and occasionally provide clients with investigative services, liable to the law.

There have been voices advocating the formation of a representative organisation for (all) corporate investigators. At the moment of writing, there are multiple representative organisations available (both nationally and internationally), however none that brings together all four major groups of corporate investigators. In the same vein, the formation of a central register for (corporate) investigation experts in the Netherlands has been

39 As explained in chapter 4, there is a duty for public sector organisations to report crime to the police (article 162 WvSr [Criminal Code]). In many cases, organisations do not comply with this obligation and deal with the matter privately. Furthermore, there is a general obligation to give notification of suspicious transactions, based on the Wwft. This does not seem to lead to a more comprehensive overview of corporate investigations at the moment.

suggested. At the moment there is a multitude of certification and educational institutes, resulting in a vast number of different professional titles and accompanying professional registers (Dubbeld, 2015). "I feel like our Dutch market is relatively juvenile. For example, we don't really have a good institute to represent us. Look at the ACFE [Association of Certified Fraud Examiners], with all due respect, some of its members got their membership as a free gift or something" [Respondent 13 – corporate investigator]. This quote from a manager of a private investigation firm expresses the feelings of many respondents: even though there is a multitude of representative and certification-type associations available, many corporate investigators do not feel represented by them because of a perceived focus on certain types of investigators within the association, or as a result of the perception that the quality standards of these associations are low. This research has not investigated the validity of these perceptions. However, the result is that many corporate investigators are not members of a representative association, and those that are, are divided among many different associations. Recently, new initiatives have attempted to create the desired uniformity by the formation of a representative organisation for financial forensic experts, with an accompanying register – and title.[40] In the field of education, new initiatives are also formed to create courses in fraud examination.[41] The question remains whether these initiatives will be successful. At the moment of writing it seems that rather than constituting a representative organisation which may represent all corporate investigators, the new initiatives add to the fragmented corporate security landscape. Because of the fragmented nature of the sector, combining all different actors into one representative organisation seems a considerable challenge. In the words of Thumala, Goold and Loader: "if the industry is not a coherent whole, it cannot be represented as such" (2011: 293).

Unifying the legal frameworks for corporate investigations into one would not mean that there is no room for additional (self-)regulation with regard to the specific elements in which certain investigators differ from others. The legal privilege for example should not be rendered completely obsolete in cases of corporate investigations. Legal privilege is an important principle of law and when used correctly it protects those involved in legal disputes. However, as the court ruling in the Vestia-case has indicated, the applicability of legal privilege to 'fact finding' investigations should not be taken at face value. Additional (self-)regulation is likely to occur as a way for the different types of investigators to market their perceived

40 According to the website of the in 2015 established NFFI (*Nederlands Financieel Forensisch Instituut*), its register is to date filled with a very modest number of experts (see www.nffi.nl). The Institute for Financial Crime (IFFC) was also founded in 2015 and is an example of a new representative organisation, active as a knowledge centre and explicitly aimed at public/private cooperation (see www.iffc.nl).

41 See for example https://www.accountant.nl/nieuws/2017/5/nieuwe-opleiding-fraudeonderzoeker/.

superiority. This is already done at the moment as this chapter has shown. One could envision a system in which more specific (self-regulatory) codes that are desired by different professional groups of investigators are incorporated in the existing Privacy code of conduct. If all investigators fall under the Wpbr, it follows that the Privacy code of conduct applies as well. This is essentially self-regulation which has been approved by the Data Protection Authority. Any addition to the Privacy code of conduct by distinct professional groups may then also be handed over to the Data Protection Authority for approval. In practice, the different groups of investigators seem to be largely following the same rules already – but only one group does this based on an explicitly codified legal framework (private investigation firms).

With regard to the fragmented nature of the legal frameworks in the Netherlands, it is interesting to look at other national jurisdictions. In the context of this research a very modest side-step was made to the UK.[42] It seems that the private security sector in the UK has historically had more of an image problem than the private security sector in the Netherlands (see also White, 2014). The corporate investigator quoted below indicates that this circumstance might have made relations with the police more problematic, going on to suggest that this is one of the reasons the corporate investigations sector in the UK is eager to be regulated.

> This brings me back to the appetite to be licensed because if the police could see this is a licensed, regulated occupation then they would have to say well ok you're recognised now, you're a lawful entity. You're not criminals, you're a profession and you can be regulated, you can have your license revoked if you don't comply with the rules. [UK Respondent 3]

This connects to the point of applicable legal frameworks, in relation to which a notable difference with the Netherlands may be discerned. As Button already remarked in 1998, "there are no special statutory requirements to become a private investigator in the U.K." (1998: 3). In spite of a 2013 announcement by the home secretary that the private investigations industry was to be regulated, a permit system and the accompanying

42 This is a result of the Liverpool-seminar that I have organised together with John Moores University. The seminar served as a platform for discussion between participants (being academics, corporate investigators and law enforcement professionals) and myself. In addition, three corporate investigators were interviewed in this context. Interestingly, from the UK interviews similar information was derived as in the Dutch context. The UK respondents mentioned the same type of norm violations, investigative methods and corporate settlements as the Dutch respondents. With regard to public/private relationships the same kind of frustrations emerged from the discussion with seminar participants as can be derived from the Dutch interviews and, similarly, from the UK interviews these themes also emerged.

legal framework have yet to be arranged (Home Office, 2013).[43] As such, the situation is that "there aren't any all-encompassing rules, no. As long as they stick by the law of the land then they virtually do whatever the company expects them to do to carry out the company procedures and enforce the company regulations" [UK Respondent 1]. In the meantime, representative organisations have introduced their own licensing-type arrangement, however this is not obligatory. The very modest work in the UK points to a situation in which the corporate security market is (even) less regulated than in the Netherlands and the legal frameworks (even) more fragmented. It would be interesting to make a proper comparison between the Dutch situation (in which a licensing system and a formalised legal framework does exist – at least for private investigation firms) and the UK situation (in which no such obligation rests upon corporate investigators). An important question in such a comparison would be whether the type of regulation and the absence of a licensing system (combined with an even greater lack of control over the sector than in the Netherlands) have bearing on the manner in which corporate investigators provide their services and whether this affects the perceived legitimacy of the sector.

As this chapter has shown, there are both similarities and differences between the four groups of corporate investigators. The differences are used as a marketing tool, setting each type of investigator apart from the others. The nature of these differences does not justify a separate account of each group of investigators in the remainder of this book though. When the differences are relevant, mention will be made. The above suggestion to unify legal frameworks for all corporate investigators should not be considered as the solution to the problem of control in the corporate investigations sector. As the following chapters show, the corporate investigations industry has, by its marketing and professionalisation of its unique characteristics, created a private legal sphere in which it operates. Corporate investigators largely remain out of sight of the state, making effective control very challenging (Williams, 2006a). To fully understand the extent to which corporate investigators may stay within the private legal sphere, it is important to examine their day-to-day business. Thus, the investigative process is discussed in the next chapter, after which the ways in which the investigations are used by clients to deal with the matter at hand are examined in chapter 4.

43 This does not, however, mean that the UK corporate investigation sector is completely unregulated. UK Respondent 2, for example indicates that in addition to having to notify the Data Protection Authority that personal data is being processed, there might be certain additional standards that apply to investigative work in for example the health care sector. "Fundamentally, the back-story to everything I do will be UK criminal law, police and criminal evidence act, procedures and investigations act. So how you do your investigations will always be to that sort of standard. But then, having worked in different sectors, the different sectors themselves all have certain rules and regulations that are applicable to them" [UK Respondent 2].

Chapter 3

Corporate investigations

The investigative process and sources of information in corporate investigations[44]

44 A version of this chapter was published in *Erasmus Law Review* (2016): Meerts, C.A. (2016). A world apart? Private investigations in the corporate sector. *Erasmus Law Review, 9*(4), 162-176. I thank the reviewers and editors for their useful insights with regard to that paper.

Introduction

> I remember from my time in the police that we were always complaining that private investigators were able to do anything and could just barge in somewhere. And now that I'm on the private end we as private investigators complain that we *can't* go in because we don't have the authority to do so. If someone doesn't want to cooperate we can't do much [Respondent 5 – corporate investigator].

Private investigations are often contrasted with criminal investigations done by the police. A recurrent image within law enforcement is that corporate investigators have much leeway to perform their investigations the way they see fit because a legal framework is lacking.[45] At the same time, corporate investigators feel restricted in their work because they cannot perform the same activities as law enforcement agents can. As we have seen in chapter 2, corporate investigators are regulated, although the legal framework is quite scattered over different professional groups and control over compliance to these regulations is rather limited. The most specific regulation available to corporate investigators is laid down in the Privacy code of conduct for private investigation firms (NVb, 2015). While this is legally binding only to those investigators who possess a permit, corporate investigators without a permit (in-house investigators, forensic accountants and forensic legal investigators) seem to largely comply with the rules of the Privacy code of conduct as well.

The contrast between the view of law enforcement professionals and the wider public on the one hand, and that of corporate investigators on the other is interesting. The key point in this controversy has to do with (the absence of) formal powers of investigation. Powers of investigation are, by law, granted exclusively to law enforcement professionals.[46] As a consequence, there are no private powers of investigation: corporate investigators have the same investigative powers as any citizen. The sense of limitation, expressed by many corporate investigators formerly working in law enforcement, stems from this lack of official investigative powers. Having no access to formal powers of investigation simultaneously means, however, that corporate investigators can operate with considerable flexibility (Williams, 2005). Crucially in terms of access and speed, there is no need for them to wait for the approval of a prosecutor or judge prior to the use of the methods which are available to them (although corporate investigators do need the client's/management's

45 See for example the report of KRO Brandpunt, *Bespied door de baas* (1 June 2014) for a public image of corporate investigations. Available on http://brandpunt.kro.nl/seizoenen/2014/afleveringen/01-06-2014.

46 See article 141 and 142 of the Dutch Code of Criminal Procedure (*Wetboek van Stravordering* – WvSv). Article 141 charges the prosecution, police officers, military police and special investigative agencies of the ministries with the investigation of criminal offences. Article 142 states that the minister of security and justice may define additional persons as 'special investigating officer'.

approval). This contrast between the perceived bureaucracy of the state apparatus versus the expected freedom private investigators enjoy is a reason which is often given by corporate investigators with a background in law enforcement, when asked about their career switch.

> I think we can do a lot less than the police for example. We don't have any powers to retain someone. On the other hand, we might not have the threat of prison sentences but we do have the threat of losing your job. Don't underestimate the power of that either. Keep in mind that mostly we're not dealing with hardened criminals here, mostly it's just an employee who has done something wrong. [Excerpt from observation 2 - informal conversation]

Although corporate security actors have no formal *powers* of investigation, their *possibilities* to investigate are extensive: through the (property) rights of the organisation as an employer, they may use much information about employees. When corporate investigators investigate a case, they might gather a great deal of information by talking to people (interviewing), by looking into internal systems (e.g. personnel logs), firms' communications (email, phone records), financial systems (accounting, sales and other systems) and open sources (e.g. social networks) and by tracing assets. Much information gathering by corporate investigators relies on the cooperation of the people and organisations involved as it is impossible for corporate investigators to for example lay claim to financial records of individuals or organisations other than their client, or to enter premises other than those belonging to their client – these being powers granted exclusively to public law enforcement. This may mean that it proves impossible for corporate investigators to investigate a norm violation fully and in this case, law enforcement agencies may need to be mobilised by a report to law enforcement authorities. Whether or not the decision is made to do so depends on the client.

> A big difference is that law enforcement has powers we don't have. That's an essential difference. But the fact that we aren't the police also has an effect on people. In some investigations it would be nice to have powers of investigation, for example I'm working on a case now in which we think there has been a kickback somewhere but we can't prove it. The police could subpoena bank records and create a money trail. But, what I just said – people are different to us. Our big advantage is that they talk more easily to us. They are more relaxed with us in interviews because we're not the police. So on the one hand it's a disadvantage not to have powers of investigation, on the other it's an advantage because people see you as less of a threat. [Respondent 3 – corporate investigator]

The greater part of internal norm violations occurring within organisations never reaches the criminal justice system but is investigated by and settled with the help of corporate investigators within the private legal sphere (Dorn & Meerts, 2009). One of the reasons for this is that while investigations may concern (alleged) criminal behaviour such as fraud, they may just as well be about behaviour that is considered undesirable rather than criminal, for example conflicts of interests. In the latter case, there is no possibility to report the norm violation to the police and no criminal investigation will follow (Meerts, 2013).

This chapter follows the investigative process from start to finish, describing the investigative process and the investigative methods and sources of information available to corporate investigators. Some corporate investigative methods are broadly similar to those used in public policing (e.g. interviewing the people involved or observing someone – although the degree of duress, rights of the interviewee, etc. may differ), other investigative methods are more private in origin and in 'ownership' (e.g. forensic accounting methods or an audit of internal systems). At the conclusion of the investigative process, findings need to be reported to the client, most commonly in a formal investigations report. The chapter follows a corporate investigation chronologically, starting with the way norm violations reach corporate investigators and the assignment that follows (section 3), through the different sources and information gathering methods (section 3 and 4) to the conclusion of the investigations, culminating in the investigative report. Before discussing the investigative process and methods, section 1 reflects on corporate investigations by looking at the starting point of corporate investigations: the client.

1. The setting of corporate investigations – client centeredness

Private persons are allowed to investigate behaviour that is harmful to them – or to ask other private persons to do so – as long as they do not violate any laws. Legal persons are considered private persons in this sense and when they act as a client to corporate investigators, corporate investigators may use the investigative possibilities of their client. As an employer, an organisation has the right to control certain behaviours of its employees and many organisations have made provisions in the labour contract for the use of this information for investigative purposes (Schaap, 2008). Corporate investigators thus often have access to a considerable amount of information provided by the client.

Chapter 2 discussed the different legal frameworks that apply to different investigators. Some investigators' activities are regulated by law or self-regulation (e.g. private investigation firms and forensic accountants), while others rely on

disciplinary rules (in the case of lawyers, these rules are not specifically applicable to investigatory activities) or internal regulation (in-house corporate security). It is argued in the previous chapter that this situation leaves room for forum shopping by clients, and may lead to situations in which clients acquire the services of the investigator who is least regulated. However, the Dutch law safeguarding the protection of personal privacy (WBP) guides all corporate investigations and general prohibitions, such as breaking the (criminal) law, apply to all investigators. Chapter 2 has furthermore shown that corporate investigators indicate that they are guided by general principles of law and that they tend to commit to the guidelines codified in the Privacy code of conduct for private investigation firms (NVb, 2015) and the guidelines for person-oriented investigations for accountants (NIVRA/NOvAA, 2010). Because respondents indicate they largely follow the Privacy code of conduct, this chapter alludes to these more specific rules when applicable.[47]

The large diversity in professional backgrounds in the field of corporate investigations also creates a wide variety of skills and expertise, going well beyond those used in police investigations (Gill & Hart, 1997). These skills are applied to provide clients with swift results that can be used to prevent future incidents and, possibly, restore at least some of the damage done. The diversity in backgrounds and accompanying expertise make the corporate security field of interest to prospective clients. In his work on forensic accounting and corporate investigations, James Williams (2005) has pointed out certain characteristics of corporate investigations which are highly valued by clients. Not bound to the definitions of behaviour given by criminal law or by the (often slow and bureaucratic) structures of criminal procedure, corporate investigators may offer a high level of flexibility in investigative methods and solutions to clients. Secondly, the orientation in corporate investigations is on the client and the private troubles the client may have, rather than on criminal acts (which are defined in the Dutch criminal justice system as being against society). This means that whatever norm violation is deemed harmful by an organisation may be investigated by corporate investigators (and the assignment may also be limited to that specific norm violation). Thirdly, corporate investigations provide an organisation with a high level of discretion and a certain measure of control over the process and information flow. While following chapters show that there is consideration for common good considerations through non-contractual moral agency by corporate investigators (Loader & White, 2017), the main focus in corporate investigations is therefore on the client. Investigations are directed towards answering the questions that have been formulated in the assignment by the client. In addition, the internal information and systems that are available partly

47 See the previous chapter (2) for a general overview of legal frameworks applicable to the different professional groups of investigators.

determine the path the investigations will take. "At the start you will consult with the client about indicators, what is it we can do for you and what is it that we need to do to get there, what is the planning and of course what are the costs" [Respondent 5 – corporate investigator]. Thus, the services that are provided are tailor-made to meet the needs of the client. For example, when investigating a suspicion of fraud, corporate security investigators can be very cautious in their investigations, so as to not create unrest within the organisation. The interests of the client are prioritised in the investigations and this may mean that the investigations need to take a more subtle road than the police would take. Police investigations might be damaging to the operational practices of an organisation, especially since it is difficult for an outsider to understand the workings of internal systems (Gill, 2013). "[The police] do not understand our systems. We are the experts of our own systems and we have the necessary access" [Respondent 16 – corporate investigator].

> Ok so the police come in, take the administration. Do you have any idea what that does to an organisation? People go home sick, totally lost. And with us, things go more quietly. They don't even notice. They do when we start interviewing and that will produce unrest of course but that's at the end of the investigations. What we do is more subtle, we do custom made work. [Respondent 1 – corporate investigator]

The client-centeredness of corporate investigations may mean that corporate investigators go about the investigations more cautiously and more efficiently, but also that they focus on different information than law enforcement investigators would. An organisation is often in need of information fast so action can be taken. This information may not be the same as the information produced in the criminal justice process (as not the interests of the organisation are taken as a point of departure, but public interests).

> A corporation wants to know what happened. I just finished an investigation for a large Dutch company that suspected it had some issues abroad with one of the directors. That has to be cleared up within three, four weeks otherwise they can't act. No way that you go to the police first because that's not going to help you. They have their own responsibilities. They are not going to ask the organisation, what is it you need and I will look into it. It doesn't work like that. [Respondent 26 – corporate investigator]

2. Preparation for the investigations – the assignment

Depending on the position of the investigators, an investigation usually starts with an intake of the assignment (in the case of an external investigator) or the report of a norm violation to the security department (in the case of an in-house department) (Williams, 2014). Investigation firms and departments differ in their backgrounds and structure, as reflected by the observations conducted during this research. This means that there are also differences in the way corporate investigators are notified about norm violations. For example, there are large and small investigations bureaus (or forensic departments within accountancy or legal firms), and there are large and small in-house departments within large organisations. These may all have their own way of organising notifications. Observation Company 1 for example – a private investigation firm – had at the time of observation six employees, of whom five were involved in (all kinds of) investigative activities. Observation Company 2 – an in-house security department – had at the time fifteen employees, of whom eleven were involved in investigative activities. In Observation Company 2, there was a division of labour, with one team being responsible for the intake and registration of cases, one team focusing primarily on desk research and one team (in the lead of the investigations) focussing on interviewing. Leaving these organisational details aside, in general notifications are done by management or, in case of an in-house notification system, someone within the organisation.

Respondents suggest that not every assignment is accepted. In in-house departments this is more or less a decision based on priority: all cases are accepted in principle but during busy periods, it may be decided either not to investigate norm violations with minor importance, or to do so at a later point in time (which may very well be the same since the problem may by then be solved in another way by for example the manager).

> As a rule, cases are brought to the attention of the helpdesk and registered there. After that, cases are sent to the right place (internal, external, ICT). When it is an internal case, the case is prioritised (in reference to urgency, delicacy and harm) and the manager decides who will handle the matter. Sometimes a case will be reported directly to an investigator and he will start the case and register it on his name. Investigators also need to prioritise what to do and what not to do, sometimes there are just too many cases to do it all. [Excerpt from observation 2]

For those investigators working on contract basis, there is a greater necessity to accept cases, as they are commercially dependent on them.

> It's quite simple actually – basically we take on everything. In principle. Because we really can't afford to say no. Once you start turning clients down because you're too busy, chances are that that client will never come again. The nature of the work is such that you can't say 'things are too hectic right now, come back in three weeks'. The client has an immediate problem which warrants immediate action. So you need to get to it right away. So one way or the other, in principle it's a yes. And we can do it. [Respondent 2 – corporate investigator]

If the necessary manpower is not available, other investigators may be contracted as an addition to the team (the same goes for in-house departments that are temporarily short-staffed). Both Observation Company 1 and 2 had particular investigators from (other) corporate investigation firms who would be used in such cases. In spite of this commercial necessity to accept all cases, there are still assignments that are rejected by corporate investigators. Respondents are wary of being used by a client; there should be a sound basis, or in accountancy terms a 'just cause', for the investigations (NVb, 2015; NIVRA/NOvAA, 2010; see also chapter 2). The above-cited respondent goes on to say:

> So the only question is really, should we take the assignment and do we want to? I mean first of all, is there enough cause for an investigation? You're dealing with privacy aspects here so there needs to be a valid reason to investigate. Imagine that a CEO comes to you and says, 'look I have Mr. Jones here and he's in his late fifties, rather expensive, we would like to get rid of him but firing him would be expensive so could you have a look at his expense account and see whether you can't find something or other'. Well, no, sorry, we don't do that. By the way, it's not always that straightforward because if the same person contacts us, saying 'we think that Mr. Jones is fiddling with expense accounts for this or that reason...' The story is the same, it's just told differently. So it's not always possible to know exactly but you have to try. That's why an intake is so important, to get an impression of the context of the case, what kinds of signals are there, how were they discovered, is it specific enough to warrant investigation? When we are convinced of these aspects we may accept the assignment. [Respondent 2 – corporate investigator]

Respondents also indicate that it is not just a question of whether the assignment that is to be executed has a sound basis to commence investigations. In addition, investigators should be aware that clients might want to ask the wrong question, either on purpose or because of incompetence.

> The thing I have noticed in investigations for governmental organisations is that they purposively – at least I think it is purposively – pose the wrong question. Maybe

> you have read it, this case about that whistle-blower who committed suicide. And there were articles in the paper about officials who travelled on the expense of the organisations they should have been overseeing. So what happens, they hire an accountancy firm with no track record in investigations whatsoever and they are looking into the declared expenses. But that wasn't the issue, the issue was with the expenses which *were not* declared. I think that is purposively asking the wrong question. The answer will be, sure there was something off in the expenses here and there but those were minor things and with the other expenses they found no fault. No of course not. But that never was the issue raised by the whistle-blower or the newspapers. So, in such a way investigations can be used as a lightning rod, to distract people from the actual issue. [Respondent 41 – corporate investigator]

Some respondents indicate they do *pro bono* work as well. Observation Company 1 is an example of this. A small portion of the yearly capacity for investigations is reserved for *pro bono* work. It was explained to me that this usually is work for individuals rather than organisations, although small-scale organisations (which do not have the funds to facilitate investigations) may also be accepted as a *pro bono* case.

> And another thing is – assignments from individuals, how to deal with that. Individuals may also end up in a situation in which you think... Costs are an issue for individuals normally of course but sometimes you come across a case in which a very unjust situation has arisen and the person involved cannot go anywhere else to set it right. In such cases we might decide to do it anyway, even though it is a bad decision from a commercial point of view. Sometimes we agree on this beforehand with the client, then we make it *pro bono*. But in general what we do is, we assess what comes in, judge whether there is enough grounds to investigate and if that's the case we will in principle take the job. With the statement in mind that we have to be available all the time, otherwise clients will never come back. [Respondent 2 – corporate investigator]

When a case is indeed accepted, it is customary that the 'problem owner' – be that the manager of the suspected employee, the board of directors or someone else – and the investigators talk about the reported norm violation in order to form a clear idea of the scope of the problem. The extent to which this is possible at the start of an investigation can differ widely. Respondents indicate that investigations may start with a very clear suspicion towards one person or a pretty straightforward problem but it is also possible that the question put to the investigators is very broad. It happens that the client is for example merely aware that something is not quite right, but cannot put his finger on the actual issue. This means that the assignment of corporate investigators may be very specific or pretty broad. Respondents state

that the goal is to define the assignment as strictly as possible before commencing with the investigations. This is especially relevant for investigations conducted by external firms (as distinct from in-house or self-investigations) and in cases in which a certain individual is investigated (person-oriented investigations).[48] While this predetermined focus is helpful and beneficial to involved persons in the sense of the protection of their privacy, there are also some inherent dangers.

> Ok so there are suspicions against someone, we are going to investigate, that's why we're here. But it needs to be objective, unbiased. Not 'we want to get rid of him'. I have done an investigation where a director voiced suspicions against another director, something to do with expenses and overtime. I said, I'm not going to do that. Because, there are three directors here and if I'm going to investigate I need to have the context, so I will have to look at all three. Then you're investigating the way in which rules XYZ are applied. So that's what we did and it turned out the one pointing the finger was no angel either. So carefulness and clarity are important in your investigations, making sure you are not being used as the stick to beat the dog with and ensuring the individual is treated fairly. [Respondent 27 – corporate investigator].

However narrow an investigation may be at the start, during the investigative process the scope of the assignment may, in consultation with the client, be broadened or narrowed down. A broader scope usually means more investigations and thus more expenses, which makes deliberation with the client necessary. Respondents from in-house investigative units indicate they have more independence in determining the scope of the investigations. This is also apparent from the case studies from observation 2, which was done in an in-house department. In 8 out of 11 selected cases, the investigations commenced with a broad question and the scope of the investigations would be expanded during the investigations. For the case studies from observation 1 (executed within an private investigation firm) the situation was reversed: in 8 out of 10 cases the investigations started with a focused question. However, in these cases the investigations might also be broadened during the investigative process, in consultation with the client.

Respondents indicate that the dialogue with the 'problem owner' is especially relevant in the first phase of the investigations.

> [The level of contact with the client] depends on the phase your investigations are in and the nature of the issues involved. In the beginning of the investigations you're going to have much more contact with the client about things like, what kind of

48 As distinct from broader investigations into the organisation, not focusing on an individual but on an issue.

> information are we going to need, what is available internally, which information will need to be secured right away... That's contact on the operational level, with the IT-department, the business line, the department that's responsible for the issue. And the question is for example, will it be necessary to collect your information quietly or do the employees already know there's going to be an investigation and is it ok for you to contact the department and deliberate? How are we going to secure the information, is it a lot, are we going to gather everything, digitalise the information and put it in a big computer so we can search efficiently later on? Or is it limited in scale and maybe already digitally present? Well, those are the kinds of questions that are relevant at the start of your investigations. [Respondent 13 – corporate investigator]

After the assignment is determined and the problem defined, the investigations can commence. An inventory needs to be made of the type of information available and location of the information. The client is an important source of information here.

> You need to be introduced to the people you are going to need within an organisation. Because we want to interview them or need insight in the administration and things like that. The decision how to investigate and who to interview is ours, we might discuss with the client but in principle we are autonomous in that. [Respondent 5 – corporate investigator]

The methods to be used depend on the case. The use of cameras may be very helpful to see who has taken money from a cash register but it might prove useless in case of loss of money through digital channels. In addition, some clients may have their own camera systems, track-and-trace devices or other useful tools for investigations, while others do not. It might happen that an employee suspected of wrongdoing is suspended from active duty at an early stage of the investigations so he or she is not in the position to cause more harm. However, in other cases the employee is kept in place purposively to aid the investigations by trying to catch him or her in the act. This also depends on the severity of the matter.

> When it is someone high with a sensitive position within an organisation you don't want to wait until you have the results of the investigations before you act, he will be suspended immediately. That person will therefore know about the investigations in advance. When it's about the disappearance of items from the work floor or someone taking money from the till, you can wait and see what happens if you for example would mark a certain item [CM: to see who takes it]. There's much less of a rush there and the critical risk is less prominent. [Respondent 50 – client]

In general, corporate investigators prefer a suspension over an immediate dismissal of the involved person as long as the investigations are not yet concluded. "Sometimes the circumstances warrant immediate action. We prefer a suspension [CM: over a dismissal]. So they are still held to comply with your investigations because of the labour relation they have with the client" [Respondent 1 – corporate investigator].

The order in which the various methods are used may differ. However, it is common to start with the investigation of administration and the interviewing of witnesses. The interview of the involved person(s) is usually reserved for the end of the investigations, so as to be able to confront the person with the evidence against him or her. During the investigations, many corporate investigators generally keep an investigative journal for internal use. This journal records relevant actions taken by the investigators, contacts they may have had with people and other relevant information. Especially when there are multiple investigators involved in a case, this may prove very useful (however, respondents also indicate the thoroughness with which this journal is kept differs among investigators). The journal can be regarded as a log and can be used for the eventual report.

After the investigations have been concluded, a draft report is made. Relevant parts of the report are then usually handed to the involved person to read in accordance with the adversarial principle, which *inter alia* states that one has the right to be informed and be heard (see section 5.1 of this chapter). Part of the adversarial process is that the involved person has the right to know what has been written down in the report about him, and that he may react to this. After all involved persons have had the opportunity to make use of their right of inspection, the draft report is finalised and given to the client.

As do most professional procedures, private investigations have their own language (Falk Moore, 1973). This could also, as Thumala, Goold and Loader suggest, be "'occupational legitimation talk' that seeks to emphasize specialist expertise, competence and [client]-centeredness" (2011: 296). As a commercial market, corporate security tries to emphasise the niche value of its services by using different terminology. In this way, corporate security as a semi-autonomous social field sets itself apart from other professional fields. Chapter 2 shows that this process also occurs within the field, between the different professional groups of investigators.

In legal terms, investigative activities which are executed within the context of corporate security and those which are executed within the context of the criminal justice system are separated by a different terminology. As pointed out before, corporate investigators do not have powers of investigation and someone who is subject to corporate investigations is not protected by the rules of criminal procedure. Words such as 'suspect' and 'interrogation' are part of the criminal justice system and

therefore should not be used for investigations done in a different context. Most respondents from the private sector also refer to their activities with different words than commonly used for public investigations and some made a point of avoiding 'law enforcement terminology'. In the context of both observations, the same can be concluded: the investigative processes were defined in different terms in the official document than those used in criminal justice procedures and the informal conversations within the observation settings also followed these linguistic rules. Interestingly, clients and law enforcement respondents seem less rigid in their use of terminology. However, most respondents for example avoid the word 'suspect', using the words 'subject' or 'involved person' instead.[49] The same goes for the information source of personal communication: private investigators do not *interrogate* but they *interview* (NVb, 2015). This difference in terminology emphasises the difference in investigative powers, as the power to interrogate someone is exclusively granted to law enforcement agencies. The Privacy code of conduct for private investigation firms also explicitly avoids the use of law enforcement terminology (NVb, 2015: 26):

> This code of conduct abstains from the use of concepts that are present in the Code of Criminal Procedure to avoid confusion with the detection of crimes by law enforcement agencies. Private investigations do not take place under the authority and responsibility of the public prosecution office after all, and furthermore, its goals are different.

The use of different terminology separates private investigators and law enforcement on a symbolic level, something which respondents seem to underwrite. "We should really get rid of the image of being private coppers and get the focus on our problem-solving capabilities instead" [Respondent 40 – corporate investigator]. In the words of an investigator working for Observation Company 2: "I'm no private police". This difference is not purely symbolic: from an empirical point of view the differentiation also holds firm. Even though there are many corporate investigators with a law enforcement background, and their work may seem similar to the work of police and prosecution, there are notable differences. It has been remarked before that corporate investigators do not have any powers of investigation and that their investigations are not merely focused on crime. The point of departure – public or private interests – also differs between public and private investigators. Services provided by corporate

49 This research also avoids 'criminal law terminology', as the use of these terms would be incorrect in the context of corporate investigations. An involved person for example is not a suspect in the sense of a criminal procedure (and as such does not enjoy the same rights). The adversarial principle could be interpreted as being a criminal justice term (as it is a leading principle of law in criminal proceedings), however in the Dutch legal system, this is a term that is used in all legal proceedings, from administrative to civil to criminal, and it is thus not specifically linked to the criminal justice system.

security providers are thus more encompassing and focused on client interests. Below, the principle components of a private corporate investigation are discussed.

3. Gathering information – investigative methods leading up to confrontation

3.1 Internal documentation

A common first step in corporate investigations is to look at 'the paper work'. "It's difficult to assess whether the person is telling the truth and by starting with the financials, you can get a sense of what might have happened" [Respondent 5 – corporate investigator]. When business is conducted, actions are documented. This (digital or) paper trail is a very valuable source of information in the reconstruction of where the money went. Since the client usually is the organisation where the irregularities occurred, its records are generally available to the investigators. Because the client can order its employees to cooperate fully with the investigations, relevant parts of the organisation may deliver documented information quickly. These documents include 'anything that has been written down'. "We usually start with the records. And that is a very broad concept of course. There are financial records, digital but also hard copy. Digital is for example the books, and hard copy the invoices, source documents, everything that the books are based on" [Respondent 5 – corporate investigator].

It depends on the types of services or products the client delivers how these documents are constructed, but generally there are invoices, contracts, tenders and project reports available. Respondents state that this is a good place to start the investigations, after the initial talks with the client. These source documents may provide an overview of what happened fairly quickly.

> And then you directly have a lot of information, transactions are documented. There is someone ordering, there is someone who approves it, there is someone who enters it into the system... Payments are usually cashless, which means there are bank records of them. So you try to gather all relevant information, refine your knowledge and document it. [Respondent 28 – forensic legal investigator/client]

Much can be derived from the financial administration of an organisation. In case of a suspicion of fraud, the first step is often to identify the amount of money that went missing and where it went. Sometimes this provides a straightforward story and not much additional investigation is necessary. Outgoing payments from the accounts of the client often provide information on the person who received

the money. However, there are situations where ingenious constructions are used to disguise the path the money has taken and to hide the recipient. Information provided by the client might not be enough to trace the money or to find out what happened. The access to documentation is limited to internal information from the client, although involved persons may (and sometimes do) provide access to their personal accounts. Sometimes this means that – because of the lack of investigative powers – corporate investigators will not be able to pinpoint the problem. "There are situations in which you need the powers of investigation of the police. Especially in these financial investigations. Sometimes you need a warrant to get bank records. We can't get to bank records of third parties – that would be highly illegal" [Respondent 1 – corporate investigator]. This problem of access makes it more difficult for corporate investigators to investigate the norm violation fully when for example subcontractors are involved. "In the big investigation I told you about, there was a subcontractor involved and he had his administration, probably, at home. It wasn't available at our client company so we figured he kept it at home. We asked him for it but he didn't give it to us of course" [Respondent 5 – corporate investigator].

3.2 Internal systems

The situation presented on paper may not provide the full story to investigators and is liable to incorrect interpretation when used as the sole source. Additional information sources are necessary to answer the questions posed in the assignment. A logical next step is to look at other information which is internally available. A multitude of internal systems may provide much information for corporate investigations. Generally speaking, all these internal systems may be put to use for an internal investigation, as long as certain requirements are met (e.g. the employer has to announce in general terms to his employees that their movements may be tracked) (CBP, 2015a). Most of these systems are not meant for investigative purposes but can be used nevertheless. What kind of system is available depends largely on the (economic) activities of a client organisation. For example, logistics companies often have track-and-trace systems in their vehicles and security cameras are used more often in a large warehouse than an office floor.

3.2.1 Communications and data carriers

Organisations often have their own internal communications systems and they make use of (systems of) hard- and software. Email-inboxes, mobile phones, personal computers, laptops and external memory devices may all contain valuable information. Privacy legislation allows for these to be investigated when they are owned by the employer (NVb, 2015). By extension, corporate investigators have access to the information provided by the use of organisational facilities by employees.

There are multiple, more and less intrusive ways to investigate communications and data carriers. According to the widely used principles of law of proportionality and subsidiarity, investigative methods should be proportional to the goal (and the interest of the client for reaching this goal) (proportionality) and the least intrusive methods should be used when possible (subsidiarity). Respondent therefore indicate that they always attempt to use the least intrusive method of investigation.

> We don't wire-tap telephones. But for example, our stock-traders, they may only use the company phones for their activities. And all these calls are registered, to make sure no confusion may occur later on about amounts etc. People know this, those conversations are recorded. And if necessary we may listen to those tapes. And we can make analyses of the phone records, who are they calling, what are their contacts. But we're not wire-tapping for investigative purposes, listening in on their conversations. [Respondent 39 – corporate investigator]

To stay with the example of recording telecommunications, it is possible to record a telephone conversation, but one could also use mediation to track a phone. Data mediation in general refers to the process in which usage data from networked devices (such as mobile phones) is collected and processed, usually for billing purposes (Balter & Bellissard, 2003). It can however, also be used in investigations. Mediation is less intrusive because while it shows where the phone has been and who has (been) called, the content of the conversation is not recorded. Often, mediation is a very useful tool. For example, case study 21 of the case studies, mediation was used to prove that an employee was near the building where some equipment was stolen on the day of the theft, even though he had called in sick and was no longer working in the building.

When for example some property has gone missing it might be helpful to know what has been said in phone conversations or by email. Phone calls cannot be retrieved retrospectively so a recording device has to be present at the time of recording. When it comes to email, older information could be retrieved. Email-boxes may be 'imaged' and stored in a database to search. This also goes for 'the digital environment' more generally. "In the larger investigations, data recovery is a standard ingredient. This means that the digital environment is imaged and put in a database. This may become pretty complex because you have to take privacy regulations into account and when the data crosses the national border, this may be a problem" [Respondent 28 – forensic legal investigator/client]. Data carriers such as personal computers, laptops, external memory devices and tablets can also be investigated on content or on activity (e.g. internet logs) if they are property of the organisation. The growing use of BYODs (bring your own device, usually a laptop) may in this regard prove problematic for corporate investigators, as it is not permitted to investigate these.

As mentioned before, corporate investigators lack the powers of investigation law enforcement has and therefore their access is limited (though still quite extensive). Within the boundaries of available information, corporate investigators may however investigate more effectively than law enforcement would, especially when it comes to complex internal systems.

> Of course they [law enforcement agencies] may demand information and we will have to provide that. But often they don't quite know what kind of information they need. For example they ask for the laptop of the involved person. But with that they don't have access to our system, just the computer. You need authorised log in codes to access the system and they don't have that. I sometimes try to explain this but unless you're talking to someone from a specialised high tech team, they don't know what you're talking about. They don't understand how our systems work. Neither do I for some part but we have people here who do. Generally they just look at the laptop and stop there. There's an entire world of information behind that which they'll never see in this way. [Respondent 43 – corporate investigator]

3.2.2 Other internal systems

In addition to the abovementioned communication systems, there are many other internal systems that may provide information. Many organisations for example use a key card system for employees to gain access to a building. These can be used to find out whether someone has been present at a certain site.[50] Track-and-trace or GPS systems are also used by some employers, to keep track of their deliveries or vehicles and these may provide information on someone's whereabouts. In addition, regular personnel files, such as a record of someone's work history at that employer, can be used as background information. A more controversial internal system is the blacklist. Although a blacklist meant for internal use is allowed by privacy law, it is obligatory to report sector-wide use of this beforehand to the Data Protection Authority (CBP, 2015c).[51] Many respondents indicate that they do not know for sure whether their blacklist meets the criteria, but they do keep a database with information on people who have been investigated or fired in the past.[52] These are often used as reference points in investigations (and in the process of hiring new staff). Finally, the use of (hidden) cameras is not entirely free from controversy. Cameras may provide valuable information, for example when the footage can be used to ascertain which employee took money from the cash register. Although it is allowed to

50 Although this circumstance alone is not sufficient proof, as people tend to use each other's key cards even when this is prohibited by the internal code of the organisation.

51 See article 22 under 2 sub b WBP.

52 This does not necessarily mean that the blacklist does not comply. Many larger organisations have a privacy officer who is better informed on these issues than the respondents mentioned here.

record employee's movements, privacy law prohibits the use of cameras in certain places (such as the restroom). Furthermore, employees should be made aware of the possibility of camera surveillance (CBP, 2015d). "We have many cameras placed in our buildings and people know this, they are made aware of it. When we have for example a missing item at a certain location, we can look at the camera footage and see whether we can find suspicious actions that are not part of the work process" [Respondent 15 – corporate investigator]. Under certain circumstances, the use of covert cameras is allowed, however these rules are pretty strict. Respondents furthermore indicate that the use of covert cameras is the exception rather than the rule.

3.3 Open sources

Much information can be derived from open sources. Many people are lax in the protection of their personal data on the internet. A large proportion of both professional and social life occurs online and for a person who knows where to look, the internet contains much interesting information. In Observation Company 2, the investigations were organised in such a way that some investigators focused on doing 'desk research'. Desk research consists of the investigations of internal systems as discussed above, but also the investigation of open sources. One investigator, especially, was highly skilled in this type of desk research. He for example had several (fictitious) accounts on social media sites so he had easy access to this information. Social network sites such as Facebook and LinkedIn may provide a broad overview of someone's life (e.g. posts, photographs, likes, sites followed) and professional network (which may be useful, for example to see whether a third party that is involved knows the involved employee).

Another open source of information is the database. There are some very valuable openly available or on-subscription databases such as the databases containing information on Chamber of Commerce records, name and address data and domain name registration. Many investigators have a subscription to these databases. Additionally, traditional media and the internet more generally (and search engines more specifically) could also provide a lot of valuable information for investigators.

3.4 Other sources

Depending on the type of norm violation and the circumstances surrounding it, there are multiple additional methods of investigation at the disposal of corporate investigators. Observation, to take an example, may be useful, although most of my respondents did very few observations. Observations (and the use of camera footage) are for example used when an employee is suspected of sick leave fraud. Site visits may also prove useful to see whether the 'reality on paper' matches the 'reality in reality'. "For example, go and take stock for yourself and make sure that that what's in the administration is in fact what's in stock. To determine that, ok, there is a possibility

that the warehouse keeper or someone else took part of the stock" [Respondent 13 – corporate investigator]. Some organisations furthermore do a standard search of employees and their belongings when they leave the workplace.

> We also search people before they leave. We use a metal detector for that as well. Sometimes things come to light during that. You know, situations where people take something that isn't theirs and that the alarm will ring. They're asked to empty their pockets and well, if something's in there that doesn't belong to you, you're going to have a good conversation with me. [Respondent 15 – corporate investigator]

Other activities of corporate investigators include the evaluation (and correction) of previous investigations, the evaluation of internal control systems, the calculation of damages in light of private action and tracing of assets. When a report is made to the police (which often happens only after the internal investigations have been concluded), law enforcement information may also be used to investigate further. However, law enforcement agencies are very careful with the sharing of information[53], as this conversation with two in-house investigators from the Observation Company 2 shows:

> That's the thing. They *think* there's no room but there is. The shutters close on mention of information sharing but that's not necessary. When I report a crime to the police, I would like to have insight in their interrogations etc. They say, 'no, that's impossible because of privacy'. They're so afraid that they go wrong that the solution is not to share anything. We don't need operational details; it would be very helpful if they could just give us directive information without them having to have to start an entire investigation. Just to let us know whether we're on the right track. [Excerpt from observation 2 – informal conversation]

4. The interview: confronting the involved person

A final category of information gathering is that which occurs through personal communications. Usually this takes the shape of an interview with colleagues, managers (serving as witnesses and sources of information) and, finally, the subject of the investigations himself. Respondents highly value the interview as an essential information source. An interview with the involved person usually is the last phase of the investigations, in which (s)he is confronted with the information that has been collected with the use of the methods and sources described above. Interviews with witnesses

53 See chapter 5 for more on public/private relations and information sharing.

often occur at an earlier stage as they are informative (adding to the big picture, instead of confronting someone with it). Many corporate investigators have a law enforcement background and are experienced interviewers. However, there are notable differences between an interview and a police interrogation. For example, there is no formal caution at the start of the interview because the interviewee is not a suspect in the sense of a criminal procedure. However, respondents indicate that they do point out at the start of the interview that the interviewee is not obliged to cooperate and that he cooperates on a voluntary basis. This is also codified in both the Privacy code of conduct (NVb, 2015) and the guidelines for person-oriented investigations (NIVRA/NOvAA, 2010).

> His statement is made freely, I mean if during our conversation he decides he doesn't want to talk about it, ok that's his decision. I'm not sure he's going to be better off with that but when someone walks out the door, he walks. I'm not going to grab him by the neck and say, ok now you're going to talk. [Respondent 15 – corporate investigator]

The voluntary nature of the cooperation of an employee should not be overstated. There is a definite power imbalance between the employee and the investigators (providing a service to the employer).

> The conversation turned to the measure in which people tend to cooperate with investigations done by the in-house department. Investigator [X] stressed that they have no formal powers to make people cooperate and that they are dependent on the voluntary cooperation of people. But, as he continued "you shouldn't overstate the voluntary nature. We are acting as the employer here so people do feel pressure. If someone refuses to cooperate he does so but we do stress that that's not in accordance with being a good employee. That's one of the things that's challenging in an interview. And a lot of people are just scared, that happens everywhere, also at our organisation, people are afraid of management. Afraid that when they talk about them they'll lose their job". [Excerpt from observation 2 – informal conversation]

Investigators stress their independence of investigation within the assignment they receive. "We have our own set of rules on how we conduct our investigations and we give this to our client at the intake of the assignment. Sometimes they say, can't you do this and that. No, sorry. These are the rules; this is how we do things" [Respondent 2 – corporate investigator]. However, this does not mitigate the power imbalance much. An employee is technically free to refuse to cooperate – in practice he or she can feel forced to cooperate with the investigations by his employer. Investigators are aware of this 'limited voluntariness'.

> We caution people at the start of an interview, so to speak, by saying they are not obliged to cooperate. But they feel obliged of course. Sometimes someone asks, what will happen if I don't? Well then I will have to talk to your manager about that. An interview is very confrontational. I dare say we give high priority to fair play, we stick to our own procedures. But we're not treating someone with kid gloves. If someone has done something wrong, it's ok to let him feel that. We are about finding the truth, that can be in someone's advantage. If you did nothing wrong and we're totally off track, here's your chance to fix that. [Respondent 44 – corporate investigator]

As discussed in chapter 2, the law dictates that private investigation firms with a permit implement a privacy code of conduct similar to the one drafted by the NVb and approved by the Data Protection Authority. Other investigators tend to follow these rules as well, either by taking the Privacy code of conduct as guidelines or by drafting their own guidelines according to the Privacy code of conduct. The guidelines for investigations presented in the Privacy code of conduct include for example the right of representation by a lawyer or union representative and the general obligation for the investigators to treat the interviewee with respect and refrain from applying undue pressure and presenting false information (see for example Grant Thornton, 2010). Regarding the question of undue pressure, the Privacy code of conduct (NVb, 2015: 31) states:

> The mere questioning of someone by a private investigator produces a certain amount of pressure. As interviews are done on a voluntary basis, as a rule there will be no undue duress. It is hard to draw the line between what is and what is not allowed. Keen interrogation is in itself legitimate. It is thus allowed to confront someone denying involvement with evidence and to point out his weak position. Undue pressure is exerted, however, when physical pressure is used. Making false promises and verbal abuse are also illegitimate.

As an investigator of Observation Company 2 explained, this is not just a matter of due process: especially when there is not enough evidence to take measures against someone, working relations may be affected by corporate investigators' actions.

> And you need to be careful, when we have a case in which we can't really make it stick, when there's not really enough evidence and the person does not confess, you can't be extremely tough on him. If he continues to be a co-worker you need to be able to shake his hand in the future. At least that's my opinion on the matter. [Excerpt from observation 2 – informal conversation]

Moreover, interviewees are given the opportunity to have a break and are offered something to drink and eat. "As of late we also include this in the interview report, you know, that someone has been treated correctly, had something to drink and had to opportunity to use the bathroom. That's also to have proof of this for a possible court case of course" [Respondent 45 – corporate investigator]. Because "the first thing a lawyer tries to do, also in a police investigation, is to discredit the statement that has been made by the involved person" [Respondent 44 – corporate investigator]. These basic principles are (in a more general manner) also present in the guidelines for person-oriented investigation for accountants. Respondents indicate they are aware of the situation in which an involved person finds himself, especially in an interview setting.

> The complaints that I get I can count on one hand. It used to be mostly about people feeling pressured in interviews. I get that, if you did something wrong and you know it and you're faced with two investigators who start asking you questions and who are trying to get you to admit you did something wrong, that is a stressful situation. I take these complaints very seriously. But usually it's just the context of being investigated, that in itself is intimidating. The conversation in the interview may feel awkward but I haven't found that rules have been broken as of yet. People are treated with respect, they are not held against their will or any of that. So the percentage of complaints is pretty low, usually all runs smoothly. We've started to write down some of the procedural precautions we always took but now it's recorded in the interview report. Things like that we tell people they are there voluntarily, that they are offered a drink and maybe some lunch, that they were able to go to the restroom. And we ask them now at the end of the interview how they feel about the interview. That prevents many complaints. [Respondent 46 – corporate investigator]

The rules and normative considerations guiding investigations more generally and the interview in particular are there to ensure a fair treatment of the interviewee and at the same time guard the quality of the interview, so the information gathered through this method may be used in whatever legal solution chosen in the end (see chapter 4). The rules and principles of law leave room for interpretation – it is possible to stay within the width of the legal framework but still put a fair amount of pressure on the interviewee. It depends in part on the investigator what the stance towards the interviewee is. Some respondents empathise with the interviewee, saying that they can understand the position he is in during an interview. However, most state for example that

> You need to be completely neutral in these things. You didn't contribute to this misery, you're just hired to get a clear picture of the mess and fix it. You need to be

> professional about that. Of course, you need to be friendly. When someone needs a break, you offer him one and you record this in the interview report. 'At that and that time interviewee was very emotional and we took a break'. So you also report what time you continued, you give the man some water, maybe suggest that he takes a walk in the garden. And sometimes, I join them, have a smoke, then some other kind of conversation unfolds. And when he's ready, you reopen the interview. [Respondent 1 – corporate investigator]

Interviews are generally done by two interviewers (see for example NVb, 2015). There are multiple reasons for this. One of these is to have a witness for what has been said during the interview. Furthermore, having two people present is beneficial to the pace of the interview.

> We conduct interviews with two people, one takes care of the conversation, the other takes notes. So, we can write the whole thing up on the spot and print it out and then the interviewee can read it and sign. When there are corrections that need to be made we will adapt the document, print again and sign it. The interviewee signs for having been made aware of the content of the interview report and he gets his own print to take with him. It happens that people don't want to sign because they do not agree or because they want to talk with a lawyer. In that case, we sign it anyway. And sometimes people don't even want to talk to us. [Respondent 44 – corporate investigator]

As the cooperation is voluntary, people may refuse their assistance in an investigation. This could for example mean that he or she does not want to talk to the investigators, or that the interview takes place but the person will not answer relevant questions. Respondents indicate that most people tend to cooperate. In a conversation with an investigator in observation 1, I was told that 'most people are curious; they don't have any experience with this kind of stuff so they come and have a look at what we do and what we know'. After the interview has taken place, the interviewee is asked to sign the interview report with the interviewers. However, the interviewee may refuse to do so. In this case, a note is made at the end of the interview report and in the final report (see also below).

4.1 The interview process

Respondents explain that although an interview is often done in a comparable manner, this is not according to a rigid standard. Different interviewers have different styles and flexibility is an important asset. In addition, the way in which the interview is executed depends on the position of the person who is interviewed within the investigations. Respondents indicate that an interview with a witness is different from

an interview with an involved person. Interviews with witnesses are more informative than confrontational and often happen at an earlier stage. (Self-imposed or legal) rules regarding the interview with a witness are less stringent than when it comes to an interview with an involved person. It is required by privacy law that an involved person is made aware of the investigations he is subject to at the very beginning of investigations (see article 33 and 34 WBP). However, there are some exceptions to this rule, for example for the protection of the rights of others (including the client) (see article 43 WBP). In practice, this means that involved persons are often notified about the investigations at the moment of their interview. Although there are situations "in which you need to talk to the involved person as soon as possible, you often postpone this interview until you know exactly which questions to ask, based on the information you gathered" [Respondent 2 – corporate investigator]. Respondents prefer to interview the involved person at the end of the investigations, since they are able to confront him with the investigations' results by that time. In this way, the chance that the involved person might destroy incriminating evidence is also diminished, as (s)he will only be aware of the investigations at a later point in time. The following quote depicts the procedure respondents follow with regard to notifying involved persons quite nicely:

> In principle, you provide the code of conduct for investigations to the involved person at the earliest occasion you have, unless investigative interests are opposed to this. So in case you have to start your investigations and the involved person is still working there, there's a chance evidence will be lost. For example because he erases all files from his computer or removes physical documents from the administration and throws them in the shredder. That would be a reason not to inform him just yet. You will first have to secure the evidence and only after that, when you know everything is safe, you will notify him. [Respondent 2 – corporate investigator]

The Privacy code of conduct and general principles of law leave room for the use of flexibility in when to inform an involved person about the investigations. Flexibility is generally an important part of an interview. During one of my informal conversations with investigators during observation 1, an investigator talked about how interviews may take a very different turn from what was anticipated by investigators and responding to such a situation in a good way is vital. It is therefore important to stay flexible when conducting an interview. Respondent 5 displays the same opinion when stating:

> Sometimes you decide on a certain tactic for an interview but it turns out very differently. I remember a case where we were expecting this person to be uncooperative and so we decided to start with a confrontation right off the bat. But

> we entered and he was very open and he wanted to talk to us. You start with a certain tactic but just like that it's useless and then you need to converse with someone in a different manner than you expected. And it also depends on the subject matter. Or for example when someone is very emotional. Of course there are parts you can prepare beforehand but when you discover during the conversation that the important stuff is somewhere else you have to let go of your neatly prepared list and move to that subject. So you can come up with a certain grid but in practice it seems that you need to be very flexible with that. [Respondent 5 – corporate investigator]

As this quote shows however, interviewers do apply certain tactics during an interview and they prepare for it (see Coburn, 2006).[54] The level and depth of preparation depends in part on the information that is already available. When the interview is used as a close to the investigations, usually there already is much information and "you can write much down in advance, you can make a draft of the interview report and confront him with it. Then you add his reaction, his declaration" [Respondent 44 – corporate investigator].

4.2 Phases in the interview process

The two investigative interviews that I was able to attend during the observations had a certain structure. Since this structure is also put forward by respondents, it seems to be more commonly used.

> There's always a difference between interviewers, I always say, you need to do your own thing. But the standard elements are that you start with a social talk, an explanation of the context of the interview, his rights and sometimes his duties. So basically what's in our code of investigations. And usually, you move from a general conversation to more specific elements. In this conversation, you need to explain your assignment as well. So, you use a funnel so to speak, as an interview technique. The more specific questions are somewhere in the middle of the conversation. And then you start to show your evidence to the interviewee. There's a turning point in an interview from informative to confrontational. That structure is always there. And these interviews can take a lot of time. [Respondent 1 – corporate investigator][55]

54 There are many (mostly US) textbooks, e-learnings and other professional information available on different approaches and interview techniques. In this section the broader outlines of the interview as a source of information are described – these very detailed instructions on how to interview are beyond the scope of this chapter. Additionally, the fieldwork reveals that many corporate investigators feel that interviewing can be taught but much importance is given to experience and following one's own instincts. Although respondents state that there are no standard ways to interview, stressing the importance of flexibility, they seem to broadly follow the process as delineated in this section.

55 Unsurprisingly, an investigative interview follows some of the same basic rules followed by social scientists when interviewing respondents (Baarda, De Goede & Van der Meer-Middelburg, 1996).

In general, the interviewers seem to build the interview around three phases. The first of these is centred on pleasantries – the interviewers start with light conversation to make the person feel at ease. This includes small talk, for example about a person's job. The voluntary nature of the conversation is stressed in this phase. "I want to tell you that you are here voluntarily, which means that you don't have to cooperate and when you want to leave, you are free to do so. But of course we hope you will cooperate with us" [Excerpt from the interview witnessed during observation 2].

After the interviewee has had the opportunity to talk freely about what he thinks is the reason he is there, the interviewers start with the second phase, 'confrontation'. Here the evidence that has been gathered through other channels is used to confront the interviewee with 'the holes in his story'. The ambiance changes from being amicable to more stern. Although the interviewee is treated with respect, the situation could put pressure on the person even when no boundaries are being crossed.[56] Especially when the employee is alone and without representation, he might feel pressured to talk even though he does not want to. The interviewers are experienced and as mentioned above, respondents indicate that interviews are done in couples, which brings a certain force with it. The situation in which people are placed, and the consequences it may have on their lives, is something investigators tend to take into account in an interview setting as well.

> Let's be honest, we have nothing to hide here. When we have the information to close a case, the adversarial principle dictates that the employee has the right to be heard but they don't *have to* talk, they *may*. And I assume that there are very few people who will actually admit that they did it. But when we have a tight case we can say at that moment, 'look it doesn't matter whether you talk or not, we're done. This is how you did it', if necessary they can see the camera footage and such. No problem, all cards on the table. [But you should also be aware that that person] is often by himself in that interview situation. Because, as an investigator you're not always aware of the impact it has on someone, you know. And taking that into account your mind-set is different as well for an interview. Even if someone did something wrong, he's still a person. And the reasons why people do what they do may be heart-breaking. But the consequences of these actions as well. Because that person will have to go home and explain what happened. Especially with some types of norm violations that can be very painful. So I get it. So we try to interact on a human level, and in the end of the day I need to be able to look myself in the eye about how I acted. And sometimes I think, what a waste that this happened to this person. But that's the way it is. I have done my job in a fair manner. [Respondent 18 – corporate investigator]

56 This research has found no evidence of corporate investigators abusing their power by mistreating the interviewee. This does not mean however, that such a situation never occurs.

The final phase of the interview is the conclusion. At this stage the important information that has been discussed is summarised and either typed up directly, or the notes that the interviewers have taken are checked to make sure they are complete. Most respondents prefer to finish the interview report on the spot.

> When it comes to an involved person, [to type the interview report at a later point in time] may not be the best course of action because then you run the risk he will rethink what he has said. 'I said that but maybe it wasn't wise to do so, so I want it deleted'. When you correct the report directly, print it, let him read it and comment and ask him to sign, this risk is much mitigated. [Respondent 2 – corporate investigator]

Other respondents feel that this is not really an issue and take a different approach.

> We always send the interview to them and tell them to take the time to read it carefully, and tell them, what you send back, that's what you agree to. Then I will edit it and send it again and if you say this is correct, that's what we discussed during the interview. They don't even have to sign it then but we're trying to get the most objective outcome as possible. And if someone says something in the interview but realises later that he should have put it differently, fine. That's his story and that's what's going to end up in the report. So we're trying to be as transparent as possible in the whole process. [Respondent 18 – corporate investigator]

After the interviewee has been confronted with the information gathered during the investigations, the atmosphere seems to change back to amicable. The interviewers and interviewee might discuss what will happen next and other matters, such as the motivation for the transgression, also tend to be referred to. In case the report is typed up on the spot, the interviewee – in accordance with the adversarial principle – gets the opportunity to read it and comment on factual errors. He is then asked to sign the document, along with the interviewers. This is also on voluntary basis – the interviewee is not obliged to sign. "For example, this involved person refused to sign his interview reports. We did sign; these were the statements he made to two witnesses [interviewers]. So if it comes to a trial, we can testify under oath about this" [Respondent 1 – corporate investigator]. If the report is typed up at a later point in time, the interview report is sent to the interviewee to comment upon and sign. A refusal by the interviewee to sign the document is not considered to be overly problematic by respondents. When this occurs, a note is made that the document has been offered to the person to read and sign but that he or she has refused to do so. Generally, this is considered to provide enough information to make the interview report useable (Van Wijk et al., 2002).

The interview reports differ in size but they are often a summary of what has been said instead of a verbatim account. The interview reports available to me during my research were mostly limited to a few pages. This is not a good indicator for the duration of the actual interview – only the relevant parts of the conversation are summarised in the interview report. This means that the interviewers have quite some freedom in drawing up the interview report. However, the interviewee has the opportunity to amend the report when he thinks important parts are missing. Respondents also state that it is possible that the interviewee wants to exclude certain information from the interview report "for example private information that his manager has no business knowing" [Respondent 45 – corporate investigator]. In some cases, investigators may honour the request of the interviewee, when the excluded information is not relevant to the case.

> And when someone wants to change something we don't agree with, we make a note of that and sign that too. Openness, transparency, completeness. Pro and contra. Those are important principles. It rarely happens that an interview report is reproduced in full in the final investigative report but such a comment will be mentioned in the report when relevant – either to support or to defy your conclusions. [Respondent 1 – corporate investigator]

The fieldwork reveals that using the methods of investigation discussed, corporate investigators are often able to provide a fairly complete reconstruction of the norm violation. Using mediation of phones, combined with open sources such as social media, investigators can map who has been in contact with whom, where a third party lives, works, etc. Investigations into financial records and other relevant documents can furthermore provide insight into fraudulent financial transactions. When it comes to for example theft from a shop, cameras and employee log files can be very useful. Although these are all valuable methods and sources of information, respondents tend to place most importance on the interview as a source of detailed information. Usually, the investigations lead up to the interview with the involved person(s). In these interviews, information can be checked, details can be added and errors can be corrected – that is, when the interviewee decides to cooperate. All this information needs to be made available to the client in a concise and clear way. To achieve this, an investigative report is written.

5. Reporting on the investigations

Once the investigations have been concluded and the questions that were the basis for the assignment can be answered, the information has to be made available to the client.[57] Reports are often quite short and to the point, as respondents indicate that this format is most appreciated by their clients. A report needs to be clear on the facts and easy to read (Van Almelo & Schimmel, 2014). Depending on the nature of the assignment and the complexity of the norm violation, reports may be merely two pages (not including appendices) while others may span one hundred and fifty pages. "The size of a report varies between assignments but thirty pages is usually about the length for us. Sometimes they are very factual, and then a lot of appendices might be attached, for example interview reports" [Respondent 36 – corporate investigator]. Some investigators prefer to use appendices, while others do not. For example relevant parts of interview reports or other findings may be integrated in the report without them being attached, or they may be added in an appendix. "These interview reports are for internal use, to build our case. They are not an integral part of the subsequent report. But we do use them to quote from, especially crucial parts" [Respondent 5 – corporate investigator]. Multiple investigations may turn out to be related.[58] Whether or not these are condensed into one report depends on the client. For example, it was explained to me during observation 1 that if a client wants to take different actions against different involved persons, multiple, separate reports for each individual might suit this purpose best. Also, the same case may involve multiple clients, who all receive their own report. Observation Company 1 had multiple investigations which were concluded by more than one report. Observation Company 2 (an in-house investigations unit), however, usually only produced one report. In-house investigators have an internal client and when multiple departments are involved the same report may be circulated.

It is difficult to give a standard format of an investigative report, as there are notable differences in the way the findings are presented. However, most investigative reports contain the following subjects:[59] "a report is typically formatted like, what was the assignment, what was the scope, what did we do and what did we find?" [Respondent 36 – corporate investigator]. Some investigators also add some legal information, a preface with some kind of disclaimer or other relevant information. Opinions seem to differ about

57 Not every investigation yields enough information to answer the questions asked in the assignment. When this is the case, a report is made about the findings and the lack of certainty is stated.

58 For example because other norm violations are discovered within the organisation during the investigations that warrant their own separate investigations (often referred to as 'by-catch') or because business partners of the organisation want to have internal investigations as well to ensure they had nothing to do with the norm violation.

59 There are some standards provided for forensic accountants, but not all corporate investigators use them.

the necessary information for a report, however there is some consensus that a report should at least be transparent about the presented findings and how these have come to the fore. The client needs to be able to make an assessment of the validity of the report and to interpret its findings (Rense, 2004). The reports of the cases examined during observation 1 (case study 1 to 10), contain a justification of the investigative efforts which have led to the findings presented in the report. In this sense the report also serves as a way to show accountability to the client. This 'disclaimer' is typically not part of the reports of the cases analysed during observation 2 (case study 11 to 21). Observation Company 2 being an in-house corporate investigations department, it did not have a commercial relationship with its client, based on an official assignment and contract. As such it is not necessary to provide such a justification in every report.[60] In these case reports, the explanation of the kinds of investigative methods which have been used is done in a less all-embracing manner. For example, although an investigator of Observation Company 2 explained that the investigation of open sources such as social media is a standard part of the investigations, the use of this method is not always mentioned in the case studies (it is excluded when it yields no results). The investigative actions may however still be retraced as they are recorded in the investigative journal (if kept properly).

Interestingly, respondents working in an in-house corporate security department indicate that not every investigation merits a report. In such a case, the case notes, kept in the investigative journal, are simultaneously the final product of the investigations.

> We don't always write a report, we get a lot of rubbish cases. It's no use to write an entire report then. The rule is that when they want to fire someone, we do write a report for the involved business unit, with an advice attached, for example about the processes that made the transgression possible. But when they are just going to give the involved person an official warning, there will be no report. Maybe we'll give some advice but nothing written down. When there is no report, your notes, the journal and our registration system 'is the report'. [Respondent 43 – corporate investigator]

Some commentators suggest that it is necessary to have a predetermined goal for the investigations, for example a report to law enforcement authorities or a dismissal (Schimmel, 2011). When this has been agreed between client and investigator, this predetermined goal is usually presented in the report. However, in practice the decision what to do with the results often is made only after the results are clear. "For example, we hand in the report and the client says, 'I didn't know it was this serious, I want to report to the police after all'. Ok, so then we go and report to the police"

60 As we have seen in chapter 2, investigative costs are also important for in-house departments, however they are usually justified in more general terms (e.g. in a yearly report, calculated over a whole year) and not in every investigation.

[Respondent 1 – corporate investigator]. If the decision to report to law enforcement authorities is made at the end of the investigations, this may potentially provide an issue with the value that will be given to the evidence. The standard of evidence in a civil court procedure is lower than that which is used in criminal court. If a civil court ruling or internal solution is sought but a report to law enforcement authorities is deemed necessary as well, this might thus be an issue. "Improperly obtained evidence is not as problematic for the procedure in civil court. A civil judge will not easily dismiss evidence, he might reprimand you for it but he has heard it anyway and will use it. Plus, often it is not the only evidence you have, you can build your case with the other evidence as well" [Respondent 50 – client]. Cases may also be concluded entirely without the involvement of a judge (Meerts, 2014a), which makes the way evidence is gathered even less of an issue in that sense. It is not necessarily a case of improperly produced evidence though – the information might be gathered through all the right channels and according to all the rules and still not comply with the standard of evidence used in criminal court because it must be considered circumstantial. This might be enough for a civil court solution, termination of the labour contract or internal sanctions but it will not hold up in criminal court.

Taking the above considerations into account, the situation may be less serious than one might expect. Because there always is the possibility that a client decides to report to law enforcement authorities after all, respondents state that they try to aim for the standard of evidence that is used for criminal investigations in all investigations. "You have the highest standards for the burden of proof there, beyond reasonable doubt. If it complies with that, it will comply with the others as well. So this way, these other settlement possibilities will all remain an option" [Respondent 1 – corporate investigator]. As such, respondents indicate that they feel it is important to 'go by the book', both in a moral and professional sense and because in many cases the decision how to handle the matter is made only after the investigations have been concluded and the report is handed in to the client.

Whether or not a conclusion of findings is drawn in the report depends on the type of investigator. For example forensic accountants consider drawing conclusions from the presented facts, or providing advice to their client in a report 'not done' (see also chapter 2)."Clients always ask for a conclusion, 'just write down what you think'. But that would be subjective. The report sticks to the facts. Accountants are not supposed to draw their own conclusions, that's up to the client or a judge" [Respondent 36 – corporate investigator]. Others prefer to give some advice on how to proceed but the extent of this advice also differs among respondents. This respondent for example does include some advice on the possible ways of settlement but provides no opinion on the best solution in the current case:

> Every case is different, the interests involved are different. Every time you're faced with a different web, different tensions. The outcome is different every time. But you know, I don't really care about that. We have a job to do and do it well. You can provide your client with the options but I'm not going to be the one to say, this is the way to go. Who am I to say they should report to the police? [Respondent 1 – corporate investigator]

Corporate investigators with a legal background are more inclined to provide an advice on how to proceed:

> And eventually you will come to the point that you write your report and explain your findings but also draw conclusions based on that. That could be that there must be measures taken against certain persons or that the structure of the organisation should be changed. And it could also lead to the question whether or not the incident should be reported to the police. And that's often a tough one to answer. [Respondent 30 – forensic legal investigator/client]

The extent to which corporate investigators may influence decisions about settlement of the norm violation differs, however respondents indicate that the actual decision is not made by investigators. The client is the one deciding. In in-house security departments, the division between the investigators and the decision makers may get blurry at times. "Whether or not it needs to be reported to the police is a decision that does not concern HR. They want to be in charge of that, but I am the one to decide whether or not I find it useful. The policy is, report every time, in practice it hardly ever happens. I am the one who has to go there and file the report so I am the one deciding" [Respondent 48 – corporate investigator].

> We do the investigations and that's it. Two of my colleagues have a different opinion, [they think that] when they say someone's guilty he should be fired, [but other colleagues] have a more nuanced view. Our job is the investigation, getting the evidence and building a case that would hold up in court if necessary. The decisions lie with the involved manager and HR. [Excerpt from observation 2 – informal conversation]

5.1 The adversarial principle

Before the report is handed over to the client, the involved person will be given the opportunity to read the relevant parts of the report and comment upon it. This implementation of the adversarial principle is derived from accountancy rules, however, most respondents state they comply with this rule even if they do not have

an accountancy background (Rense, 2004). The adversarial principle relates to the more general principle of law of due process, which respondents claim to comply with. For private investigation firms with a Wpbr-permit, the use of the adversarial principle is codified in the Privacy code of conduct as well (NVb, 2015: 7).

> And especially when it concerns an involved person – because it's a person-orientated investigation – we use the adversarial principle. The first phase of that is to invite him to answer some questions. And the second is that when you make a final draft of your report which contains parts that concern that person, you give him the opportunity to react to it. So he can read it and comment on it. And those comments are added to the final report. And I think this is a good thing and very reasonable. I think that's very important, it can't be the case that you just go about your investigations without ever speaking with this person and still write a report about him. Obviously, that's not right. [Respondent 5 – corporate investigator]

Not every involved person takes the opportunity of reading the relevant parts of the report. Respondents indicate that this is not necessarily problematic, however it does mean that caution should be applied when presenting findings. An example from observation 1:

> Three investigators are having a discussion about the adversarial process in [case X]. When possible, relevant parts of the report are send to the involved person. In this case however, it is decided to make the draft report available at the office of Observation Company 1 instead of sending it to the people it concerns. The reason for this is that multiple people who are involved in the case have indicated they are worried about consequences to themselves, should the report be circulated. To limit the chances of this happening, the draft report is not distributed but only available for inspection in the controlled surroundings of the office of Observation Company 1. To comply with the adversarial principle, the draft report is still available for inspection to the involved persons, however it will not be sent to them. The lawyer of one of the involved persons demands the (full) report to be sent. It is decided this will not be done. [Excerpt from observation 1]

This solution is not limited to Observation Company 1. Other respondents indicate they make use of the option to present an opportunity for inspection at their own location as well, instead of sending it to the involved person.

> That draft report is presented to the involved people. It depends on how sensitive the matter is whether that happens by sending it to them or whether we place it

> somewhere where they can come and inspect it. If we have the slightest inkling that they will abuse the content of the report or that they will go public with the draft, they can only inspect it at our location. This is usually followed by a discussion with their lawyer who will state the involved person has the right to inspect the draft report based on the adversarial principle. Yes he does. But he does not have a right to the report itself. He is not our client. So he may take notice of the relevant content of the draft but we do not report to him – we report to our client. That's the way the game is played. Usually they try to slow down the process by refusing to inspect the draft if it's not actually send to them. Then we write to them again, giving them the opportunity to inspect the draft. Usually we give them a reasonable term of 2 to 3 weeks to respond, followed by a reminder and a couple of weeks more. But if they don't respond we will notify them that we assume that they do not want to take the opportunity to read and comment on the report. The suspense builds and in our experience, people will eventually cooperate and inspect the draft. It also depends on the way you communicate with them. Usually they sense the importance of knowing what we wrote about them. So after all that we edit the draft according to their comments. Which may provide another heated discussion when someone says 'I don't want this to be in the report'. Our response to that is: we are deciding about the content, if you don't agree please write it down and we will make sure to attach your comments to the final report. We will present our view on the matter and yours alongside it. Some people write an entire report in response, ok fine we will attach that too. Let the client figure out what he wants to do with it. And then we finalise the report and present it to the client. [Respondent 40 – corporate investigator]

The inspection of the draft report may take a substantial amount of time because involved persons do not respond or try to stall the investigations in a way similar to the one described in the quote above. During observation 1, this issue also occurred for an investigation which was almost finalised by Observation Company 1.

> The assignment of [case X] provided Observation Company 1 with multiple additional assignments because other organisations that had dealt with the involved persons in the past want to know whether they are also affected by the norm violations. [Investigator] is now working on the finalisation of one of these additional reports and I am having a conversation with her about it. "You know what the difficult part is here – we have concluded investigations already which are basically about the same people but for different clients and different norm violations. In those cases we applied the adversarial principle and this particular person referred us to his lawyer. So, theoretically, it would make more sense for me to contact his lawyer now as well. But I can't because it's a different investigation. But the thing is, for this involved person it's

> not a separate matter, he's being investigated, that's it. He's refused all the registered letters we have sent and other communications he just sent back to us. But I will have to send him an invitation to make use of the possibility for inspection for this case as well. And if he does not make use of that that's his problem. We did everything we could to comply with the adversarial principle." [Excerpt from observation 1 – informal conversation]

When the adversarial principle has been applied and the draft is amended, the report can be finalised and signed. The (lead) investigator is the one responsible for investigations and, in case of a commercial relationship with the client, the signature of this investigator is necessary. For investigations done by a private investigation firm, the report is often (also) signed by the director of the firm.

Respondents working for an external client indicate that they agree on the terms under which the report of the investigations may be used. If the client wants to use the report for other purposes than agreed beforehand, the corporate investigators who executed the investigations will have to agree to that.

> In the report we state the purpose for which it may be used. Should the client choose to use it for a different purpose than to which we agreed, he has to get our written consent previous to that usage. We can't enforce that – but at least the statement is there. To cover our risks, make sure clients do not run off with the report and abuse it. Say a client tells us that the report will be used for procedure X but when he gets the report he thinks, 'it suits me well to post in on my website or share the contents with the newspapers'. That means he has an issue with us because he's breaching our contractual agreement. But we can't really stop it from happening in practice. [Respondent 40 – corporate investigator]

The reports which are publicly available through the internet (mostly investigations done for (semi-)public sector organisations) contain a similar disclaimer. This disclaimer usually explains that the report is made for a certain client and meant for the purposes defined in the report and that if the report is made public, written consent is necessary.[61] Because of the laws regulating transparency in public office (*Wet openbaarheid van bestuur* – Wob), this is partly moot though: if for example a municipality receives a request under the Wob-regulations, (relevant parts of) the report needs to be made publicly available (unless one of the grounds for refusal

61 See for example a 2012 report by Grant Thornton for the municipality of Eindhoven (https://eindhoven.raadsinformatie.nl/document/184307/1/Bijlage_5_Grant_Thornton_eindrapport_TA), a 2015 report by Hoffmann for the municipality of Urk (http://www.omroepflevoland.nl/SiteFiles/Doc/Rapport_onderzoek_naar_lek_E48A8C53F9EC9A01C1257DE400371DDF.pdf), a 2012 report by Deloitte for Avalex (http://www.politiekdelft.nl/avalex_rapport_deloitte_20120330.pdf) or (in a more limited way) the 2015 report of De Brauw for NS (https://zoek.officielebekendmakingen.nl/blg-614489.pdf).

applies, article 10 and 11 Wob). However, such a formal addition in the report does protect the corporate investigators against liability claims from people involved when the report is made public without prior consent.

5.2 Complaints procedures

Persons and organisations who feel wronged by corporate investigations or by the final report have recourse to civil court proceedings on the basis of wrongful act/tort (article 6:162 Civil Code [BW]). Corporate investigators may be held liable for damages in this way. When the corporate investigator in question is a forensic accountant or forensic legal investigator, disciplinary procedures are also open to people and organisations affected by corporate investigators' actions (see also chapter 2). Respondents indicate that they are faced with disciplinary action or civil suits on a regular basis, as it is a way for the legal representation of the involved person to discredit the report and in this way remove the grounds for action against the involved person. This goes more generally for the report as "even the slightest detail might be problematic. If they find something that doesn't fit, this can discredit the whole report" [Respondent 3 – corporate investigator]. In this way, control is exerted over corporate investigations and when a transgression has been made, the judge may correct the situation by allowing damages to the aggrieved party.

> At first I got nervous and I would think my god, we're in trouble here. But now I know it's just part of our business. It's a standard defence strategy: if you can't win on content... For example the big investigation we've just finalised, we and the [board of directors] are charged for slander by the people involved. This happens all the time. [Excerpt from observation 1 – informal conversation]

Before taking recourse to a civil or disciplinary court, persons affected by corporate investigations may turn to the complaints procedures of corporate investigation units. For private investigation firms with a Wpbr-permit it is obligatory to have a complaints procedure in place (article 18 *Regeling Particuliere beveiligingsorganisaties en Recherchebureaus* [Rpbr]), however other corporate investigators tend to have a complaints procedure as well.

> When someone has an issue with the investigation or the outcome there are several recourses. For people still employed by the company there is a general complaints arrangement to be used for every decision by the company related to a person. This is not specific for actions by the in-house investigators. These complaints end up with the manager and there is an option to appeal to higher management. There is also an official employee confidant an employee could turn to. When a person has been fired

> that usually goes through court so the employee in question then has the option to complain to the judge. [Excerpt from observation 2]

As this manager of an in-house security department explains, the complaint is usually initially dealt with by the manager of the corporate investigations department or corporate investigation firm.

> I don't get many complaints of people who have been the subject of investigations. Complaints end up with me first and I decide whether they have merit. If people do not agree with the way I handled the matter they can use the official external complaints procedure. As a matter of fact I have one complaint I am looking into right now. That one is about the use of our protocol for investigations and the Privacy code of conduct [CM: respondent is the manager of an in-house security department so the Privacy code of conduct is not legally binding to his investigators but is used nonetheless]. It is a question of proportionality here and they have a point. It's a valid question to ask why we first looked at the emails instead of open sources. If you want to upgrade to more intrusive means of investigation you're going to have to start with the ones which are least intrusive of course. [Respondent 46 – corporate investigator]

Discussion

This chapter shows that corporate investigations into norm violations within organisations may be executed with the aid of multiple sources of information and methods of investigation. These are only partly the same as the ones at the disposal of law enforcement agencies, since corporate investigators lack formal powers of investigation. This circumstance is a defining difference between law enforcement and corporate investigators, making the arguments put forward by pluralisation theories as presented in chapter 1 hard to maintain. Corporate investigators and law enforcement agencies are not interchangeable because of corporate investigators' lack of formal powers of investigation. This seems to be underlined by the avoidance of 'criminal justice terminology' by corporate investigators. As a result of the lack of formal powers of investigation, corporate investigators are not able to perform some investigative tasks; on the other hand, this circumstance also creates much more flexibility in corporate investigations (Williams, 2005). A high degree of discretion and operational flexibility thus defines the process of corporate investigations.

Corporate investigators' *possibilities* of investigation are extensive. The fact that corporate investigators are working directly for a client, being responsive to clients' needs, creates a greater willingness in clients to volunteer information. The

close connection to the client and a contractually-created duty of confidentiality make much information readily available. Furthermore, because of this and the absence of the need to wait for formal approval from for example a judge, corporate investigations can be executed and concluded fairly swiftly. The absence of formal investigative powers may have sparked the creativity of investigators to take a broader approach to investigations and use methods of investigation that may be regarded as more private in nature. The use of forensic accounting techniques, IT-tools and open sources (for a large part digital social networks) does not fall in the category of 'traditional police work' (although, the police are also increasingly making use of these techniques and information sources).

The lack of formal powers of investigation leads to more freedom for corporate investigators. Corporate investigations are regulated by law and self-regulation (although the specificity of the legal framework depends on the type of investigator – see chapter 2). Certain core principles of law are used by all respondents included in this research and by the observation companies as well. Leading normative values are competence and diligence, integrity, objectivity, professional conduct and discretion. Within this, broad principles of law such as subsidiarity, proportionality, fair play and the adversarial principle are central to corporate investigations. However, the fact that the limitations put on corporate investigations present themselves in the shape of (general) principles of law, makes that there is quite some room for a flexible application of said principles. In this way, much responsibility is given to the moral code of corporate investigators themselves (see also the following chapters on non-contractual moral agency by investigators).

One example through which this may be elucidated is that of the relationship with the client on the one hand, and with the people subjected to the investigations on the other. Starting with the latter, there is a power imbalance present in corporate investigators' dealings with subjects. Corporate investigators are professionals and have the backing of an organisation, while subjects are usually individuals (sometimes with the backing of some form of representation) who are not used to the processes of investigation. Respondents seem to be aware of this power imbalance and indicate that they use the guiding principles of law described above (subsidiarity, proportionality, fair play and the adversarial principle) to ensure a fair treatment of the involved person. The procedures codified in the Privacy code of conduct and the guidelines for person-oriented investigations, followed by most respondents, are meant to protect subjects. In addition, subjects may use complaints procedures and recourse to civil and disciplinary court is available to them to ensure their rights. This, however, does depend on the resilience and pro-activeness of individual subjects.

Corporate security cannot force people to cooperate,[62] nor is it allowed to, for example, enter and search private premises. This means that much relies on voluntary cooperation by involved persons and others within or external to the client organisation. Respondents indicate that many people do cooperate, which circumstance some contribute to the fact that corporate investigators appear to be less threatening than law enforcement professionals to people involved in investigations. However, the next chapter discusses the types of corporate settlements which may follow corporate investigations and which may have a serious impact on people's lives. The voluntary nature of such cooperation should not be overstated. Subjects have a labour relationship with the client and cooperation with the investigations may be demanded through that channel.

Corporate investigators must strike a balance between the interests of the subjects, the wider interests involved and the interests of the client. The latter are leading, this being contractually defined by the assignment. This is one of the main reasons for organisations to hire corporate investigators (Meerts, 2014b). However, corporate investigator respondents stress the importance of independence within the limits of the assignment, and are wary for too much involvement in and influence over investigations by the client. Once the investigations are finalised and the report submitted to the client, clients are the owner of the product (the report) and, as such, are responsible for its further use. Corporate investigators may assist in that by providing advice and assistance with a report to law enforcement authorities or corporate settlements. Chapter 4 discusses these various solutions following corporate investigations into internal norm violations.

62 Neither are the police of course, although they do have the power to summon documents, enter buildings without consent (when this is approved by a prosecutor or judge), etc.

Chapter 4

Corporate settlements

Solutions to norm violations constituted by criminal justice, private action, labour law and internal regulations

Introduction

As a result of the investigations described in the previous chapter, a decision needs to be made about how to deal with the norm violation identified through the investigations (if any). This chapter describes such solutions as put forward by respondents. Although reporting a norm violation to the law enforcement authorities is a possibility in the case that a criminal offence has been committed, most solutions are more privately focused (Williams, 2014: 67). The different settlement solutions presented in this chapter relate to different parts of the Dutch legal system and show the unique position of corporate investigators (Williams, 2005). As discussed in chapter 2 of this book, corporate investigators move in multiple regulatory contexts and legal frameworks, which creates room for forum shopping. The interdisciplinary character of the sector reveals itself also in the context of jurisdiction: corporate security constitutes a commercial sector (regulated by private law), offering a product that may have an outcome either relating to public law (criminal proceedings), private law (contract or tort), labour law (labour relations) or internal regulations.

In this chapter the solutions are identified as what I have previously termed 'private settlements' (Meerts, 2013). As will be discussed below, not all settlements are (completely) private in nature. There is a 'degree of publicness' in them, which may be defined as a scale moving from public to private (ibid.). Figure 3 below shows a schematic representation of the most commonly used settlements. What these solutions have in common is that they are (often) the result of corporate investigations and are chosen by the client organisation of corporate security. For this reason, this book refers to these solutions not as *private* settlements but as *corporate* settlements. A key feature of corporate settlements is thus that they are a result of corporate decision-making within the context of organisations (as a reaction to internal norm violations). Corporate investigators are involved in this process, though the extent to which they are involved differs from case to case and from investigator to investigator. As discussed in chapter 2, some investigators are focused solely on the investigations and reporting on factual matters (mostly forensic accountants), while others also include advice and assistance with settlements in their services. Generally speaking, the decision on which kind of corporate settlement will be used in a specific case is not taken by corporate investigators: that responsibility lies with management, HR or specific employee committees.

There are instances in which organisations are not provided with the choice to file an official report to law enforcement authorities. One category of norm violations which cannot be reported to the criminal justice system is formed by those norm violations which are not defined as criminal in the Criminal Code. These behaviours fall outside the jurisdiction of the criminal justice system. In addition,

there is a category of cases in which the authorities are already involved, prior to any conscious decision by the organisation. Cases that start with criminal investigations and in which corporate investigations are initiated only after the organisation has been informed by law enforcement authorities, are an example of this (such as is the case in case study 1 and 11, see the next chapter for more details). A report to law enforcement authorities is a logical outcome here, as these authorities have initiated the investigations and criminal charges are likely. Although not necessary *per se* (law enforcement authorities are already investigating *ex officio*), a report to the authorities is used in such a situation to provide the authorities with additional information, and as a reputation management tool as well (see below for more on this strategic behaviour). An official report to law enforcement authorities does not exclude other types of corporate settlements though, as multiple settlements may be chosen alongside each other in a single case. An organisation may for example choose to report a crime to the police, dismiss the person and launch a civil claim for damages based on private law.

The options presented in this chapter are reactions to a situation in which an involved person can be identified. However, it is also possible that the investigations do not provide any (definite) answers to this question. When there are serious suspicions against someone but no compelling evidence is found, actions are often still taken. A person might for example be removed from a sensitive position or access to certain internal data might be blocked. Still, sometimes the investigations do not provide even a vague suspicion that would merit such actions, in which case no further actions are taken against individuals. "There are of course cases that don't have any consequences for employees because you might have a hunch but you're just not positive about what happened. Those are the trickiest, when you know there has to be internal involvement but you can't find who did it" [Respondent 14 – corporate investigator]. The investigations might lead to changes in the organisation more generally, for example more stringent procedures. Even when investigations result in a clear depiction of norm violations, the organisation may not act upon the information. For example, this situation was mentioned in an informal conversation with one of the investigators of Observation Company 1:

> They'll probably won't do anything with it, which makes sense. CM: why? Investigator: because they can't. To go after him in civil court would be somewhat useless, they can't get the money back. The work was authorised by someone in the organisation so the only thing they can do is sue the person for giving unauthorised permission. But that person doesn't work there anymore, otherwise it would have meant that he'd be fired. And if they go public, the person who should have gotten the contract for the

> work will want compensation. So it'll only cost more money. But they wanted to know what was going on so they're satisfied with the results of the investigations. [Excerpt from observation 1 – informal conversation]

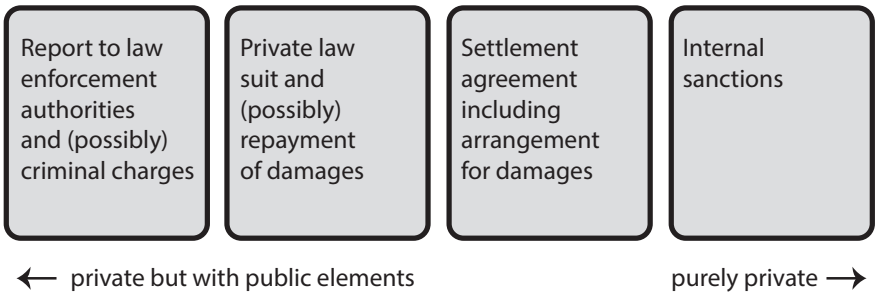
Sometimes the person has already resigned and there is not much hope of reclaiming damages so the case may end with the corporate investigators' report of the investigations. "It might be that an organisation feels, ok he has resigned on his own, so we don't have to go through a dismissal procedure. Claiming damages – there's nothing to get there so we won't get anything from him. Just leave it" [Respondent 2 – corporate investigator]. Though there are situations in which 'no action is the best action', respondents indicate that generally, the organisation will react in one way or another, at least by improving internal procedures.

> Usually, doing nothing is not an option. That's my fall-back position in these kinds of situations. On one side of the spectrum you have the option to solve it entirely internally. So think of measures to prevent this happening again. And I always say, doing nothing is not an option because once you are aware of an internal issue and you *don't* act and it *does* happen again, that will make you liable based on article 51 of the Criminal Code [as being responsible for *de facto* committing the offence by not acting to prevent it]. So you really have to be careful there. But it may happen that an organisation wants to just solve the situation internally, for example by creating a new code of conduct and implementing that. It may also be that they want to involve their auditing accountant so then these measures which are taken to improve procedure have to be coordinated with the accountant. So you can choose how many people you involve. [Respondent 30 – forensic legal investigator/client]

When there is enough information available to take measures against individuals and there are no considerations opposing action, broadly four categories of possible consequences that follow a corporate investigation may be identified. These break down into criminal justice solutions (criminal justice), a resort to civil court (private law proceedings), settlement agreements (contract law) and internal solutions (internal regulations). The fieldwork shows that one major first decision point is whether or not to report the matter to the police.[63] Below, the considerations for and against reporting to law enforcement authorities are discussed, after which more private forms of corporate settlement are considered.

63 This is, of course, only an option if the behaviour may be defined as criminal.

Figure 3. Corporate settlement solutions following corporate investigations[64]



1. To report or to not report, that's the question

There is no guideline or any directive from above with regard to the decision whether or not to report a case to the police, the decision is made on a case-by-case basis. A report to the police is not very common. There are several reasons for that. First, as you'll probably know by now, the police don't give such cases priority so they will almost never investigate. Secondly, we have noticed that if it does come to a court case, judges often will dismiss the case or apply no sanction as they see the dismissal as punishment enough. Thirdly, it takes a lot of time to report a case to the police, especially when it comes to specialist knowledge from within our organisation. It is difficult to make lay people understand what happened. Reputation can play a role, but the organisation isn't very much bothered about that. As I said before, we are a reflection of society and rotten apples are found in society so they are also found in our organisation. When a report is made to the police, it hardly ever happens that we report to the police at the moment we get a case. Usually we investigate and see what has happened before the decision is made whether or not to report. Sometimes, for example in a case like [case study 11], law enforcement is already in. FIOD [the investigative service of the Dutch tax authority] brought the case to us. Then we may report during the process as the injured party. In [case study 13] it was decided to report because we found that there was a criminal organisation involved. It had happened before, in other organisations: two temps are placed in the financial administration department of an organisation as Trojan horses and at a certain point in time these persons start to falsify invoices. These are then paid to shell companies 'owned' by straw men. We wanted to prevent that they carried on with their activities and victimise other firms, so we reported the case to the police. [CM: the police did not investigate] [Excerpt from observation 2 – informal conversation]

64 This schematic is an adaptation of one published in Meerts (2013: 4).

After the investigations have been concluded, the first decision a client has to make is whether or not to report a (criminal) norm violation to law enforcement. Law enforcement authorities may be (formally) involved in a number of ways. As stated above, some cases start with criminal justice investigations. As a result of information provided by previous criminal investigations, media coverage, whistle-blowers or information from regulatory agencies, law enforcement agencies may initiate investigations into internal norm violations without the organisation that is involved having previous knowledge about this. This knowledge may come only when law enforcement auhtorities make a request for information, arrest employees or conduct a raid.

> In that big case we did recently there have been multiple raids by the police. The people in charge of the company had no idea. So they came to us, 'there has been a raid, apparently we have a fraud problem but we are completely in the dark about specifics, so please investigate'. [Respondent 5 – corporate investigator]

Corporate investigators are often called in to investigate further. The information flow from law enforcement to the organisation is often very limited during criminal investigations. The corporate investigations are then meant to provide the organisation with information – usually law enforcement authorities will only inform the organisation after the criminal investigations have been concluded (which may take a long time).

When law enforcement agencies are already involved prior to corporate investigations, the process of investigation as described in the previous chapter is also influenced. In these cases, corporate investigators try to adapt their investigative activities to the criminal investigations. "When the police or FIOD are involved you have to wait to take action because otherwise you'll disturb their investigative process" [Respondent 43 – corporate investigator]. This may for example mean that certain people are not interviewed just yet or that a dismissal is postponed. Respondents indicate that in these cases in which law enforcement agencies are already involved, they often make an official report to law enforcement authorities during the investigations, as this allows them to hand over information without the risk of breaking (privacy) laws. Chapter 5 discusses public/private relationships and information sharing in more detail. At this point, it is important to note that although the corporate investigations form independent investigations, ending in a report to the client, in the specific situation of law enforcement involvement prior to the corporate investigations, the autonomy of corporate investigators is rather limited. The question whether or not to involve criminal justice authorities is not relevant is such a case and during investigations, law enforcement authorities may influence the process by asking for specific information. The centre of gravity in such situations lies

with the criminal justice procedure: respondents indicate that they try not to hamper criminal justice proceedings with their investigative actions.[65]

Many cases, however, start without the initial involvement of law enforcement agencies. Here, organisations and corporate investigators retain the autonomy to decide whether or not to make an official report and mobilise law enforcement authorities. As we have seen chapter 3, many organisations prefer to conduct internal investigations before such a decision is made. One reason for this is that it is not always clear from the beginning whether or not the norm violation may be defined as criminal in the sense of the Criminal Code (Klerks & Scholtes, 2001). The decision whether or not to involve law enforcement authorities is commonly made only after corporate investigations have been concluded. Below, (strategic and normative) considerations which may induce organisations to report are discussed (section 1.2). Section 1.1 focuses first on considerations organisations may have to avoid reporting to the authorities.

1.1 Considerations against reporting to the authorities

> In the report, Observation Company 1 mentions the option of a report to the police. The advice was not to report to the police. The report does conclude that the actions can be qualified as criminal in the sense of the Criminal Code. The reasons given to substantiate the advice not to report in this case are that the chances the case will eventually reach criminal court are slim; that the criminal justice system can take a lot of time even in the decision whether or not to proceed with the matter, leaving everyone involved in a situation of doubt and uncertainty; and finally, that there is a real possibility of publicity, which can harm the persons involved as well as the organisation. [Observation 1 - investigations report of case study 5]

It is a well-researched phenomenon that organisations do not report many (criminally definable) norm violations against them to law enforcement authorities (cf. Steenhuis, 2011; Gill, 2013; Gill & Hart, 1997, 1999; Hoogenboom, 1988; TNS Nipo/WODC, 2011). Research by PricewaterhouseCoopers for example reveals that in cases with employee involvement, in 24% (for traditional crimes) and 42% (for cyber-crimes) of the cases a report is made to the police (PwC, 2014). Another interesting outcome of this research is that merely 9% of cases (of economic crime) are revealed by investigative endeavours of law enforcement authorities. It therefore seems a plausible conclusion that most cases of internal crime[66] within organisations do not reach public law enforcement.

65 See chapter 5.

66 The word crime is used here, as only crimes can be investigated by law enforcement agencies. However, the work of corporate security investigators is much broader and also involves non-criminal norm violations.

There are multiple reasons for this circumstance and this section focuses on the most prominent ones.

One reason to prefer a private solution over a report to law enforcement is that while law enforcement agencies are bound to the definitions as described in the Criminal Code, corporate security is not. Even if investigated, non-criminal norm violations will not be prosecuted. Corporate sanctions may follow corporate investigations regardless of whether or not the norm violation may be defined as criminal (Williams, 2005). This flexible way of framing norm violations has multiple benefits for organisations. It opens the door to the investigation and settlement of a much wider category of norm violations: for something to be problematic or harmful to an organisation, it should not necessarily be criminal.

> The things we investigate are cases with an internal component and they are linked to either criminal behaviour or integrity breaches. You could say criminal is what is defined as such in the Criminal Code and integrity breaches are defined in our code of conduct. There are crossovers off course, for example our internal guidelines. Business principles. [Respondent 10 – corporate investigator]

In cases of breach of internal guidelines or other codes of conduct, often a report to law enforcement authorities is not an option as the behaviour cannot be defined along the lines of the Criminal Code. Additionally, in many cases, it remains unclear for a long time whether or not the behaviour can indeed be defined as criminal. For this reason, many organisations prefer to conduct corporate investigations to start with. In some cases it remains questionable whether the norm violation is 'criminal' or 'merely wrong' even after corporate investigations are concluded. "Let's take theft as an example. It starts with a missing item. But that doesn't mean that this item has been stolen. If we immediately go to the police and we have to tell them later on, never mind we found it – that doesn't really reflect well on us does it? And that might mean that next time you report something they won't take you seriously" [Respondent 15 – corporate investigator]. In such cases, reporting might backfire. Contrary to this narrow approach of law enforcement agencies towards criminal behaviour, corporate security investigators are broader in their approach.

> The forensic instruments are not just there for a quest for the truth in criminal cases. Our society has become so complicated that there are also norm violations outside criminal justice that need forensic expertise and forensic surety and truth seeking have become quite important there as well. [Respondent 26 – corporate investigator]

Conversely, not being bound to criminal justice definitions of behaviour also leaves (more) room to decide whether or not certain behaviour is (investigated and) acted

upon. This is an important asset for an organisation, as there might have been involvement from the side of the organisation in the wrong-doing. "Once the police are in, they often come across additional matters that might not be directly related to the matter at hand. Usually it's not just one isolated incident. We come across these things as well" [Respondent 1 – corporate investigator]. Corporate investigator respondents indicate that they do report about these additional findings to their client but that it is up to the client what happens with this information. When law enforcement agencies are conducting an investigation, there is a substantial risk that this by-catch is also criminally prosecuted. Respondents do stress that they pride themselves on their independence in investigations. Some even indicate that they turn down an assignment when they feel that they are not able to investigate independently (see also chapter 3).

> I feel pretty strongly about this, when you feel you can't conduct your investigations in an independent and professional manner, you have to give the assignment back. So if a client or a lawyer obstructs our investigations in such a way that I will not be able to responsibly put my signature at the bottom of the report, that it will tarnish our good name as investigators, well then I think you should cease your investigations. [Respondent 13 – corporate investigator]

The fact remains, however, that even when investigations are done independently and norm violations of the organisation are included in the report, the client may decide not to act upon that part of the corporate investigations report. Respondents indicate that while (punitive) sanctions often fall upon individuals, organisations commonly take action with regard to the adaptation of procedures as well as a result of the corporate investigations report. In this way, the organisation is able to correct the situation without being punished or held liable in criminal or civil court.

A second, related, advantage for an organisation of a private solution is the control corporate investigations and solutions provide over information (discretion) but also over the investigative process (see also chapter 3) (Williams, 2005). Reputation is often mentioned as an important reason to keep things private (e.g. Aon, 2017; Perry & De Fontnouvelle, 2005). "Reputation is an important issue, off course – do you really want to air your dirty laundry in public? Rather not" [Respondent 19 – corporate investigator]. Similarly, Blonk, Haen, De Lannoy-Walenkamp & Van Gelder (2017: 64) give the advice to organisations to "carefully weigh the consequences of reporting or not reporting beforehand. Here we for example think of a situation in which the media pays attention to the case. It is not always desirable to have the name of the organisation used in such a context". Interestingly, although reputation is often mentioned as being part of the equation, respondents state it is not always a decisive

factor (see also below). "You know I often say, we have about 3000 employees, just take a random village with 3000 inhabitants – things happen. It's the same in a company such as ours" [Respondent 15 – corporate investigator].

> People often say 'It shouldn't come out because that's bad press' but look it can happen to anyone. It happens. But just say, 'this is bad, it shouldn't have happened, we gave the orders to look into it and to figure out how we can prevent it in future. We've learned from it and we've held the person responsible liable, through private law or criminal law or whatever. We've done everything you may expect from us in these circumstances'. Hiding behind lawyers will only make the damage far worse when it comes out in the end. 'If we report to the police we'll have to face open court'. So? So be it. And we say, we have plenty cases to which no one takes any notice. And even if they do, fine. You can say: it happened and we've dealt with it. [Respondent 13 – corporate investigator]

In addition to the control over information flow and the possibility to manage the reputational damage that might occur, the control over the *process* is also a consideration for organisations.

> You lose control. You don't know how long it will take, what they're going to investigate. They might say ok we've looked at it but by the way we also found something else and we're investigating that too. It might back-fire on you. So the criminal justice part is the least interesting solution for organisations. [Respondent 27 – corporate investigator]

Respondents furthermore suggest that any action an organisation may want to take to solve the internal problem may have to wait until the criminal justice procedure has come to an end.

> After a report to the police, you lose control over the matter. It might be a very simple case but it could easily take a year and a half to reach a court and all the while you have to deal with someone who is just a suspect, not someone who has been convicted. So it is very difficult for you as an organisation to take action against him. [Respondent 18 – corporate investigator]

The loss of control over the situation may also prove problematic in the sense that the prosecutor may decide not to prosecute a matter which has much impact on the organisation in question.[67] While the norm violation may be minor in the eyes of

67 Many instances of white-collar crime are settled out of court by prosecutors (see Beckers, 2017).

the authorities – thus making it a low priority – the impact on the organisation may be significant. Public sector organisations, for example, place high value in public trust. A minor norm violation may do much damage to the organisation. In addition to the impact of the violation itself, a criminal justice procedure also has much impact (through reputational damage, loss of control and lengthy investigations and criminal procedures). In the Netherlands, public sector organisations are obliged to report (most) crimes committed by public officials (article 162 of the Criminal Code). However, because of the impact of (often lengthy and complicated) police investigations, in practice public sector organisations often opt for private investigations, just as commercial organisations do (Kolthoff, 2015: 165).

A third important asset of corporate investigations and corporate settlements is what Williams (2005) calls 'legal flexibility'. Because corporate investigations are not bound to the criminal definitions of behaviour, the settlements that may be chosen go well beyond the criminal justice system (for more on this see below). Schaap (2008) poses that organisations are much more interested in repairing the damage done, than in retribution. To define a norm violation as criminal might not be in the best interest of an organisation, since the criminal justice system is not seen as providing an adequate solution for the problem at hand.

> It's not practical to report every one of these cases as there is no added value in that for us. About a year ago we had a big fraud case – in such circumstances you are going to have to decide whether or not to report. So will you report and never get your money back – or with a lot of effort and costs. Or you can choose not to report and he will hand over the money. Well if you can cash five million in this way, the company will probably choose that road. [Respondent 19 – corporate investigator]

A connected issue is the possibility of negative effects of a report to the authorities (NOS, 2016). This is connected to the loss of control mentioned above, since negative effects cannot be mitigated by corporate investigators or clients when they have no control over the situation.

> So reporting to the police means a loss of control. This means that your production processes are probably going to be interrupted, because, say they arrest the guy and think 'we need more information', they'll just come and take it. Even if you are the one reporting. And they might think, 'great that you reported this but we feel that there might also be a suspicion against the organisation here'. So, they come and take your books, interrupt your production process, you have no clue what the result of the criminal investigations is going to be, it might back-fire on the organisation or management, you will get bad publicity... It's not the case that the prosecution office

> reports every investigation to the papers but there are cases in which they do want publicity. And they are in charge, the best you can do is try to exert some influence by consulting with them. [Respondent 28 – forensic legal investigator/client]

Reputational issues have been mentioned above but there are also other negative effects of a report to law enforcement authorities. It might for example influence the chances of an organisation to reclaim damages. "It might mean that other parties will get knowledge about the fraud and they might also want their damages repaid. The more plaintiffs, the smaller your chances to get your damages repaid in full" [Respondent 2 – corporate investigator]. Additionally, a report to law enforcement authorities takes many hours in manpower and thus money. The services of law enforcement agencies may not be charged to the organisation, they are far from cheap according to respondents. "A big disadvantage is the time it takes to report something. And even more so when nothing happens with the report" [Respondent 16 – corporate investigator]. Both corporate security respondents and clients furthermore feel that law enforcement agencies do not respond with adequate actions to reports from organisations (Gill, 2013; Rovers & De Vries Robbé, 2005). It takes a lot of time for a case to move from an investigation to a conviction and in many cases it might never reach the court. During that time, the organisation often has to wait to take other action (unless this has been dealt with prior to the report).

> Say you have an employee who has stolen a phone or something. Someone saw, he is confronted, he confesses. He will be suspended, two weeks later the labour agreement is dissolved, done. Now look at the other side, what if we would go to the police with this? Fourteen, fifteen months waiting for nothing? He'll be at home, we'll have to pay him every month and wait until he'll be convicted? Then the question is will he appeal or not. If he does, that's another few months at home for him. Well, take that, combined with the non-communication from the police and justice department… [Respondent 18 – corporate investigator]

A report to law enforcement authorities is therefore not a very efficient solution to the problem at hand. "A procedure to get the labour contract dissolved takes 8 weeks, the criminal procedure will not be concluded by a long shot by then. If your goal is reached by using labour law, there's no added value in a criminal procedure" [Respondent 50 – client].

> When there's a way to get through an investigation relatively quickly and settle the matter at once, that's what an organisation will choose to do over a report to the police. And that's also because – I have been a policeman myself and it's in my blood,

> but it sometimes concerns me that the reaction to a report to the police seems to be more like a policy of discouragement than that they'll actually try to help. Often people expect a lot from a report to the police, they think ok I have reported a crime, everything's going to be ok now. And then absolutely nothing happens. [Respondent 18 – corporate investigator]

As a 'solution', a report to law enforcement authorities is not seen as being very helpful by respondents.

> Ok so there's your report to the police. Three months later it will be discussed in a meeting and then they will prioritise and then they'll make a plan and then they'll have to make some room in man-hours. So about six months later they'll start looking at it. That's not really making much progress is it? And I've represented some victims, don't think that you as a victim will be very happy with what they do with your case. They're on your side? No they're not. So I always say, please don't get your hopes up. The problem-solving abilities of the criminal justice system are very, very limited. [Respondent 28 – forensic legal investigator/client]

This low confidence in law enforcement is often mentioned by respondents. They feel that law enforcement is poorly equipped to respond efficiently to reports made by organisations after corporate investigations, and state that often the case is not investigated at all or is dismissed by the prosecutor as not being a priority (Blonk et al., 2017). "Financial administrative expertise is scarce within the police organisation and the expertise they do have is mostly used for the big cases, organised crime, drugs... So when you come to report a fraud, they don't exactly rejoice. Which makes things difficult of course" [Respondent 2 – corporate investigator].

> If you go to the police with such a case, they look at you as to say, don't you have anything better for us? I mean, petty theft, that will be dismissed or maybe they get a minor fine or something. And the involved person would have lost his job already so that's a punishment in itself. If you go the criminal justice system then and make a case out of it, that's useless. The judge will say ok he's been fired and he'll just get a symbolic sentence. What's the use of that? [Respondent 15 – corporate investigator]

An additional complaint of organisations faced with norm violations is that, within the criminal justice system, only parts of the norm violations are investigated. A criminal justice investigation and a possible conviction as a result of that may be limited only to some specific norm violations, while the problem for the organisation may be far more widespread. Police and prosecution often only investigate what

they need for a conviction, while the organisation needs the complete picture to take internal measures, dismiss the person and/or reclaim damages.

> And after all that, the criminal court will decide whether or not a criminal act has been committed and if the judge is convinced this is the case, he will sentence the suspect. And then the public enforcement machine has done its job. The law has been enforced. And whether all those things the employee did were investigated in detail is not really important in that perspective. [Respondent 3 – corporate investigator]

A report to law enforcement authorities is thus hardly ever the only action taken according to respondents. Much more than an independent measure, a report to law enforcement authorities is often seen as being an addition to private measures. Interesting in this light is the '*optimum remedium*' argument that may be found in many (legal and professional) writings (see e.g. Blonk et al., 2017; Minister of security and justice, 2016). The idea here is that criminal law has moved away from being an *ultimum remedium* (criminal law is used as a 'last resort') to being an *optimum remedium* (criminal law is used as an efficient way to react to a (criminal) problem). In section 1.2 reasons for reporting to law enforcement agencies are discussed and it may very well be that in a specific case the *optimum remedium* argument is the reason for reporting. It is important to keep in mind though, that a report to law enforcement agencies is usually seen as an addition to the private solutions provided through corporate settlements.

> A company that is faced with such a problem has certain considerations. It wants, first and foremost, to make right in a private law sense: when there are damages, these must be compensated. Related to labour law, they have another issue on their hands because if someone has behaved badly, they want to get rid of him. And finally, there are the criminal justice considerations: the common good demands this to be prosecuted in criminal court, so we will report to the police. But the criminal justice consideration is not top priority, it's the least interesting one for companies. [Respondent 27 – corporate investigator]

In short, organisations seem to be mostly concerned with finding an efficient solution, preferably with the reclamation of damages suffered. "It's just not efficient for an employer to report to the police. They don't even always reclaim damages [through civil court]. Apparently it's just not worth it compared to the effort it takes. Let alone that they take the trouble to report in those cases" [Respondent 50 – client]. "And especially when you're not really hurt by the norm violation as an organisation, it's not in my best interest to crucify someone. My problem is solved. Done" [Respondent 19 – corporate investigator]. Interestingly, protecting the (former) employee seems

to be one of the considerations not to report to law enforcement authorities. When someone with a good employee record transgresses once, some employers feel the dismissal is punishment enough.

> Ok, say you're an employee here. And I think, something's off with her expenses. You may have made some claims of expenses in the past which haven't been entirely by the book. The moment I decide – without prior internal investigations, it is a possibility – to go to the police and report, that's quite some way off. Because I will damage you with that. Even if it turns out that there's nothing there, maybe the rules were just interpreted differently or you've made a mistake – you will still have been damaged. That's quite something. And additionally, I lose control over the situation, they might go and search your house, they might dig into your past, etc. And I won't know any of that. So that might be disproportional to the situation. [Respondent 27 – corporate investigator]

The abovementioned considerations combine to create considerable reluctance towards reporting a case to law enforcement agencies. Some respondents indicate that even when private investigations are not an option for the organisation, for example because of the expenses involved, many cases will still not be reported.

> I think that when they handle the matter privately, it's something that will not be reported very quickly anyway. You know, if they hadn't hired a corporate investigator. That wouldn't end up with the police anyway because that's just something they don't want. [Respondent 3 – corporate investigator]

1.2 Considerations in favour of reporting to the authorities

There are many reasons for organisations *not* to report a norm violation to public law enforcement agencies, however respondents also indicate that there are reasons to report. Especially large and (semi-)public organisations often have a policy of reporting criminal norm violations to law enforcement authorities. However, this does not necessarily mean that they do so in practice. "Formally, our position is that we report to the police but often we don't. There is a reputational issue involved here and especially when it comes to minor cases, you just fire the guy. It's not worth it to report that" [Respondent 19 – corporate investigator]. Although some organisations thus have a policy to report every crime, usually a decision is made on an *ad hoc* basis. This in-house corporate security respondent lists some considerations which might lead to a report to law enforcement.

> Considerations are, well first of all our self-interest as an organisation. That also means that without a formal report you won't get anything done from the police. And secondly, the claim of damages but also the use of formal powers of investigation, we have no access to that. Or certain information sources and paying damages to clients always requires a report to the police, you need to be transparent. [Respondent 10 – corporate investigator]

Respondents seem divided about whether or not to report to law enforcement authorities. However, the overall picture that arises from the interviews is that respondents do not expect a report to law enforcement authorities to provide a solution to the problems at hand. It is often used as an additional measure, either for strategic or pragmatic reasons, or as a result of moral considerations.

> If you report, there has to be a combination of measures, just a report to the police does not make much sense. A report is not a solution, you also need a private law remedy or a settlement agreement. A report to the police is never the ultimate solution for an employer, you're going to have to act yourself as well. A criminal case does not fire the person. [Respondent 50 – client]

The above-cited respondent refers to the practical situation in which an employer needs to use a corporate settlement to dissolve the labour agreement and might additionally report the norm violation to law enforcement authorities. This additional action of reporting to the authorities may also be done as a result of moral sensibilities.

> It is possible to settle privately but still combine it with a report to the police. Because they feel it's so reprehensible that they can't accept it and want to make an example. Also towards the employees, show how you handle internal fraud by reporting to the police. As a warning, use the possible preventative power of that. [Respondent 20 – corporate investigator]

On the whole, respondents seem less concerned with reputational damage than one would expect from literature sources (see for example Klerks & Scholtes, 2001; Jennen & Biemond, 2009, Coburn, 2006). Reputational damage might be a consideration when deciding to report the norm violation to law enforcement (as discussed above) but most respondents do not consider it a crucial reason, preventing them from reporting. According to this respondent there has been a shift in this regard as "before, there was a reflex in the corporate world to keep everything inside. But in the board rooms I frequent now you see the discussion happening that it's actually good to go public. To show, things do go wrong but when that happens we are right on it. We are handling it" [Respondent 30 – forensic legal investigator/client].

> I always say, an organisation is a collection of people and mistakes will be made, it's about human actions. The most important thing is that you stand for what you do and that you are transparent in doing so. And that you own up to things that go wrong and say ok this was bad, we take our responsibility and we're going to fix it. You see, sweeping things under the rug will not help you in the long term. So we're not going to advice our clients to do so. [Respondent 27 – corporate investigator]

Most cases corporate investigators deal with are minor and the reputational impact of it reaching the public realm will be limited. A report to the authorities might not get much attention in these cases, remaining unnoticed by journalists and/or the wider public.

> Theft and fraud, it happens. And whether it's here or at a competitor, we all have to deal with it at some point. My colleagues from other companies say the same. That's no breaking news. And I don't reach the six 'o clock news with a report to the police, nor with a court case, believe me. [Respondent 15 – corporate investigator]

However, some big scandals are dangerous to the organisation's existence and respondents' views on how to handle this differ. Most state that when it is likely that a norm violation will get publicity, reporting to law enforcement authorities is the wisest course of action. "[Reporting] is inevitable once something has reached the papers, then you just go and report to the police. Otherwise you appear to be covering stuff up or to be an accessory to the norm violation" [Respondent 27 – corporate investigator]. "You know, the [a large scandal] is also out in the open, speaking of reputation... You won't keep that inside. So you shouldn't try to because that will only work to your disadvantage" [Respondent 18 – corporate investigator]. Numerous examples can be derived from the media of organisations taking a different path though (see for example Radar, 2015; NRC, 2017). The damage of the information reaching the media in the end indeed seems considerable. It would be speculation to argue that the damage could have been contained if the organisation had been open about the norm violation from the moment the internal investigations were concluded. However, there seems to be merit in the above argument of respondents.

Interestingly, respondents suggest that because of a lack of specialised expertise and insight into the internal systems of an organisation, the police sometimes partly have to rely on information provided by corporate security investigators. This might mean that investigators may be able to provide a direction for the police investigations. This is a benefit for the police as police investigations may then be done more efficiently, however it also means that there is room for corporate investigators to leave out the more embarrassing details for the organisation. Many corporate investigators have a law

enforcement background and they prepare the report to law enforcement authorities in such a way that they feel it is easiest for the police to act upon the information (Blonk et al., 2017). "I always make the report to the police beforehand. So, I take my laptop and make the report in such a way that everyone who reads it may understand. So it's clear even to outsiders with no knowledge of our internal processes" [Respondent 16 – corporate investigator]. Law enforcement respondents indicate that for a case to succeed in criminal court, at the very least the suspect needs to be officially interrogated by the police with all the procedural guarantees. However, when the suspect again states in that formal situation that (s)he stands by the declaration made earlier to the corporate investigators, the law enforcement efforts may remain relatively minor. "We always try to shape the official report to the police as a sort of witness statement, in which we put all the relevant information from our investigations. So you can steer them a bit for the benefit of your client, point them in the right direction" [Respondent 41 – corporate investigator]. It depends on the views of the policemen and prosecutor involved how much room there is for corporate investigators to influence a criminal justice procedure in this way (see also chapter 5).

Respondents also indicate that organisations occasionally report to law enforcement authorities "just as window dressing. They'll report but actually they just want to wipe the slate clean and move on" [Respondent 27 – corporate investigator]. As we have seen above, organisations often do not expect much from a report to law enforcement authorities and some just report because 'it looks good'. This might be regarded as a strategic way to manage the reputational impacts a case might have. Below, some other strategic considerations are discussed, followed by some normative considerations to report.

1.2.1 Strategic considerations

There are instances where a report to law enforcement may help the (content of the) investigations, because corporate investigators lack the necessary access to information or powers of investigation to reconstruct what happened (Blonk et al., 2017). In such situations a report to the authorities is used as a strategic tool to get the police to investigate with the use of their formal powers.

> There are situations in which you can't get to the truth but it is in the company's interest and that of the stakeholders to get to the truth. But as a corporate investigator I don't have powers of investigation and especially when there is a third party involved and that third party does not want to cooperate, well that's that for me. And they have their reasons not to cooperate of course. But in such a case, you might have to go to the police and say, look this is as far as I could go but with the use of your powers of investigation you can get much further. So if powers of investigation may get you

> information that internal methods of investigations can't provide, yes, a report to the police is an option. [Respondent 28 – forensic legal investigator/client]

Respondents furthermore suggest that reporting a crime to law enforcement authorities might be helpful to other measures they take. A report to law enforcement authorities is often combined with other corporate settlements, as the problem for the organisation usually is not solved with such a report. However, it can be useful as an additional measure. It might for example strengthen private action proceedings, as the standard of evidence is higher in criminal court than in civil court. A criminal conviction has to be accepted as true by civil court (article 161 Rv [Code of Civil Procedure]). It is therefore likely that a civil court (when a private action is initiated) will accept the dismissal of the involved employee when he is found guilty of a crime in criminal court. However, as argued above, criminal cases take a lot of time and other forms of 'private justice' (see also Henry, 1983) are much faster. This may mean that the criminal case is not yet before the court at the time of a civil court hearing. Respondents indicate that a report to law enforcement authorities might still serve a purpose for civil court proceedings though, for example to show the court that the case is taken seriously by the organisation. "Sometimes a report to the police might help your civil court case. You say to the judge, we have reported it to the police, that's how severe we think this is" [Respondent 50 – client]. The fact that a report to law enforcement authorities is made is not a guarantee for a 'successful ending' in the civil court procedure though. While a conviction usually provides enough grounds for dismissal or a claim of damages, a suspicion of a crime is not necessarily the same thing as a breach of labour contract. Even when a criminal justice procedure is initiated, the dismissal may still be problematic.

> But the complicated situation might arise, I know from my colleagues specialised in labour law, that the employee has defrauded the company, a report to the police might be made, there can be an investigation but it is still difficult to fire him. So he might still be awarded a severance payment by a judge. [Respondent 30 – forensic legal investigator/client].

Another way in which a report to law enforcement authorities may be strategically used in corporate settlements is when it is employed as a fall-back option, with the purpose of pushing for another type of settlement (usually a settlement agreement as described in section 3). In this case, a report to law enforcement authorities is often not made after all because the involved person agrees with the settlement agreement. This is another way in which the power imbalance between corporate security/the organisation and the involved employee, described in chapter 3, comes to the fore.

> [A report to the authorities may be presented as an alternative for a] settlement agreement with the involved person guaranteeing that he will repay the damages within a certain time span. Well, if you cooperate with that we will not report to the police. So that's a trade-off, whether it's right or wrong is another thing but clients may choose to use a report to the police as leverage. [Respondent 2 – corporate investigator]

Another strategic consideration might simply be a question of costs. Although reporting a norm violation to the police also costs money in the sense of time and resources, and possible reputational costs, some organisations do not have the resources to privately investigate the matter. This may mean that measures are taken against an employee without an investigation (e.g. when there are enough grounds for dismissal), however it may also mean that a report to law enforcement authorities is made so that the authorities might investigate and file criminal charges. As stated above, most respondents do not expect the report to law enforcement authorities to be a solution to the organisation's problem though and many reports to the police are disappointing to an organisation.

> I can give you an example as well of why they *would* report to the police. It is much cheaper to have the police and prosecutor look into it than to do it yourself. For example with a charitable organisation that might be an issue, because an internal investigation may cost 50.000, 100.000 euro, easily. And curators [in a bankruptcy case] often think like that as well, just report and let the prosecutor do it. That saves me the trouble. So money may be a reason to report instead of investigating for yourself. [Respondent 28 – forensic legal investigator/client]

Fourthly, there is a category of organisations that is compelled to report to either the police or to a regulatory agency. Article 162 of the Code of Criminal Procedure dictates that when a civil servant breaks the law, this must be reported to the police. In practice, however, even these cases are often not reported (De Vries Robbé, Cornelissen & Ferweda, 2008). In addition, some organisations are under heavy scrutiny from regulatory agencies and these might also feel compelled to report to law enforcement authorities. "Some companies are obliged to report, for example financial institutions have to disclose to the regulator for financial markets. And listed companies have to disclose information that might influence the stock price" [Respondent 30 – forensic legal investigator/client]. In these situations, it might be best to make an official report to law enforcement agencies as well, as part of the reputational management strategy.

> If it's a listed company – they make reports to the police more often. Not always, but more often. It depends in part on the scale of the fraud, is it to be considered of material importance to the financial accountability of the organisation? That's a difficult matter but if the result would have been '50' and after the fraud it's '-50' then [it is of material importance and] the public interest is affected. And then there are those who are under scrutiny of a regulatory agency, they report more often. There are some arrangements for that, they have to report discrepancies and they often report to the police as well in such a case. Some regulatory agencies have leniency arrangements – if you self-report you might get off with a minor fine or nothing at all. That may be of importance in the decision. It's a very complex field of operations, there are all kinds of organisations and combinations. But in none of these categories of organisations reporting to the police is a law of nature. [Respondent 1 – corporate investigator]

An obligation to report to a certain regulatory agency is not the same as an obligation to also report to law enforcement authorities. For those compelled to report to their regulator, this does not necessarily mean that a report to law enforcement authorities is also made but it might be best reputation-wise to do so.

> The regulatory agency might expect a company to report to the police. And they might expect the company to get to the bottom of what happened. And inserting criminal law into the equation means that the company can move on without being afraid that some government organisation might get them at a later point in time. That can be very threatening to a corporation. For example, say you are an international trading firm and there are suspicions against you from British or American or Dutch authorities, that may limit your business severely. You're not able to give World Bank approved products to your customers anymore. And every contract has its anti-corruption provisions. And you'll be excluded from public tenders from the government. So settling the matter with the use of criminal law has certain benefits for companies, it allows them to move on and participate in tenders and the like. Of course they can choose not to. But they do run the risk the government will step in anyway, for example because the guy is fired but the matter becomes known in the public realm anyway. [Respondent 32 – forensic legal investigator/client]

Related is the last category of strategic considerations found in the fieldwork, which is a prime example of forum shopping by organisations and corporate investigators. Here, norm violations are reported to for example the Dutch law enforcement agencies to avoid prosecution in another, harsher jurisdiction. Although a prosecution in the Netherlands does not prevent prosecution in other national jurisdictions every time, respondents indicate that the chances of double prosecution are limited.

> But what I wanted to say, BallastNedam [a Dutch construction company] is a case which is in the news right now, I suspect that they thought, let's just go to the prosecutor here [the Netherlands] as fast as we can, it's almost begging for prosecution, please prosecute us and keep us safe. Although, oddly enough the *ne bis in idem* principle is not recognised internationally. By most countries at least. So the nasty thing is, if you report to the Dutch authorities, get a settlement, that doesn't mean you're off the hook in the US if you're involved there as well. I remember a case, Axo, 10 years ago or something – Axo was prosecuted in the Netherlands, it had something to do with trading with Saddam Hussein. But anyway, they were also prosecuted somewhere else but they [the prosecutors in the second country] did take the Dutch fine into account. I would prefer it if there was a treaty of some sorts about this. But right now, the unofficial trend seems to be, if you slip up try to get prosecuted in the Netherlands, because these prosecutions are reasonable. All my American colleagues say, had Van der Hoeven [Ahold] been prosecuted in the US, he would have gotten 10 years imprisonment. Without a doubt. [Respondent 37 – client]

Respondents are divided about the validity of the use of the *ne bis in idem* principle (the principle of double jeopardy) between different jurisdictions. However, internationally operating organisations may strategically choose to report a norm violation to the Dutch authorities to try to avoid prosecution in for example the US, where punishments are far more severe.

> There may be a strategic interest for a corporation to self-report to the Dutch authorities. For example, in a case that has worldwide relevance, where American and English regulators or prosecutors may get involved, it might be in the best interest of that company to make sure that the criminal case is done here, because of our lenient criminal climate. The Code of Criminal Procedure prohibits the Dutch prosecution office to comply with requests for legal assistance in cases they are investigating themselves. So you sometimes see lawyers running to the prosecutor to please investigate, because they know the risk that there's an American criminal investigation is greatly diminished then. [Respondent 30 – forensic legal investigator/client]

By forum shopping in this way, the organisation may attempt to be tried in the more lenient jurisdiction, aiming for the outcome which is most beneficial to the continuation of the organisation.

1.2.2 Normative considerations

Apart from the more strategically motivated choices for a report to law enforcement authorities, it seems that normative considerations also influence this process.

Corporate investigators are mostly focused on the client's interests, however it seems that they also take other considerations into account (Blonk et al., 2017). In their article about the role of the public interest in the private security market, Loader and Walker (2017) state that private security providers and clients are moral actors. They argue that non-contractual moral concerns guide private security providers alongside the contractual concerns they have regarding the private interests of their clients. The same can be argued for corporate investigators specifically (see chapter 6 for more on this issue). Although the involvement of corporate investigators in the decision whether or not to report a crime to the authorities differs, often they do exert a certain amount of influence. Many corporate investigators have a public-sector background (mostly police, but also military (police) and prosecution) and this might influence the way they think about the necessity to report to law enforcement agencies (see also White, 2014; Van Dijk & De Waard, 2001). However, among the respondents interviewed in this research, a clear difference in opinions between investigators with and without a public-sector background could not be discerned. Some corporate investigators and clients feel that any criminal activity that has been uncovered should be reported to the state.

> I feel that when someone has stolen 200.000 euro, that person should be held accountable in criminal court and you should report it to the police and you should make an example out of him. You know, to show that you will not accept that as an organisation. And that you'll do anything to make sure it doesn't happen again. [Respondent 5 – corporate investigator]

Most respondents express that while they expect no actual benefits from reporting to the authorities, they feel it is 'right' to do so: "Advantages? There are none – reporting a crime to the police is just something we do because we believe that when you know there has been a crime committed against you as an organisation, you need to report that. Period" [Respondent 20 – corporate investigator]. Not all respondents agree with this sentiment, as is shown by this quote from a lawyer:

> Tell me, what do you think you will accomplish dear manager? With the interests of your company in mind? You don't have the obligation to report, just look it up. So it's a feeling they have, especially in the semi-public sector, of 'didn't we all agree at some point to bring all criminal offences to the attention of the law enforcement agencies?' Well those who actually do it are heavily disappointed. [Respondent 28 – forensic legal investigator/client]

This quote shows an interesting tension between the private interests of the client and the public interests that are involved when a crime is committed. The fieldwork suggests this is something many respondents struggle with, whether they are corporate investigators, clients or law enforcement professionals. Contrary to the widespread believe that corporate security, as part of the private security industry, is focused solely on private interests, 'common good considerations' also seem to influence decisions made in investigations and settlements. Reports to the authorities are often made out of principle, respondents suggest.

> I'm working on an international fraud case now, we've been involved in the factual investigations for some time now to see what the options are. But there's also a matter of principle for them, the client has been defrauded and in truth he just wants to report to the police out of principle. We told him, the likelihood of it being investigated by the police is very low, the chance of the person responsible ever serving one day in prison is basically zero – all of that doesn't matter, it's a principle thing. If that's the goal and we can help him achieve that, that's fine. But it doesn't happen very often because it doesn't solve anything. We try to be of added value to the client, it is our job to help solve the problem. A report to the police has added value to a very limited extent. It can be to satisfy the retributive needs. [Respondent 41 – corporate investigator]

The added value of a report to law enforcement authorities is not very practical but moral instead. A second normative consideration to report is an experienced need for punishment. "Sometimes the client wants to also report to the police. It depends. Some are furious and want to report to the police no matter what" [Respondent 2 – corporate investigator]. "The moment it gets emotional they feel the police should be involved. Private law is more about procedures, the criminal justice system is about the person, punishing the suspect" [Respondent 12 – police investigator]. The corporate settlement options that do not involve a report to law enforcement authorities lack the moral indignation that can be expressed by a criminal case. "I had this case, they had been to civil court and the person was ordered to repay the damages. But he didn't have any financial means. That was a reason for the organisation to report to us [prosecution office], they felt he would have gotten off too easily. They wanted retribution" [Respondent 51 – prosecutor]. This expression of punishment inherent in the criminal justice system is also one of the reasons for organisations *not* to report, as organisations might feel that the actions taken against the employee are 'punishment enough'. These other actions, however harsh in their consequences, do not express the moral condemnation present in a criminal justice procedure. It depends on the organisation and on the severity of the transgression whether or not this need to show moral indignation is felt.

Thirdly, a report to law enforcement authorities may be made out of a sense of responsibility for the market in which the organisation operates. Some respondents expect some kind of preventative (moral) effect of a report to the authorities, either within the own organisation or within the market more generally. "My opinion is that you should report to the police, exactly because you want to prevent that someone keeps repeating this behaviour when given the opportunity. But it's not my call, it's the organisation that has to decide" [Respondent 27 – corporate investigator].

> In that regard it may help that someone is convicted and ends up on a blacklist. Because if he wants to work for a competitor in future he won't get a certificate of good conduct because he has the conviction. So should we fire someone without reporting him to the police, he will just apply for a job at a competitor tomorrow and he may continue with his norm violations. And it has a preventative effect within the organisation as well. Employees talk. So they know we are serious about it. There are stories to be told about managers taking stuff home and employees copying that behaviour. If you don't act upon it, that bad apple will spoil the barrel. So that's the preventative side. And looking at it more from a societal angle, us reporting will help to ensure that that specific person can't go on with defrauding organisations. We work with many temp agencies, should we just get rid of the person and not report and not notify the temp agency, he'll just be put at another company. And it works both ways, if a competitor gets rid of someone without reporting and he applies here he might get the job. Because he has relevant experience and a good resume, seems good. But all the while you will welcome a fraudster into your company without being aware of that. [Respondent 15 – corporate investigator]

Case study 13 can be seen as an example of this. The reason for reporting this case was that investigators found that there was an organised crime network behind it and that Observation Company 2 was not the first victim. In order to prevent the frauds to continue, it was decided to report the case to the police. Investigators indicated they were disappointed that the police did not investigate the matter.

1.2.3 Timing of law enforcement involvement

Interestingly, respondents indicate that in cases where there is a choice whether or not to involve the authorities and the choice is made to do so, it is preferred to file the report only after the internal investigations are concluded.

> Sometimes the authorities are already involved from the get-go but if you stumble upon the matter yourself you're going to have to see whether there's any validity in your suspicions first. It depends on the urgency of the matter but generally you want to take some time to assess the severity. You don't want to act on every false alarm.

> You have to realise, the moment an organisation is faced with something like this, it creates a lot of turmoil. People start to speculate, the dynamics in the organisation change, so you have to be very careful in dealing with that. [Respondent 37 – client]

As we have seen when discussing the reasons for organisations *not* to report a norm violation to the authorities, organisations place great value on the control over the investigation process and the resulting information. "Say there is a rumour, or something improper has occurred but they have no clue what has really happened. Is it just an error, are we maybe wrong or is there really something amiss? Before you report to the police you want to know, is there really something to be concerned about here" [Respondent 27 – corporate investigator].

> Let's say you report to the police the moment you get the feeling something's wrong. If you do that and they do act upon it, you'll lose all control over the situation. It's possible that the prosecutor decides to just arrest the person. Ok so then he knows what's going on right away. That could be a problem. So that means that in practice, many clients choose to report – when they want to do that – only after we finish our internal investigations. And the recoverability of assets may be of influence here. First you make sure you seize all assets of the involved person, maybe use a settlement agreement et cetera. [Respondent 2 – corporate investigator]

Finalising corporate investigations before reporting to the authorities is therefore considered wise from the point of view of client's interests.

> I usually tell them, do yourself a favour and make sure you investigate the matter first. At the end we will know what happened, if you still think you want to report – I wouldn't know why, but if you still feel the justice department needs to be involved in this, you can report then. But it is not illegal not to report, you don't have an obligation to report and you're not doing anything wrong by not reporting. On the contrary, I think that if you are a responsible manager, you will investigate privately first. You have to take the interests of the organisation and your employees into account. You have to make sure that there is no unnecessary reputational damage. And the only thing you're doing is saying, I want to know more before I decide how to handle this. [Respondent 28 – forensic legal investigator/client]

Postponing a report to law enforcement authorities until the internal investigations are concluded also has the added benefit for an organisation that this enhances the chances of the authorities acting upon it (see also chapter 5). Traditionally, fraud is not a high priority for police and prosecution and respondents indicate that the

better the information is that accompanies a report to law enforcement authorities, the easier the case will be for the police to investigate (Blonk et al., 2017).

> Nowadays they have lists of priorities and they have to do a certain amount of fraud cases every year. Well, it's nice for them when you can deliver a case that's a piece of cake. When you attach a full investigative report, including the underlying evidence, with a big bow around it, it makes things easier for them. So that means you're less likely to end up at the bottom of the pile. So if the client wants to report to the police, we can help them to increase their chances of it being investigated. [Respondent 2 – corporate investigator]

Even though the above course of action does enhance the chances of a case being investigated and tried in the criminal justice system, it is far from certain this will actually happen. This section has discussed reasons for and against reporting a norm violation to the law enforcement authorities. In the remainder of the chapter, more private types of settlements are discussed.

2. The civil suit

The considerations set out in section 1 finally lead to a decision to report to the authorities or to abstain from doing that. When a report to the authorities is not deemed the (sole) solution in a case, other options are available. The most 'public' one of these is the use of the civil court system. As a judge is involved here, chances are that (some) details of the case may become public knowledge. As mentioned before, this does play a role in the decision making, however, the influence of fear for reputational damage should at the same time not be overstated. Civil courts may be involved in a corporate settlement after corporate investigations in multiple ways. For example, a civil suit may be launched against the employee for the repayment of damages suffered. 'Damages' is a broad term here, as the costs for investigations can also be claimed as damages. In addition, the organisation may ask the judge to compensate for the interest missed over the sum that has been defrauded and to make the involved employee responsible for possible fiscal consequences of the fraud. "Damages can also contain the costs the organisation has made for the investigations. So, the repayment of damages includes the costs for the investigations. However, the costs of the use of a lawyer do not fall within 'damages'" [Excerpt from observation 1 – informal conversation]. Case study 1, 9, 11 and 13 are examples of cases in which a civil suit to reclaim damages was initiated against the involved persons in addition to a criminal justice procedure. In case study 6, 7 and 10

a civil case was brought against the employee to reclaim damages, without a report to law enforcement authorities.

Respondents state that they often initiate civil court proceedings in addition to other measures, such as a report to law enforcement authorities. The Dutch Criminal Code has a possibility to insert compensation measures in the criminal procedure, which is considerably cheaper for the organisation than initiating a civil suit. While costs may be compensated in part in a civil court procedure, this will only occur when the organisation is deemed in the right by the court. The organisation need not pay for the criminal procedure and the insertion of a request for compensation measures is therefore free of costs as well (though the compensation is usually lower in criminal proceedings) (Blonk et al., 2017). However, according to respondents, the applicability of such a request in practice is limited in many cases. The matter at hand is too complicated for the non-specialised criminal court and many claims of damages are referred to civil court. In case study 21 the other organisation that was involved[68] reported the case to the authorities and included a request for compensation measures as well. However, a civil suit was also prepared to reclaim additional damages.

> Often you see a report to the police being combined with civil court proceedings because, you can join as an injured party in the criminal procedure but the criminal judge will only take it into account for simple cases. For example, when you can say: 'I've suffered damages, see here's the receipt'. The moment it's more complicated than that he'll refer the case to civil court. [Respondent 1 – corporate investigator]

Civil court proceedings may also be initiated by the involved employee, for example when (s)he feels (s)he is being treated unfairly. In this way, an employee may give a judge the opportunity to assess whether the actions of corporate investigators and their clients are lawful (see also chapter 2). Since a civil suit creates expenses in legal fees and litigation fees and since it requires an active stance from the involved person, respondents indicate that a civil suit is usually not initiated by individual employees. However,

> It does happen. Once I had to provide legal assistance to an organisation in summary proceedings that were held against it. An ex-employee who was being investigated started the summary proceedings to get the judge to block the internal investigations.

68 See chapter 5. In this case, the involved person was an employee of (a subsidiary of) Observation Company 2 but the damages were suffered by another company (to which the involved person was providing services).

> He lost the proceedings of course, there were no grounds but it does occur that the employee takes the organisation to civil court. [Respondent 30 – forensic legal investigator/client]

A civil suit by an employee is often initiated to prevent the organisation from dismissing the involved person. Case study 4 is an example of this. Respondents indicate that while it happens that a judge retracts the dismissal, usually the relationship between employer and employee has been disrupted in such a way that the labour contract is dissolved. However, the court may award the employee with a financial compensation in such a case.

2.1 The civil suit to terminate a labour agreement

A civil suit may also be initiated by the organisation to dismiss an employee.[69] Often, employer and employee may have attempted to negotiate the termination of the contract and the conditions under which this will take place, but were not able reach an agreement. The dispute may then be settled in civil court. Damages are usually included in this civil court procedure as well. In case study 11, one of the employees involved was dismissed through the aid of civil court.

In general, a ruling by a civil court is necessary in case an employer wants to terminate the labour contract without the consent of the employee.[70] The grounds for such termination may be a disrupted labour relationship or culpable malfunctioning by the employee. In both cases, the employer will need to make a plausible argument to underpin these allegations. The termination is initiated by the employer, who has to comply with the term of notice. When the judge agrees with the allegations, the employee usually has no right to unemployment benefits, nor will he be granted a severance payment. The judge may decide to award the employer with a compensation in the case of culpable malfunctioning by the employee, to be paid by the employee (Ministry of Social Affairs and Employment, 2015a). In the case of a disrupted labour relationship that can be attributed to the employer, the judge may grant the employee an additional compensation (Ministry of Social Affairs and Employment, 2015b).

69 This chapter only discusses types of dismissal that are used for individuals who are suspected of wrongdoing. There are also dismissals for economic reasons (large scale dismissals), as a result of bankruptcy or as a result of disability but these are unlikely to be used.

70 Not all types of termination of the labour contract merit interference by civil court. See section 3 and 4.

2.2 The pro forma procedure

One interesting (though it seems, not very frequently used)[71] possibility is that the civil court is asked to validate a private agreement between employee and employer. In this case, the two parties will have negotiated the terms of separation and will have come to an agreeable solution for both parties. During the *pro forma* procedure, the parties provide the judge with their agreement, who looks it over and ratifies it. The actual content of the agreement is not considered closely by the judge, nor is this desired by either party. The employee formally disagrees with the solution provided by the employer but simultaneously states that (s)he will not contest it if the judge rules in favour of the employer. This practice is described as a 'puppet show' by many commentators (see for example Beltzer, 2005). The employee merely contests the agreement to ensure the right to unemployment benefits will not be lost. This situation was deemed undesirable by the Dutch government: "the government notes that it is no advocate of *pro forma* procedures because of the unnecessary pressure on the judicial system. If parties agree about the terms of termination, no interference of a judge should be necessary" (Eerste Kamer der Staten-Generaal, 2014: 89).

As a result of changes in labour regulation, employees no longer lose their right to unemployment benefits by agreeing to a termination of the contract (such as a settlement agreement). The advantage of the *pro forma* procedure for the employee is therefore no longer present. According to respondents, the employer might still deem it wise to formalise an agreement with the employee through civil court. The added value of a *pro forma* procedure for an employer is that it provides more security than a settlement agreement (see below), because the employee has the option to revoke the settlement agreement, while the *pro forma* procedure produces a court ruling which cannot be contested (although the employee may still appeal to a higher court).

Respondents mostly seem to feel that the *pro forma* procedure has become obsolete. "The judge does nothing really in such a procedure, I see it more as an extension of a settlement agreement. But it hardly ever happens, I don't see the usefulness of a *pro forma*. We hardly ever use it" [Respondent 50 – client]. According to respondents, many organisations feel a dismissal or a settlement agreement is a much more efficient solution. Nonetheless, the *pro forma* procedure remains an option. It may be used to shorten the legally defined waiting period which is used by the Dutch unemployment agency before allowing benefits or in a situation in which it is expected that the employer will not pay the severance payment agreed to (ontslag.nl, 2014). It provides both employee and employer with an enforceable court sentence and thus with more security that the termination of the labour contract

71 To illustrate, the *pro forma* procedure appears in none of the case studies.

holds up and that agreements will be honoured, without making the details of the case known to the wider public. While the civil court makes the final determination, not only the shaping of that determination but also the choice of the court as the legal venue is privately governed.

2.3 The Enterprise Court (Ondernemingskamer)

Most settlements discussed in this chapter are initiated by the (management of the) organisation. The Dutch private law system also provides other interested parties with an option to appeal to a civil court however. In the so-called inquiry procedure (*Enquêteprocedure*) other interested parties also have the opportunity to instigate an inquiry (articles 2:344 through 2:359 BW [Civil Code]). In this procedure, an interested party (shareholders, the Works council, a director) complying with certain conditions might bring the case before the court, to claim mismanagement of the organisation (Van den Blink, 2010). This is a special procedure that is held by the court of appeals in Amsterdam. The Court decides whether or not there are grounds for investigation and if there are, an investigator is appointed. This investigator is paid by the organisation but reports to the Court. The investigator is granted full access and every person involved with the organisation has to cooperate with the investigations. Once the investigations are completed, the investigator reports to the Court. The Court then decides whether or not there has been mismanagement, which could lead to accountability of the board of directors or the supervisory board of the organisation (AMS Advocaten, 2015). Pending the procedure, the Enterprise court may take provisional measures if necessary. These measures can be very far-reaching, such as the dismissal or appointment of a director, or revoking the voting rights of certain shareholders. These measures may also be taken when the procedure has been finalised (Peters, 2006).

> That Enterprise Court is a special court for disputes relating to companies. It is a highly qualified part of the court of appeals and it is highly respected. No one will think of refusing the investigator access. If they do, the investigator will report to the court no access was granted and the court will fine the corporation, 100.000 euros a day. Its powers are enormous. [Respondent 32 – forensic legal investigator/client]

2.4 Some differences between criminal justice and civil court proceedings – the use of evidence

The rationales underlying a criminal justice procedure on the one hand, and civil court proceedings on the other are significantly different. Criminal court is about 'finding the truth' in a dispute between the state and an offender, while civil court proceedings are focused on the facts as presented to the court by the parties (who

are presumed to be equal). This means that when some facts are not contested by either party (even if not 'true'), the court will accept these facts: "in the private law system, the trial is organised in a certain way. You litigate based on presented facts. So facts which are not presented and facts which are not contested are considered to be true" [Respondent 40 – corporate investigator]. As mentioned in the previous chapter, the standard of evidence is higher in criminal court and the burden of proof lies with the state (in this case the public prosecutor). As the rationale of civil court proceedings is based on horizontal relationships, information presented in court is considered a fact when neither party contests the correctness of it. This means that information which may be considered circumstantial in criminal court, may serve as evidence in civil court.

The question of illegally obtained evidence is an interesting one in the context of civil court procedures. Case law suggests that in a civil court procedure, evidence is not excluded lightly. If the information which is presented to the court is deemed illegally obtained, this situation will usually be compensated by a (higher) severance payment (in the case of termination of the labour contract) or an award of damages to the involved employee. Whether or not the evidence is illegally obtained is judged by looking at the law (for example: was there a criminal offence which led to the information) and by principles of law used by corporate investigators, most notably proportionality and subsidiarity (see chapter 2) (Koevoets, 2004). The Dutch supreme court has ruled that evidence which is obtained illegally does not necessarily need to be excluded from evidence, which is contrary to the situation in criminal proceedings (see article 359a WvSv [Code of Criminal Procedure]).

> Article 152 Rv [Code of Civil Procedure] dictates that evidence may be given by all means and that the evaluation of evidence is left up to the magistrate, unless the law states differently. In a civil court procedure the general rule is not that the court should ignore illegally obtained evidence. In principle, the public interest of revealing the truth and the interests of parties to substantiate their claims, which are the basis for article 152 Rv, outweigh the importance of the exclusion of evidence. Only when there are additional circumstances, the exclusion of evidence is justified. (ECLI:NL:HR:2014:942)[72]

Interestingly, while evidence which is illegally obtained by law enforcement actors will generally be excluded from a criminal procedure (article 359a WvSv), the same does not necessarily apply to evidence which is illegally obtained *by corporate investigators* and

72 This court case was about the use of private investigators by an insurance company against a costumer. The more general rule the Supreme Court formulates is also applicable to the employer/employee relationship.

handed over to law enforcement authorities. Case law has indicated that as long as law enforcement actors were not involved in the process of gathering the information, the information may be used in criminal proceedings.[73] The evidence might still be regarded as illegally obtained and this might have consequences in the criminal procedure but just as is the case in a civil court procedure, the evidence might still be used.[74]

> In principle, everything which is presented to the court may be used in a civil court procedure. Solid evidence obtained with the aid of private investigators is not easily removed from the procedure. But it might still be illegally obtained if you look at it from a criminal justice perspective. A criminal procedure is so different from a civil suit, they should be viewed separately. Just speaking in terms of timing for example – the civil court procedure will usually be done before the criminal procedure even started. [Respondent 50 – client]

In addition to the difference in the way civil and criminal courts handle illegally obtained evidence and the timing referred to by this respondent, another notable difference is the symbolism that is attached to civil court proceedings and criminal justice. As stated, some organisations feel the need to punish the involved employee. The criminal justice system, which is largely focused on retribution and punishment, is much more suited for that than the private law system (although it is not the *organisation* doing the punishing in the criminal justice system but the state[75]). Civil court proceedings, representing horizontal (though not necessarily equal) relationships between parties, are more about compensation than punishment.

This section has discussed multiple ways to involve a civil court, some of which are fairly private (the *pro forma* procedure), others may become much publicised (for example some large cases done by the Enterprise Court). In any case, the use of civil court is (potentially) fairly 'open', as the norm violation or at least relevant parts of it will become known to the court and hence, potentially, to the wider public. The sections below, discuss more private ways to settle internal norm violations.

73 See for example ECLI:NL:GHSHE:2006:AY1071 (ruling of the court of appeal Den Bosch).

74 In this sense, the extent of judicial control over (indecent) actions by corporate investigators is thus rather limited.

75 This is a result of the fact that in the Dutch system, like in many other jurisdictions, a criminal offence is seen to represent a dispute between the state and an offender, rather than between an offender and a victim. In the Dutch criminal justice system, the victim is no party to the dispute (although victim rights are now incorporated in the criminal justice procedure, see for example Pemberton & Reynaers, 2011).

3. The settlement agreement: a court-free arrangement

Although some organisations prefer to dismiss an involved person themselves once the investigations have concluded that he or she is indeed involved, many prefer to part ways without the necessity of court involvement. This may be achieved by the person resigning (with or without the 'encouragement' of the employer) or by negotiating an agreement of separation between parties. The settlement agreement (article 7:900 BW) is a termination of the labour contract with mutual consent: employee and employer reach agreement about the terms of separation. This agreement is binding to both parties. This may be a contract in which parties agree on an amount payable by the involved person and it may also include conditions, such as the termination of the labour contract. "In this case, there were two people involved and we struck a deal with the one and the other is paying a monthly amount" [Respondent 6 – client]. Although "there is no binding standard – it depends on what you put in there" [Respondent 50 – client], respondents do indicate that a settlement agreement that is used as a result of norm violations usually contains the following elements:

> Party 2 [employee] commits to reimbursing the financial damage of party 1 [employer] within 24 months after this agreement is signed. (…) [Employee] furthermore declares to pay the legally established interest from the moment the illegal payments were made until the moment these are repaid to [employer] (…) In addition, [employee] agrees to pay the costs made by [employer] to investigate and settle the incident. (…) As far as the unlawful / illegal acts of [employee] have tax implications (for example, but not limited to concerns in terms of VAT and wage or income tax), [employee] agrees to fulfil those obligations independently and to free [employer] of any such obligations. (…) [Employee] states to instantly (date of signature of this Agreement) take immediate resignation from [employer] and to directly resigning from employment with [employer]. (…) [Employee] agrees to irrevocably waive the invocation of a possible claim that this agreement is null or void and to place no objection or appeal against the termination of the employment relationship with [employer].[76] [Observation 1 - settlement agreement]

Negotiations between employer and employee resulting from the corporate investigations report usually form the basis for the settlement agreement. It is possible to hand this agreement over to a civil court for ratification in a *pro forma*

76 July 2015 has seen the implementation of the new law on employment in the Netherlands. One of the changes in this law is that in cases of termination by mutual agreement, such as the settlement agreement, the employee has two weeks to change his mind (Ministry of Social Affairs and Employment, 2015a). The settlement agreement provided above was made before this change in regulation.

procedure, however this is not necessary. This type of termination of the labour contract does not need to be approved by court because it is consensual. In many cases, the settlement agreement is the corporate settlement of the norm violation. In case studies 10, 12, 16 and 20 a settlement agreement was used to terminate the labour contract. In other case studies (3 and 16)[77] a settlement agreement was used as an addition to the (one-sided) dismissal of the employee. In such a case, the agreement contains arrangements about a severance payment or (more likely) a repayment of damages.

An interesting possible addition to a settlement agreement is a non-disclosure clause. Non-disclosure may also be used in other types of corporate settlements, in the form of a separate agreement. However, the fieldwork suggests that the use of non-disclosure is most likely to occur in case of in a settlement agreement. As discussed above, organisations might be inclined to keep the information that internal norm violations have occurred, quiet, for example as a result of fear for reputational damage (see e.g. Van Dijk & De Waard, 2001). A non-disclosure clause or agreement could provide a solution for this sensitive matter. Parties agree to keep both the norm violation and the agreement that has been reached quiet. Respondents suggest that the use of a non-disclosure clause is quite standard in a settlement agreement.

> Ok so he's gone with a settlement, you settle the matter there and that's that. I'm rid of the guy. And you come to terms with each other about what you will and will not make public. You make a settlement agreement and a non-disclosure is usually in there - well, then we won't talk about it anymore. From either side. We don't always want that because we want to be able to talk about it. In case the next employer of the guy contacts us to ask, 'how did he perform when he was with you?', you want to be able to say, 'we've kicked him out'. [Respondent 19 – corporate investigator]

There is no consensus among respondents regarding the use of non-disclosure tools. Not all respondents have experience with it and some are opposed to the practice. In literature, the field of private investigations is sometimes called non-transparent an murky (e.g. Klerks & Scholtes, 2001). The use of non-disclosure agreements does not do much to improve this image and some respondents highly value transparency (this does not mean that information is volunteered for public use however). Others do make use of the practice and feel it is just part of the arsenal of solutions organisations have at their disposal.

77 In case study 16 this relates to another employee than with whom the settlement agreement referred to above was made.

> To stay with the example of the guy who is kicked out. Something will be arranged with him, he gets something of a severance payment and it's stated clearly: we will not discuss this anymore. Or the word 'fraud' is and will be avoided by both parties. When parties agree about this, they should sanction the transgression of this agreement, you know a reimbursement payment if someone doesn't stick to the arrangement. So yes, these things happen. You know, that parties keep quiet. I think you can imagine that [the employee] is fair game in a way when he sits there. And when you [CM: the investigator] have your suspicions but you can't make it stick, you may decide ok let's do it this way. I think that in the end both parties must make the best of a bad bargain. [Respondent 6 – client]

With or without a non-disclosure agreement, the settlement agreement consists of some duties for the (ex-)employee, for which he has to sign. As this agreement is preceded by a negotiation, both parties may influence the outcome. In other words, contrary to most other forms of corporate settlement, a settlement agreement is not a one-sided decision taken by the organisation. A settlement agreement furthermore holds some advantages for the involved employee. In addition to the influence (s) he may exert over the process, the employee retains the right to unemployment benefits and will usually be awarded a severance payment. Some employers find this circumstance problematic. "A settlement agreement has the disadvantage that it does not involve a registration of dismissal for this person. This means that he retains his rights to unemployment benefits and the like. But should we as a society pay for that? It was his choice to transgress. But sometimes, you have no choice other than to settle it in this way" [Respondent 47 – client]. However valuable, the influence of the involved person should not be overstated in practice (Meerts, 2014b). Although many settlement agreements contain wordings such as 'the employee hereby states that he has entered and signed this agreement freely and without duress and is aware of the resulting obligations', it cannot be denied that the employer holds the position of power in these negotiations (Meerts & Dorn, 2009). For one, the employer is in the position to report the employee to the police and to take action based on labour law. Respondents state that when a settlement agreement is chosen, the case is usually not as clear as when the organisation chooses to dismiss someone.

> A settlement agreement is done by mutual consent and it has a non-disclosure agreement. To me, it remains a bit risky to use it because it is showing your weakness. The legal representative of the employee often tries to get some severance payment for his client. A settlement agreement often is chosen because of a lack of strong evidence and they know that of course. So you're going to have to get into a negotiation. So I'd rather try a dismissal on the spot. [Respondent 47 – client]

However, this is not always apparent to the involved employee and the threat of a conclusion to the matter with more severe personal consequences (e.g. a report to law enforcement authorities or a dismissal on the spot) might put him or her under duress to cooperate. Even though respondents indicate that involved employees are allowed to bring representation, not all involved persons make use of this option. The organisation, on the other hand usually does have legal representation and, in addition, the corporate investigative report. As we have seen in chapters 2 and 3, most corporate investigators use procedural guarantees such as the adversarial principle, this however does not change the fact that the investigations are predominantly focused on employee behaviour and much less on the organisation as such (Williams, 2014). Respondents do indicate that they try to keep a broad view on the matter and also take organisational factors into account, however, the organisation remains the more powerful party in the negotiations. A settlement agreement is therefore much less one-sided than other types of corporate settlements, nonetheless there remains a definite power imbalance (Meerts, 2013).

> It is very easy to destroy someone entirely, we are aware of the enormous power of an organisation compared to a single individual. And that might mean that we present results twice to an involved person. And that we also report information that is not beneficial to the client. For example, if you would claim expense accounts falsely three times and we investigate and say ok this is indisputable, I always also look for the person's peers, how do they act in similar situations? (...) And I also check whether there has been a correction. Just imagine, you have written down in your report this person has claimed expenses thrice and you build your case on that, only to have the person prove at the end of the day that he has corrected it and reimbursed the money. [Respondent 27 – corporate investigator]

Some organisations decide to take additional steps against someone when they have settled through a settlement agreement, for example report the person to law enforcement authorities or initiate reclamation of damages. In case study 10 for example, the labour contract of the involved person was first dissolved through a settlement agreement and after additional investigations, a civil suit was brought against him to reclaim damages. Often, this possibility of additional action has been excluded as an option in the terms of the settlement agreement. An interesting case in this regard is the 2015 news story that SNS Reaal had been reported to the law enforcement authorities by a former chairman as a result of breach of the settlement agreement.[78] The CEO who was involved in the matter had come to a settlement agreement with SNS Reaal and this

78 http://www.nrc.nl/handelsblad/2015/11/07/oud-topman-vastgoedbank-doet-aangifte-tegen-sns-1553293.

agreement stated that the severance payment awarded to him could only be reclaimed by the company in the case of fraud, if this fraud was reported to the authorities within six months. SNS Reaal tried to reclaim the money because of fraud, however they were too late (but claimed to have been in time). As a reaction, the CEO reported SNS real to the police for falsification of documents. In this case, the involved person actively responded to what was in his eyes abuse of the settlement agreement (and the pending criminal and civil court cases), though many involved persons will not. However, the fact remains that there is more room for influence by the involved person in the process of negotiating the settlement agreement compared to other corporate settlements.

4. Internal sanctions as a solution

In addition to the above conclusions to corporate investigations, many organisations have their own array of internal sanctions. Some commentators use the term *private justice* specifically for this type of corporate settlement (cf. Henry, 1983). These sanctions and the transgressions which merit them are usually embedded in the collective labour agreement or in the labour contract employees sign when entering the working relation with the employer. These sanctions are discussed with the Works Council of the organisation (if available). "People know this, it is laid down in the collective labour agreement and they are warned [against unwanted behaviour, CM]" [Respondent 15 – corporate investigator]. Internal sanctions range from very mild to pretty severe. Below, internal sanctions which keep the employee inside the organisation (thus retaining the labour relationship) are discussed first. Section 4.2 goes on to consider some internal sanctions resulting in the termination of the labour contract.

4.1 Internal sanctions: disciplining the employee

In addition to corporate settlement options which place the reaction to the norm violation (criminal justice and civil court proceedings) or the involved person (settlement agreement) outside the organisation, norm violations may also be handled completely internal to the organisation. These internal sanctions are considered to be less severe (or 'permanent') than other corporate settlements by respondents, who indicate that they are more likely to be used when the transgression is not very serious or when it is impossible to produce compelling evidence against an involved person.

> When you have your suspicions but you can't prove it. In those cases someone might be removed from financial administration or you make sure he can't access certain systems anymore. Because you might have a pretty good idea about the source of the

> irregularities, especially when there is also outside involvement. Or if it simply has to come from the inside but you can't point out who is involved. We might think, 'it's him' and by removing that person you might solve the problem. [Respondent 6 – client]

Other sanctions include different types of warnings, the reduction of fringe benefits, demotion, being passed over for promotion or the denial of certain types of access.

> We have different kinds of warnings, you may receive an official warning, but there's also a reprimand and a serious reprimand with a conditional discharge. And then we have downgrading salary, downgrading pay grade. Just name it. [Respondent 18 – corporate investigator]

In the case studies internal sanctions were indeed used when the norm violation was either minor, a result of faulty internal organisation (when the norm violation was not too harmful) or when no specific employee could be identified as being responsible for the norm violation. In case study 2 and 21 the person was relocated, so (s)he could do no more harm. The involved employee in case study 21 was furthermore suspended from active duty. In case study 11, 12 and 20 some employees who had minor involvement in the case received different kinds of warnings, with or without the obligation to pay damages. In case study 12 a manager was furthermore demoted to a lower employee position. According to investigators from Observation Company 1, there were internal sanctions in case study 7 as well but which specific sanctions could not be derived from the case report (or the memory of the investigators).

There is a very wide range of possible sanctions, which have to be communicated to employees before they may be used. This is often done in the collective labour agreement or the terms and conditions of an organisation. As the internal sanctions are part of the internal regulations there is no legally defined standard set of sanctions. However, the sanctions mentioned by respondents fall within the general categories of warnings, benefits or salary, demotion, removal of access and (temporary) suspension. The termination of the labour relationship may be considered to be the 'ultimate' internal sanction. Section 4.2 focuses on this.

4.2 Termination of the labour contract

One could place the termination of the labour contract under the banner of internal sanctions. It is however, an internal sanction which effectively puts an end to the labour relationship between employer and employee (which is why some respondents do not feel it is an 'internal' sanction). There are multiple ways to terminate a labour contract. The employer may ask a civil court to dissolve the contract (see section 2 of this chapter), there may be a termination of the labour contract under mutual agreement (see section

3), the employer might want to dismiss someone on the spot, the employee may be the one initiating the separation and in some cases a contract might automatically cease to exist after a certain period in time. Some of these have been discussed above. In this section the remaining relevant ways to terminate a labour contract are discussed. It is interesting to note that apart from case study 17 and 19 (in which no involved person was identified) and case study 2 (in which there was not enough evidence to dismiss the involved person) termination of the labour contract in one way or another was part of every case study.[79]

Within the possible ways to terminate a labour contract, a scale of severity can be discerned. A summary dismissal ('on the spot'), with possible repayment of damages, would then be the type of termination of the labour contract with the most severe consequences for the involved employee. Compared to the settlement agreement discussed in section 3, there is less room to take the interests of the involved employee into account in these other types of termination. For example, a severance payment may be paid here. When the employer initiates the termination but the employee consents to the termination, it is not necessary to involve a court (article 7:671 under 1 BW; Ministry of Social Affairs and Employment, 2015a; 2015b). This leaves some room for negotiation and influence by the employee. By not granting consent to the termination, the employee forces the employer to go to court. An agreement may then still be inserted with regard to a severance payment or other arrangements. This does not necessarily have to be in favour of the employee though: in case study 16 for example an involved person was dismissed and a payment plan for damages was also agreed to. Interestingly, consent from the employee is not necessary under certain circumstances, notably when it involves a director of a legal entity (article 7:671 under 1 e BW).

Another condition under which involvement of a court is not necessary is in cases of 'urgent circumstances' (article 7:677 BW). If urgent circumstances may be argued, an employee may be dismissed on the spot without court involvement (however the employee may appeal to the court in case he does not agree). 'Urgent circumstances' include criminal behaviour or non-compliance with (internal) rules and regulations. This termination is initiated by the employer and the employee will lose his right to unemployment benefits. There is no period of notice to take into account and the labour contract will cease to exist immediately ('on the spot'). The employee cannot claim a severance payment and will have to compensate the employer. An important condition for a summary dismissal is 'immediacy'. This means that the organisation

79 Since there are multiple employees involved in some of the case studies, this does not mean that the labour contract of every employee who was identified as being involved in the case has been terminated. In case study 5 it is unclear what kind of settlement was used as this was not in the report and the investigator did not remember specifically (however, the report does give the advice to use internal sanctions – which may include dismissal as well).

may take some time to investigate the matter, but will have to act as soon as it 'has the facts' about a norm violation in order to comply with the condition of immediacy. The condition is breached, for example, if too much time passes between the discovery of the norm violation and the initiation of an investigation and if only after that action is taken against the employee (Ministry of Social Affairs and Employment, 2015c). Often, respondents suggest, the employee is suspended from active duty to comply with this condition. As this HR manager indicates, it is not always easy to dismiss someone on the spot:

> I have become less cautious, if you follow the advice of the attorneys too much you're too careful. All they see is road blocks, they would rather be too careful than to take a shot. But experience shows that employees hardly ever use the condition of immediacy against you. Sometimes you're just going to have to take a shot and dismiss someone on the spot and see whether he will fight you on it. Sometimes it's not possible, your case is too weak. Investigators find that very frustrating because to them it is obvious. I often agree and I understand where they are coming from but we have to make sure it sticks in a legal sense. [Respondent 47 - client]

The more stringent demands related to a summary dismissal may mean that management or HR chooses the easier solution of a settlement agreement. Some corporate investigators express they have an issue with this practice as the feel it is overly cautious: "I mean, if there is much evidence, everything is there except a confession, they will still go for the written warning so to speak instead of a summary dismissal. How ridiculous is that?" [Respondent 48 – corporate investigator]. On the other hand, other investigators feel that a summary dismissal unnecessarily complicates matters. If the employee resists the summary dismissal and appeals to civil court, that means more work for the investigators.

> Summary dismissal, I am not a fan. To be honest, I think that with a summary dismissal you get into a different trajectory – the person may fight it, get a lawyer, you go to trial and all of that takes time and manpower because we will have to generate more reports to help the lawyers in trial. It's just a far-reaching decision and it's hard to take it back. [Respondent 18 – corporate investigator]

A summary dismissal is often used as a sort of punishment, respondents imply. When the employer feels the norm violation is too serious to settle the matter by consent, a summary dismissal is preferred. Case studies 6, 11, 12, 15 and 20 involved a summary dismissal of the involved person. The above quoted respondent goes on to say:

> It also depends on how strongly you feel about the matter. When your evidence is not very strong but you're certain about the involvement of this person and you're not willing to compromise, you can choose dismissal on the spot and wait and see whether it sticks. Sometimes we're sticking to our guns and the employee disagrees, well he will have to appeal to the court. The thing is, our internal systems are very complex and employees may be able to hide behind them. That makes the whole thing a bit difficult in legal terms sometimes. When someone does not say in a statement that he did it, that makes things more difficult. [Respondent 47 – client]

Another option is that the employee is the one terminating the contract. The downside to this for the employee is that he cannot apply for unemployment benefits (which is not specific to resignation by the employee, several other types of termination also mean forfeiture of the right to unemployment benefits). On the other hand, resignation may serve the employee as it looks better on a resume than to have been dismissed. For the employer, there is the benefit of not having to go to much trouble regarding dismissal procedures and not having to pay a severance payment. In the negotiations which may follow corporate investigations, these things may be taken into account.

When the involved person is a temporary worker or has a fixed-term contract, it is easier to dismiss the person than when the labour contract is for an indefinite period, respondents suggest. One could for example choose not to renew the contract without having to dismiss the person. In this case the employee retains the rights to unemployment benefits, no involvement of a court is necessary and no severance payment has to be paid. However, when the employer wants to terminate the contract before that time, the same rules apply as set out above. As fixed-term contracts may be entered for multiple years, the employer might have to act prior to the end date of the contract. If the remaining period is not too lengthy, respondents suggest that the employee may be suspended from active duty in the meantime (such as was the case in case study 21).

An employee with an indefinite contract has a stronger position than temporary workers or employees with a fixed-term contract. Dismissal of a permanent employee requires a dossier, explicating reasons for dismissal (which may be formed by the corporate investigations report). Especially when it comes to summary dismissals, standards for this dossier are high as this type of dismissal does not include a notice period or court involvement. "Before you can fire a permanent employee you need a solid dossier, for the dismissal of a temporary employee this is not necessary. When they [temporary workers] transgress, saying goodbye is pretty easy, that's just a matter of immediately terminating the collaboration with this person" [Respondent 47 – client]. A temporary worker is employed by the temp agency, not by the organisation that uses this agency. The employer may simply not renew the contract (in the case of an employee with a fixed-term contract) or the services of that person

will no longer be used (in the case of a temporary worker). Case studies 13 and 14 involved temporary workers who were terminated.

When a transgression is serious enough, respondents state that organisations want to dismiss the person and not to keep him or her inside the organisation. Some feel that this is a pretty severe punishment in itself. "When you fire someone on the spot, he doesn't have any rights you know. No right to social security, no right to a severance payment" [Respondent 47 – client]. Of course, it depends on the type of separation chosen but the loss of employment is seen as punishment in itself. However, when trust is broken, it is hard to retain someone in the organisation.

> If we catch someone with a theft or fraud, they'll immediately get the worst punishment. That's the end of your job here. Prosecution works differently, you might get a probationary sentence or a fine and get another chance. Our policy is once you start doing that kind of stuff, we're going to say goodbye. That can be pretty heavy. Someone working for years and years with us and slipping once... But the trust is gone, you know. There's no coming back from that. [Respondent 15 – corporate investigator]

Discussion

This chapter has explored different types of 'follow-ups' for corporate investigations. In the case that the norm violation may be defined as criminal, organisations might decide (mostly after the investigations have been finalised) to report the case to involve the criminal justice system. There are multiple considerations compelling organisations to either report or choose not to do so. Both strategic and normative considerations may underpin the decision to report. At the same time, strategic and normative considerations also influence the decision *not* to report. There are various reasons for organisations to prefer to handle matters privately. Most of these motivations revolve around the concepts of the framing of (economic) crime; secrecy discretion and control; and legal flexibility and responsiveness (Williams, 2005). In cases where no criminal behaviour is involved, a report to law enforcement authorities is not even an option. Some respondents suggest that they do not report in certain cases to protect the employee who is involved. Some moral considerations may therefore be discerned here as well.

The decision whether or not to report is an important choice. Once this choice is made and the organisation has decided *not* to report to law enforcement authorities, other, private options remain open, as discussed in this chapter. In general terms, there are corporate settlements that involve a civil court, those that are based on

negotiations and mutual agreement between the organisation and the involved person, and those that are concluded by what is often called 'private justice': forms of internal sanctioning. In this chapter, the different solutions provided by different legal venues are termed 'corporate settlements'. More generally they can be argued to provide a system of corporate justice. Within this system of corporate justice, corporate investigators and clients may be flexible, forum shopping in a way to get to the solution which is considered best suited in a certain case. This may mean that a report to the authorities is made out of strategic (for example because powers of investigation are necessary or because there is a threat of prosecution in another (harsher) jurisdiction) or normative considerations (for example an experienced need for retribution), it may mean that civil court is used to for example reclaim damages, that the private law system more generally is used to reach a mutual agreement of termination through a settlement agreement, or that internal sanctioning systems are used to either punish but retain some in the organisation, or to dismiss the involved person. All of these possibilities may be used separately but combinations between them often occur as well. A report to law enforcement authorities is for example usually combined with another corporate settlement as the report in itself does not solve the problem of the organisation. A report to law enforcement authorities seems to be regarded as an additional measure by most respondents instead of an end in itself. Other types of corporate settlements may also be combined, for example a dismissal might be accompanied by a civil suit to reclaim damages. The case studies used in this research are dominated by a form of dismissal, combined with another type or corporate settlement.

While a driving force behind the choice for a certain settlement is 'fixing the problem at hand', certain other considerations also seem to influence the decisions taken. The desire to punish someone might compel an employer to either report the person to law enforcement authorities or dismiss him on the spot, even when a case might not be strong enough to do so. In other instances the necessity to repair the damage done and move on might make a settlement agreement the more likely option. It is difficult to discern a fixed decision-making process. Just as is the case with many other matters in the field of corporate investigations, deciding how to handle the matter is a decision which is done *ad hoc*. This chapter has however discerned some considerations that may steer these decisions. The next chapter focuses on those instances in which law enforcement agencies have become involved in the corporate investigations in one way or another.

Chapter 5

Coexistence

Public/private relations in corporate investigation settings – information transfer, information sharing and coordination

Introduction

The focus of previous chapters has been predominantly on the considerable autonomy of the corporate security sector (and its clients) when it comes to investigations and settlements of norm violations within organisations. Although corporate investigators and clients see many reasons – explained in chapter 4 – to keep matters private, there are also instances in which law enforcement agencies are involved in one way or another. This strategic behaviour, making use of the resources and options of both the public and private sphere to achieve an optimal result, is termed forum shopping in this book. Forum shopping occurs in all aspects of corporate investigations, influencing clients in the decision which investigator to use (chapter 2), influencing corporate investigators in the decision which investigative methods to use (chapter 3), influencing clients and investigators in the decision which corporate settlement to choose (chapter 4), and finally, when a public sector solution is chosen, influencing the timing of law enforcement involvement, as well as the decision where to report (chapter 5).

The question of public/private interconnections in security matters has been introduced in chapter 1 of this book, describing the views of many criminologists about public/private relations in the various spheres of security: relations between the public sector and private security are often posed in terms of cooperation by the latter with the former (Hoogenboom & Muller, 2002; Hoogenboom, 2009; Dorn & Levi, 2009; Cools, Davidovic, De Clerck & De Raedt, 2010). By contrast, as previous chapters have shown, corporate security typically acts quite independently from law enforcement (even though many corporate security professionals are ex-law enforcement). In many instances the work of corporate investigations professionals remains completely out of sight of the public sector. As Van Ruth and Gunther Moor (1997: 129) state, parts of the activities of corporate security display overlap with police tasks – here corporate security fills the gap left by police (the junior partner argument). However, another significant part of corporate security's work is completely separated from the criminal justice system; corporate investigators thus have an independent role to fulfil within the market. The corporate security sector may be regarded as a semi-autonomous social field, with a "capacity to generate rules and induce or coerce conformity" (Moore, 1973: 722). Semi-autonomous social fields are not fully isolated, nor completely autonomous. Legal frameworks provided by the state are in place for the corporate security sector, as discussed in chapter 2 – however within the context of these rules and the corporate security field, a high level of autonomy exists.

Corporate investigators do not operate in a vacuum, free from *any* public involvement in the corporate investigations. As indicated in chapter 4, there are

several reasons for law enforcement to wish to be, or to be invited to be, involved in some corporate investigations. The question remains how such contacts may be conceptualised. Chapter 1 has introduced a very crude scale of relations, ranging from separation, through *ad hoc* coexistence/cooperation, to corporate security performing obligatory tasks for the state. The focus of this book is on the first two of these possibilities, the third being more extensively researched by others (mainly in compliance literature, see for example Van Erp, Huisman, Van de Bunt & Ponsaers, 2008). Previous chapters have focused primarily on separation, leaving the *ad hoc* relations to be examined in the present chapter. Thus the focus of this chapter, is on those instances where contact is established between public and private actors. It is argued that, while these – relatively rare – relationships have been conceptualised by some researchers as a form of *cooperation* (see for example Van Wijk et al., 2002), the fieldwork reported upon here suggests that public/private relationships are rather more organised as coexistence.

The following section focuses on formalised structures of coexistence between law enforcement actors and corporate investigators. Section 2 subsequently discusses public/private relationships which occur on an *ad hoc* basis, after which a typology is presented for these *ad hoc* (or as respondents call it, 'case-to-case') relationships. Section 4 focuses on information sharing and the existence of informal networks. A discussion concludes the chapter.

1. Formal structures of coexistence: covenants and public/private partnerships

When it comes to public/private relations, covenants[80] and public/private partnerships (PPPs) are often used as a formal tool to achieve cooperation. A PPP may be defined as a "legally structured form of cooperation between one or more state agencies and one or more private entities, aiming to develop and execute a shared strategy for the realisation of policy" (Hagenaar & Bonnes, 2014: 26). PPPs are used as governance tools by receding governments to "transfer the responsibility for the design and realisation of public service delivery to the private sector through long term contracting" (Reynaers & De Graaf, 2014: 120). In this sense, the structure of PPPs fits well with the ideas of privatisation, responsibilisation and the junior

80 A covenant (in Dutch '*convenant*') is comparable to a Memorandum of Understanding, although it may also be used to create a legal basis to for example share information (Rijksoverheid, n.d.). In this sense, a covenant is more formal than a MoU. For an example of a covenant between public and private actors, see the Electronic Crimes Task Force (Rijksoverheid, 2011). The ECTF is a PPP between the police, prosecution office and banks with the aim to reduce digital bank fraud (mostly external to banks).

partner theory. Since the early 1990s there have been many initiatives for PPPs in the security field (Van Steden & Huberts, 2006). Most of these, however, are focused on physical security (see for example NVb, 2014). The formal goals of these PPPs are often formulated in language of the junior partner theory, with the private partners working towards public good objectives. Private security is seen as complementary to the public police force and is in this sense not considered to be a threat to the state's legitimacy (Van der Lugt, 2001).[81] Such a view point reflects a 'social service view' on private security, in which the private partner is defined in terms of the common good (Hoogenboom, 1990).

There are, however, also PPPs between law enforcement agencies and corporate investigators/clients. Interestingly, these PPPs are focused on types of crimes that are typically committed from outside the organisation: for example attacks on ATM-machines, hacking or skimming (NVB[82], 2016). These are incidentally also the types of crimes that, according to respondents, are reported most often to the authorities (see also PwC, 2017). Interestingly, a similar attempt has quite recently been made when it comes to issues originating within organisations internally. Two pilot projects have been initiated, both with the aim of providing insight into the role private investigation firms might have with regard to criminal investigations.[83] Respondents do not consider these pilots to have been successful. The way the pilots were structured is mentioned as a key factor for this – pilot 1 for example had a very narrow focus, which led to a disappointing influx of cases (Friperson, Bouman & Wilms, 2013). A follow-up pilot (pilot 2) was consequently executed, widening its net somewhat. This has, however, not led to more participation by private investigation firms (Kuin & Wilms, 2015).

Both pilots were meant as a way to formalise the participation of corporate investigators in criminal justice investigations. Prosecutors and police are aware of the general complaint from the private sector that 'nothing happens' with the reports they make to the authorities. The expectation was, therefore, that many private investigators would bring in cases and the choice was made to limit the influx by setting some criteria for inclusion (Friperson et al., 2013). In reality, there was very

81 See also White (2014). The author argues that the same mechanisms are at play when it comes to regulating the sector: because in-house security is less visible and less comparable to the police force than contracted-in security guards, the former are not regulated by law.

82 'NVB' refers to the Dutch banking association [*Nederlandse Vereniging van Banken*], whereas 'NVb' refers to the Dutch representative organisation for private security [*Nederlandse Veiligheidsbranche*].

83 This research has a broad approach when it comes to corporate investigators – private investigation firms, in-house security departments, forensic accountants and forensic legal investigators all fall within the scope of the research. The pilots however, are focused specifically on private investigation firms (and then, only on those which are member of one of two representative agencies and which have a quality mark). For the corporate security sector as defined in this research, working on internal cases within organisations, no formal structures for cooperation have been put into place.

little interest in the pilots from the private side. The target of twenty cases was not reached for pilot 1, settling for eight cases instead. It was therefore decided to expand the criteria for pilot 2 and the target of twenty cases was made (selected from a modest total of thirty cases). The question remains why so little cases were reported to be included in the pilots. One reason may be the narrow focus of the pilot projects on specific crimes and regional police forces. However, the authors of the report evaluating pilot 1 also mention a non-procedural issue: many clients of corporate security do not want to report the case to the police (Friperson et al., 2013). The private interests of the client are in such a case apparently not aligned with the (public) interests served by the PPP.

Chapter 4 of this book has discussed the main reasons for organisations not to report to the authorities (see also, Hoogenboom, 1990). Corporate investigators may (and often do) influence this decision with their advice, however the decision ultimately lies with the client. Whether or not corporate investigators are willing to cooperate thus depends for a large part on the wishes of the client. This focus on the private interest does not fit well with the rationale of covenants or PPPs – private interests differ among clients and corporate investigators representing multiple clients will not easily commit to a structural form of cooperation, compelling them to report all cases fitting certain criteria. As chapter 3 and 4 show, the flexibility of corporate investigators to choose one of many potential venues for (investigation of and) solution to a case is one of the sources for its existence. Additionally, the corporate security market itself is highly competitive. Hoogenboom already described this in 1994. Since his publication, the market has diversified even more, with lawyers also entering the corporate investigations arena (see chapter 2). The *ad hoc* nature of the work, the competition between both investigators *and* clients and all these different and sometimes conflicting interests make uniting the 'sector' in public/private cooperation initiatives very challenging. "The repression of fraud [within the commercial sector] is highly fragmented, almost chaotic even" (Hoogenboom, 1994: 26).

These circumstances make structural, formalised cooperation difficult – only with those corporate investigators who have one and the same client (i.e. in-house security departments), arrangements may more easily be made for long-term cooperation (and even then different parts of this one client may take a different stance). It is therefore not surprising that the covenants described above all have been agreed between public agencies and a specific sector of economic activity (mostly the financial sector). The fact that there is not *one* representative organisation, acting on behalf of the entirety of corporate investigators, makes creating a policy for cooperation even more challenging.

The next section focuses on the instances in which there is contact in one way or another between public authorities and corporate investigators. As may be expected from the above, these contacts concern specific cases, rather than representing any ambition to formalise or institutionalise longer term cooperation.

2. *Ad hoc* relations – coexistence

The nature and composition of the corporate security sector, and the types of norm violations corporate investigators deal with (internal, white-collar norm violations), make long-term cooperation between private and public actors fundamentally difficult. Corporate security/law enforcement relations are characterised by their *ad hoc* nature rather than formalised long-term structures (however, this does not mean there are no long-term (personal or professional) relationships between individuals – for more on this see below). I furthermore argue that *cooperation* is an appropriate term for only a small portion of the public/private relationships, others being more correctly dubbed as *coexistence*. The public and private sphere usually 'keep to themselves' – the low level of reporting to the authorities may be taken as a sign for that (see also PwC, 2017). There is, however, overlap between the activities of corporate investigators and the criminal justice system and in some cases the two meet. Before turning to the different types of public/private coexistence, the next section focuses on public/private relations more generally. The junior partner theory and loss prevention theory provide us with two competing arguments: on the one hand the private sector is seen as a subordinate to a dominant public sector, complementing this sector when necessary (junior partner theory). On the other, the private sector is seen as the private equivalent of the criminal justice system, doing the same types of investigations and providing corporate justice to its client; a strict distinction between public and private cannot be made (loss prevention theory). The two theories are contrasted below and found not to be applicable to the corporate security sector.

2.1 Junior partner theory revisited

The involvement of law enforcement agencies may come about in different ways. One way – the most prevalent according to respondents – is that they are actively involved by corporate investigators and clients, through an official report. Although this could be done during or even before the corporate investigations, respondents indicate that they usually wait until the corporate investigations have been finalised, to report. If, as described in chapter 4, law enforcement agencies are invited in by corporate investigators or their clients only *after* the corporate investigations have

been finalised, these private actors are largely able to give priority to their own goals. As long as law enforcement agencies have not yet been involved, corporate investigators may pursue clients' interests without interference.[84] One could claim a fair degree of autonomy for the corporate security sector here – and the primacy is then located in the private sphere. This autonomy may be diminished by clients or corporate investigators through a report to law enforcement authorities at the end of the investigations. By that stage, however, the organisational problem may have already been solved (e.g. through a corporate settlement) and a report to the authorities may be an afterthought. Reporting to the authorities has little priority for many clients and they are often not very invested in cooperation at this stage. "You see, they [police and prosecution] will deliberate about the case internally, that's up to them, we report and then it's out of our hands. We've done our duty. The rest is their business. Well, as far as responsibility goes I mean" [Respondent 20 – corporate investigator]. From the moment of reporting, the case is deemed the responsibility of the criminal justice system and often corporate investigators are no longer involved.

However, when law enforcement agencies are already investigating at the time corporate investigations have not yet been finalised (either as a result of prior law enforcement action, or as a result of corporate investigators mobilising them during their investigations), then the centre of gravity of the investigations shifts and primacy comes to lay with law enforcement actors.[85] In such a case, the 'junior partner theory' might be considered a useful analytical tool to understand the relationships. As discussed in chapter 1, junior partner theory suggests that private actors are used by public actors as a junior partner to reach the goals of the public actor (Button, 2004; Hoogenboom, 1988). Private security is in this view regarded as complementary to the public police, filling the void left by the police (because of e.g. prioritising efforts). One might say that, according to the junior partner theory, there is a division of labour between public and private, in which the private side is focused on prevention and the public side on repression: the work of private security ends where that of public law enforcement begins. In junior partner theory, the distinctions between prevention and repression and the subordinate position of private security are pivotal to ensuring legitimacy for the private security sector, which is then seen as adding to the goals of the state (public interests) (Hoogenboom, 1990).[86] This distinction between repression and prevention is not supported by the

84 Although other considerations than merely clients' interests may influence corporate investigators in the path they take (see chapter 4 for more detail).

85 Some nuance is warranted here: the moment law enforcement agencies get involved, they are 'in charge', whether that is before or after the corporate investigations have been finalised. However, if the involvement is at a later stage corporate investigators may act autonomously beforehand (and often, afterwards there is very little involvement of corporate investigators).

86 See chapter 6 for more on this issue of legitimacy.

data collected in this research, neither can a clear division of labour be discerned. However, by reporting to law enforcement officials, corporate investigators and clients do cede the autonomy to decide on investigations and settlement options. Especially in cases where the investigations originate in the public sphere by criminal justice investigations, public law enforcement actors seem to be the dominant party, using (the results of) corporate investigations to further the public good by working towards a criminal conviction. Even when corporate security and/or its client take the initiative to involve law enforcement actors in a case, the latter may demand certain things from corporate investigators.

> Look, the moment they [corporate investigators or their clients] come to us to report, things get a little bit easier because we can say: you are the one reporting, so I expect you to cooperate. The moment you report, you can't turn back anymore, that ship has sailed. The employees who are involved, we want to speak with them as witnesses. I could go and track them all down, they might refuse. I can do it all myself. But I can also tell the organisation, look, you make sure those ten people are here next week, we'll be there and we'll interrogate them. Same rules, same level of protection under the law, that's not the issue. It's just making use of the employee/employer relationship. [Respondent 55 – FIOD[87] investigator]

In addition to this 'voluntary' cooperation of organisations, law enforcement agencies may also subpoena information. Corporate investigators may in this way be used by law enforcement actors to do the preparatory work for criminal justice investigations, making the latter less complicated and time consuming for the criminal justice officials, working with scarce means. The same type of reasoning was used to initiate the (not very successful) pilots for public/private cooperation in criminal cases, as discussed above.

That the public side may sometimes be dominant does not necessarily mean that corporate investigators and clients are rendered powerless in such situations. As we have seen in chapter 4, a report to the authorities may be used strategically by corporate investigators and clients. In this way, it may serve the purpose of getting the case investigated in the criminal justice system when corporate investigators provide their report voluntarily. Additionally, keeping the limited resources of police, FIOD and the justice department in mind (especially when it comes to fraud), public-sector respondents indicate that they sometimes demand a certain action from corporate investigators before they decide whether or not to pursue the case:

87 The FIOD is the special investigative unit of the Dutch tax authority.

> FIOD might say to the person reporting, 'that's great that you have found irregularities in the books and you want to start with a clean slate but you need to make sure that your report is substantiated'. So, you basically tell them to do the work. These are big cases, taking up years and the capacity is limited – whether it is the police or FIOD, when it comes to these fraud cases taking up huge amounts of limited resources, if the state needs to do all of that itself... If you can make them do some preliminary work, tell them: it's in your interest that this thing is investigated so you make sure you make a selection for us and substantiate your claims and then we'll see what we can do. (…) Sure they can give us their entire financial administration of the last decade with the comment 'I think there's something off somewhere in there' but that won't really do. [Respondent 54 – prosecutor]

Even in those cases in which the state essentially gives 'orders' to the private party, making them investigate and not accepting an unsubstantiated report, this is not a simple question of public domination. The fact that a pre-selection of the material is made makes the process liable to a steering influence by the private parties.

> The state has limited capacity (and expertise) and when there is a report by a forensic accountant they will at least have a large portion of the information available. Sure, they'll need to do some things to meet the standard of evidence in court but especially when it comes to financial data they're happy to get it. I have heard that they might even take our interview report and just ask the involved person 'is this what you want to say, do you stand by it?' Relatively easy for them this way. [Respondent 36 – corporate investigator]

Although it cannot be ruled out that law enforcement agencies may decide to dig deeper and in another direction after all – indeed, one of the frustrations of both public and private sector respondents is that much investigative work is repeated after a report to law enforcement authorities (Van der Lugt, 2001) – corporate investigators may influence the focus of criminal justice investigations by these means. The junior partner theory therefore falls short in elucidating the more complex social realities of corporate investigations (see also Shearing & Stenning, 1983). Even in situations which may be considered to be directed by law enforcement agencies, corporate investigators cannot be regarded as simple handmaidens to the public sector. Indeed, corporate security firms (and departments) introduce into the public sphere the private interests of their clients (as a reflection of the way that public interests may still be influential in a fully private investigation – see chapter 4).

2.2 Loss prevention theory revisited

Junior partner theory, then, provides little help for public/private relations in the field of corporate security. One may, then, turn to the other popular theory of private security, which is often posed in opposition to the junior partner theory, the 'loss prevention theory' (also known as 'economic theory': Hoogenboom, 1990). This theory is primarily focused on the economic relationships between private security and its clients. The emphasis on loss reduction instead of crime reduction makes for a different focus (private versus public interests). This theory furthermore suggests that the activities of law enforcement and private security (especially private investigators) are similar (ibid.). Although the theory certainly has merit, the situation warrants a more nuanced interpretation. Many investigative methods, for example, are used by both public and corporate investigators (though not necessarily in the same way or to the same extent: see chapter 3); however, the range of investigative activities of corporate investigators is wider (and with new technologies, ever expanding). Furthermore, chapter 4 has shown that, although private interests are leading in decision making in the investigations and settlement processes, there is also room for public interest-type arguments. When it comes to public/private relations, the loss prevention theory emphasises that private security poses a threat to the exclusive position of the state (ibid.). This is the argument that public and private are 'fishing in the same pond' and are in that sense competitors and are (partly) interchangeable (depending to the needs of the person or organisation affected) (Williams, 2005). This is related to the ideas of nodal theorists in the sense that public and private are seen to be competing for the same cases (Wood & Shearing, 2007; Shearing & Stenning, 1983). As respondents suggest, however, this is not necessarily true for corporate investigations, for several reasons.

First, for reasons described by loss prevention theory itself: the range of 'problematic behaviour' which can be the object of corporate investigations is not the same as that which is described as criminal behaviour in the Criminal Code (see also Williams, 2005). For this reason alone, corporate investigators and law enforcement agencies are not (exclusively) working on the same kinds of cases. Traditionally, the criminal justice system has had difficulties responding to white-collar crime in general. There have been many initiatives over the years to make fraud a bigger priority within the law enforcement system (resulting in several different organisational forms, such as specialised teams) and even though a specialised prosecution office such as the *Functioneel Parket* (established in 2003) may boast some success, fraud cases still get relatively little attention from law enforcement agencies (see for example Verhoeven, 2015). The establishment (and disappearance) of specialised fraud units and special fraud contact points is evidence of the uneasy relationship of the police organisation with white-collar crime (see for example Faber & Van Nunen, 2002). This is not to say

that there is *no* overlap – overlap, however, is not the same as corporate security and police being interchangeable.

Furthermore, exactly because of the differences in focus between public and private, the traditional lack of attention for white-collar crime within the state and because of certain 'appealing' characteristics of corporate investigators (see chapter 3 and 4 of this book and Williams, 2005), respondents indicate that many of the cases which are investigated by corporate investigators would not end up within the criminal justice system. Chapter 3 and 4 focus on reasons for organisations to prefer a private solution over the criminal justice process – these will not be repeated here. It suffices to say that working towards a criminal conviction is not a primary focus of organisations. The criminal justice system does not provide the type of solution organisations are looking for and speaking of public/private competition would therefore not do justice to the social realities in the corporate investigations sector.

> That's the error in thinking you know. And it's very persistent in this world. Thinking that private investigations are somehow always a stepping stone to a criminal justice solution. Sure, but those are the exceptions you know. If there's no other way to solve a matter yourself, if the money's gone or out of our reach. Then there's a reason to take that path. But otherwise, no. [Respondent 40 – corporate investigator]

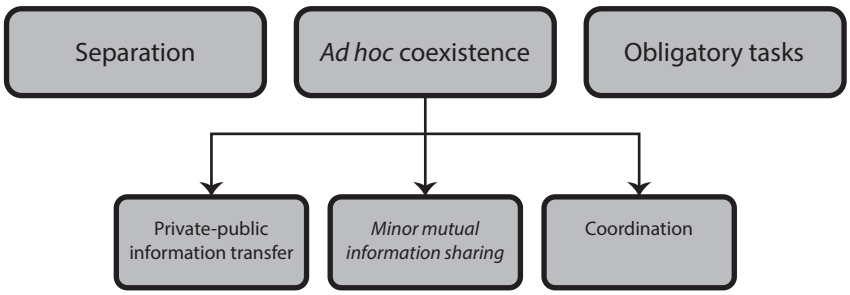
While arguing against the idea of dominance of the public sector (prevalent in the junior partner theory), Shearing and Stenning (1983: 502/503) state that junior partner theory falls short in that it is based on three fallacies: that the private security sector is only concerned with minor cases (leaving police to concern itself with the more serious matters); that it is the police who directs private security; and that the police have more resources to draw upon. Based on my research I agree with these arguments. However, the authors continue to state that the relationship between public police and private security is "a co-operative one, based principally on the exchange of information and services" (ibid.: 503). Button similarly stresses that the private security sector is "centred upon the reduction of losses for its corporate clients through preventative strategies and working in partnership with the agents of the state" (2004: 101), later adding, however, that many fraud investigations never reach the criminal justice system. Most of this book shows that 'cooperation' may not be the best term to signify public/private relationships within corporate security, as corporate investigators largely tend to move predominantly in their private niche. The next section starts with the presentation of a scheme of ideal types (figure 4), which is then elucidated in the following sections of this chapter with the use of fieldwork data.

3. A new coexistence theorisation of corporate investigations

A conclusion based on the above, then, is that public/private relationships are not easily captured within existing theories. Figure 4 is an expansion of Figure 1 presented in chapter 1 of this book, the categories of which may be considered helpful ideal types. Within each category there is a wide range of varieties possible. *Ad hoc* coexistence may mean that cooperation – in the sense of working *together* – may ensue. However *ad hoc* coexistence may very well remain on the very basic level of two parallel investigations, only touching in very minor ways – for example because in the end the private side shares information with law enforcement, without much further contact. In other cases 'cooperation' may mean there is minor information sharing both ways. It is therefore concluded that the term 'cooperation' is misleading when it comes to describing the range of possible relationships between the criminal justice system and corporate investigators. 'Coexistence' is introduced as being a better term instead.

In this section, case studies and interview data are used to examine the types of public/private coexistence more closely. A typology of *ad hoc* coexistence is introduced, ranging from 'private public transfer of information', through 'minor mutual information sharing' to 'coordination of actions'. Case studies derived from the observations are used to illustrate this typology, representing good examples of the different categories of the typology. Similar examples are also present in the interview data.[88]

Figure 4. Schematic representation of ideal types in public/private relationships (2)



88 For type A, discussed in section 3.1, a distinction is made between investigations as a sequence and parallel investigations. This distinction is not made for type B (section 3.2) and type C (section 3.3) because it is not analytically useful to do so. Although (minor or extensive) information sharing might occur after corporate investigations have been finalised (making it sequential), respondents suggest that the information flow at this point usually remains at the level of private information flowing to the public sector. For this reason, the distinction is only made in section 3.1 of this chapter.

3.1 Type A – Private to public information transfer

According to respondents, the transfer of information is the most common way in which public/private relations manifest themselves. Generally, information is transferred to the criminal justice system by private actors through an official report to the law enforcement authorities. As discussed in chapter 4, a report is most commonly done after corporate investigations have been concluded. However, there also are occasions in which law enforcement actors are involved in an earlier stage, for example because there are strategic reasons to do so (most notably because the privately generated information does not suffice and powers of investigation are necessary to reach additional information) (Meerts, 2016). Below, first those (more common) instances in which law enforcement actors are involved *after* the corporate investigations have been concluded are discussed, after which 'parallel involvement' is elucidated.

3.1.1 Private and public involvement as a sequence

Generally, law enforcement will get involved at the final stage of the investigations, preferably after the investigations have been concluded and a report has been made (Van der Lugt, 2001). One of the reasons for this, discussed in chapter 4, is that a well-substantiated report to the authorities is more likely to be investigated by the latter. "For us [the police] it is much easier if a corporate investigator comes to us after he's finished his investigations. And then gives the information to us. Then we won't get in each other's way you know" [Respondent 56 – police investigator]. Corporate investigator respondents indicate that in such cases, they hand over their investigative report but usually the contact between corporate investigators and public law enforcement ends there. "See, the police won't notify me about their progress. I hand over my material to them but they won't call me and say, 'you concluded this from your investigations but we found something else'. But if cases reach court I will attend" [Respondent 15 – corporate investigator]. Much of the information generated by police investigations thus stays unknown to corporate investigators and their clients. Through a public court, case information may be gathered, however not all corporate investigators follow up on these matters.[89]

89 Internal corporate investigators seem more prone to attend court cases of the people they have investigated. This is not surprising, as those investigators who are contracted-in are not paid for this activity. When external corporate investigators do attend a court case, it is usually to act as an expert witness or provide evidence in another way.

Case study 2 – theft of money

In this case, a care-takers organisation discovered that money had been stolen from a resident of one of their care-taking facilities. This organisation decided to report to the police but was told there was not much for the police to go on. Observation Company 1 was contracted to do internal investigations. Before accepting the assignment, Observation Company 1 made clear that chances were slim with regard to proving what had actually happened. In this case, there was no paper trail, no digital evidence or evidence of another kind. The money had been stolen from a vault, to which multiple people had access and there was no process in place to check who had accessed it.

The police were notified after the corporate investigations were concluded but there was no conclusive evidence to report. The person who was suspected of the theft did not confess to it and other information was circumstantial (consisting of statements by colleagues and inconsistencies in the involved person's story). The police were notified and given general information about the case but no official report was made. The police took no further action.

The description of case study 2 above is an illustration of a situation in which police were notified about the results of a corporate investigation, but no official report was made. According to the investigators this was done because police had indicated at an earlier stage they would not investigate and the corporate investigations did not generate enough evidence to change their minds. There was no further contact between police and corporate investigators.

Case study 13 (below) is an example of a case which has been investigated fully by corporate investigators and reported to the police in the end. In the report to the police, the corporate investigators had given a summary of the relevant information, indicating that more detailed information was available when deemed necessary. It was a disappointment to the investigators that police did not investigate the matter, as they felt it would have been 'an easy win' for the police and prosecution. Furthermore, the reason for reporting was that public interest was felt to be at stake, as there was an organised crime network involved, using the same *modus operandi* to defraud several different companies.

Case study 13 – embezzlement through false invoices to suppliers

In this case, invoices to suppliers were altered to contain a different bank account number and website. The money was then paid to shell companies instead of the actual suppliers. The security department of Observation Company 2 investigated the case, concluding in the end that two temporary workers were responsible for the alterations of the invoices. It was suspected by the corporate investigators that the two had been strategically placed in the financial administration department by an organised crime network with the specific purpose to embezzle money with false invoices.

After the internal investigations were concluded, a report against the two temporary workers was made to the police. The report to the police contained the necessary information and was a summary of the report made by corporate investigators. The full statements made by the involved persons to the corporate investigators were not included in the report to the authorities, but it was stated that these 'may be provided upon request'. Privately generated information was transferred to the criminal justice system. The police did not investigate.

Case studies 2 and 13 are examples of privately generated information moving into the public realm by a notification or report to the authorities. In both cases the police did not investigate in the end, which is something the corporate investigators learned from the client. In many cases, however, corporate investigators do not know what happened to a case once they have reported it to the police. As this prosecutor explains this is "because, you know, they're no party in this process. The organisation [client] is. And the organisation will be notified about the process if he wants that and it's his responsibility to report that back to the investigators. We don't do that" [Respondent 54 – prosecutor].

Case study 21, reported on in the text box below, is another example of a report to law enforcement at a late stage. However, the intention of (some of) the corporate investigators here was to involve the police at an earlier stage in order to make strategic use of their powers of investigation.[90] This type of strategic use of public resources has been discussed in chapter 4. Corporate investigators and clients make use of resources available in both the public and the private sphere to get to an optimal result (forum shopping).

90 From the case studies and observations it could not be derived why the decision was made to wait until the end of the investigations (as the investigators of Observation Company 2 did not know). One might speculate however, that the reasons for reporting at a late point in time (such as containing damage and getting a clear overview before reporting) are also valid here. I have no insight in the internal processes within the other company involved, on the basis of which this decision was made.

Case study 21 – theft of electronic equipment

In this case the security department of Observation Company 2 was contacted by the in house security department of another company (being a client). An employee of (a subsidiary of) Observation Company 2 was suspected by the client of stealing laptops. The manager of the subsidiary had bad experiences with the security department of the client company and wanted the corporate investigators of Observation Company 2 to take the lead. These decided otherwise, as the client company was the one affected by the behaviour. The journal indicates that the cooperation between the two in-house departments did not run very smoothly.

In the end, a report to the police was made, however, too late according to the lead investigator from Observation Company 2, who uttered the opinion that law enforcement should have been involved at an earlier stage: "Additionally, there hasn't been a report to the police (yet)! At [date] Investigator of [the client company] did say he would ask the local police to act swiftly but apparently this didn't happen yet. It would have been far better, as far as I'm concerned, to have the police involved, they have the powers of investigation and could have executed a search. Now we are left empty handed. But it is as it is" [quote from the case journal]. In a later entry it is added that "We have given them [investigators from the client company] an update about our interviews and again requested them to make a report to the police. He said he would. We'll wait and see" [quote from the case journal].

Privately generated information was transferred to the criminal justice system. No conclusive evidence has been found to link the involved person to the thefts. The corporate investigators were unable to obtain the stolen equipment because it was (probably) kept in the involved person's house and they are not allowed to enter. For this reason, the corporate investigators from Observation Company 2 were pushing for a report to the authorities. No information is available about whether or not the police investigated the case, nor whether it was prosecuted.

The three case studies presented above are examples of corporate investigators reporting to law enforcement authorities after they have completed the internal investigations. Both private and public-sector respondents indicate that many of these cases are not investigated further by the criminal justice authorities. The presented cases studies are no exception in this regard: they were not investigated by the police or prosecuted (for case study 21 it remains unclear whether there was a police investigation and prosecution).

3.1.2 Private and public involvement running parallel

Involvement of law enforcement agencies at the stage in which the corporate investigations have not yet been finalised is scarcely ever initiated by corporate security or its clients.[91] Respondents indicate that the choice whether or not to involve the authorities is usually made only after corporate investigations have provided information to the client on the events which have occurred. However, it might prove important to involve authorities at an earlier stage, when investigations have not been terminated yet (see also chapter 4). The main reason for this is that the corporate investigations are not yielding the results necessary to solve the problem (see also Gunther Moor & Van der Vijver, 2001).

> If they come to [the prosecution office] during their investigations, it's usually because they can't get to the information themselves and think, the police and the justice department have more powers to get to things they can't get to. For example when they find a missing amount of money which has been funnelled to god knows where, then we have more options to seize the money. [Respondent 54 – prosecutor]

Some cases that are investigated by corporate investigators actually originate from actions by public law enforcement agencies. Stimulated by whistle-blowers, supervisory agencies, tax information and/or criminal intelligence, law enforcement agencies (also including special investigative units of for example the tax authority) may investigate norm violations within an organisation. The organisation in question might subsequently hire (or use internal) corporate investigators to get a handle on the situation:

> We had such a situation in a case, it started with a police raid. We were hired by the organisation to investigate as well. It is very difficult for us in such a situation that the police won't share any information. It depends on the circumstances of course, here there was a lot of political pressure so the prosecutor was very wary. There was no information sharing whatsoever. [Respondent 5 – corporate investigator]

Typically, the organisation will receive no information as long as the criminal investigations are still ongoing, the only exception being the information necessary for cooperation with the criminal investigations (an organisation may for example be informed that a search will be executed on the premises). The organisation in question would therefore have to wait until the criminal investigations have been concluded and suspects indicted, to get more information. This is problematic, as no action can

91 Although respondents indicate that some clients tend to want to report to the authorities right away because it is 'the right thing to do' (see chapter 4).

be taken by the organisation until then (for example dismiss or suspend the people involved). On the subject of this lack of information sharing more generally, and the issues it produces for organisations, this respondent states:

> So what happens when law enforcement gets involved? An organisation may report and they'll tell them the case has no priority so the report is written down but they won't investigate. Or they do investigate and somewhere along the lines it all breaks down or the case is dropped. Or they only take two or three pieces out of the bigger story and the involved person is convicted for that but that's not going to solve the problem for the organisation. Or when action needs to be taken labour law-wise and the criminal investigations take two years, what are you to do with your labour issue? Are you supposed to suspend someone for two years waiting for a trial? And what if he appeals his conviction? So it's all great, saying that it is only the police who should investigate but that's not very realistic. [Respondent 13 – corporate investigator]

In such cases, corporate investigators are often hired to do a parallel investigation, so the organisation will be able to act. Typically, the corporate and criminal justice investigations remain separate and run parallel, without much contact between corporate investigators and law enforcement actors.

> Those investigations run parallel to each other usually. There's no information sharing besides that we give our results to the justice department. At most you may have a collegial conversation about how long their investigations will take, what parts they'll investigate. But we will not be given information. We know more or less what they're doing because through the client we know who they have interrogated etc. They always zoom in at some particular part while the client wants to have the full picture. [Respondent 1 – corporate investigator]

As already commented upon by the respondent quoted above, corporate investigators may still deduce the focus of the criminal investigations without formally getting information from law enforcement actors.

> We have our suspicions of course, because they interrogate people and those people get a copy [of the interrogation report] so through those means we get to know which direction they're taking. And in this case [real estate fraud], we know they are focussing only on some projects but which ones..? We can guess through the questions they ask. But that's not even close to a full picture, essentially we don't really know what they are doing. [Respondent 3 – corporate investigator]

Case study 9 (below) is an example of early involvement of law enforcement actors. Both investigations ran parallel, not sharing information until the corporate investigations were concluded. In this case, although law enforcement agencies were involved almost from the start, the corporate investigations report proved leading for the police investigations. In an informal conversation, an investigator explained that the police postponed most of their investigative efforts until Observation Company 1 provided them with a report of the corporate investigations. In this way, the corporate investigations report served as a guide to criminal justice investigations (being an example of the steering influence corporate investigators may have in criminal justice investigations – see chapter 4).

Case study 9 – employee fraud

An administrative manager used his position to embezzle money. He made false invoices for fictitious bills, while actually investing the company's money on his own behalf. Observation Company 1 was contracted to investigate and reclaim the money. At an early stage, a report to the police was also made, involving law enforcement actors. Initially, the prosecutor did not seem eager to prosecute the matter but eventually the case was investigated and prosecuted. For a large part, the criminal investigations and prosecution were based on the corporate investigations report.

One of the investigators has indicated that the corporate and criminal investigations ran parallel (they happened at the same time), without overlap between them. Observation Company 1 was contracted to investigate internally with the aim of building a civil case and reclaiming money. However, the mission statement of the assignment also states that "[Observation Company 1] will provide assistance in civil actions and a criminal report to the police". In the end the corporate report was used as the basis for the prosecution. Through the report to the police, privately generated information was transferred to the public realm.

As discussed in chapter 4, respondents indicate that when they report to law enforcement authorities with the results of their own investigations, this enhances their chances of the case being investigated and prosecuted. This is no guarantee, however: many cases are still left un-investigated by the criminal justice system (as was the case with the case studies discusses in section 3.1.1). Investigations starting by criminal justice investigations efforts, with corporate investigators getting involved later, often are investigated and prosecuted in the criminal justice system, respondents suggest. As this involves an initial investment of law enforcement actors (which is not the case if a norm violation is initially only investigated by corporate

investigators), this is not surprising. Investigative efforts would have already been made by law enforcement, making the abortion of the case less likely than in a situation when no manpower has been spent on the case yet.[92]

Case study 20 is another example of a report to law enforcement being made early on. In this case, pressure from corporate clients of the organisation led to early reporting. It seems that, as was the case in case study 9, there was no information sharing between the corporate and police investigators up till the point of reporting the crime to the police.

Case study 20 – employee fraud

The organisation of a large store which is part of Observation Company 2 was discovered to be faulty. Among other things there were issues with the manipulation of the rewards structure for sales, items were given away for free to costumers, there were problems with invoices and with the delivery of goods, and signatures were forged. Many of the identified norm violations could not be defined as criminal, but rather as being against corporate policy. All of this led to disgruntled (corporate) clients and the loss of clientele. Through pressure of these clients, a report to the police was made before the corporate investigations were finalised.

There is no mention of Observation Company 2 receiving information from the police. It seems that the investigations ran parallel (from the moment law enforcement got involved) and that the corporate investigators were not informed about the progress of the police investigations. Private information was transferred to the public realm through a report to the authorities.

As the description of the case studies in this section shows, corporate investigations, commencing after criminal investigations have already started, are an addition to the latter, providing the organisation with information and – as police and prosecution are already involved – usually complementing police evidence with additional information, through an official report to the authorities. In these instances corporate investigations may indeed serve as an addition to criminal justice proceedings in the way the junior partner theory describes. In most instances, however, the criminal justice proceeding is initiated at a later point in time as an addition to the private investigations (either after the investigations have been finalised or during the investigations, e.g. when investigative powers are necessary). In this way, the assumptions of the junior partner theory may be considered inverted.

92 This is not to say that cases might not still be abandoned (or put on hold) by law enforcement agencies.

Respondents indicate that this type of information sharing is the most common – law enforcement agencies demanding or simply accepting information but not volunteering it. Investigations run parallel and contact is limited: the two separate investigations coexist. In their own domain, corporate investigators are still autonomous; however, when information and cooperation is demanded from them by law enforcers they will have to comply. In terms of primacy, the centre of gravity therefore lies with the criminal justice investigations. Corporate security is here merely a (very useful) bystander, in no position to demand information in return for their 'cooperation'. "But if you pay close attention to what they [public law enforcement agencies] want from you, you may derive from their questions the focus of their investigations" [Respondent 27 – corporate investigator].

3.2 Type B – Minor mutual information sharing

While the coexistence between public and private actors described above only involves an information flow from private to public, there are cases in which there is some form of (minor) mutual information sharing. "Sharing information, it makes the picture you're painting so much more complete than if we as the police work on our case and for example the bank works on theirs. If they share their information with us and we share ours with them, nowadays we get good results from that" [Respondent 22 – police investigator]. In most instances, the majority of information still flows from private to public, however corporate investigators may also get something in return.

> We get some information, for example they may tell us they want to interrogate someone. That kind of stuff, that they'll keep you in the loop that something is about to happen. Sometimes you get the offer that when everything is done you get together and talk everything over. Never heard from that one again though. You know, information is shared but we share a lot and they share a little. [Respondent 18 – corporate investigator]

Private sector respondents indicate that most of the information they receive is in line with the experiences of respondent 18 (quoted above). Usually it is not very detailed or informative, being more about investigative activities than investigative results. The information that may be shared by law enforcement may be purely meant as useful to corporate investigators, however often it is also beneficial to the criminal justice investigations when corporate investigators and their clients are aware of for example a planned search on the premises, since they may then ensure that the people who have access to certain areas of the building are present.

Case study 1 is an example of this type of coexistence, in which some information was shared both ways. Although the investigators in case study 1 have indicated in informal conversations during observation 1 that they have done their investigations

separately from and parallel to the criminal justice investigations, there was some degree of coordination between public and private, at a later stage at least. It is interesting to note that although the public and private investigations merely coexisted for a large part, both corporate investigators and police investigators felt they were in good contact with each other.

Case study 1 – irregularities with construction tenders

Case study 1 was brought to the attention of the client of Observation Company 1 by a police raid. The police had been investigating for some time already, the organisation being completely unaware of this. No information was given to the organisation about the allegations. Observation Company 1 was approached by the organisation to investigate. From the initial investigations, other investigations followed.

There was no cooperation, investigations ran parallel to each other. After some time, information was shared between the prosecutor and the law firm that acted as the client for Observation Company 1. This information was then made available to Observation Company 1. The information that was shared consisted of a notification that a suspect had been arrested, the grounds for the arrest and the scope of the investigations: "The investigations by the prosecution office are limited (capacity). They'll only look into some dossiers. They will not investigate subject X unless we provide a report about him" [quote from the case journal]. The latter circumstance led Observation Company 1 to speed up its investigations, so police and prosecution could take the privately generated information about this person into account, alongside their own information.

Although information sharing or cooperation was very limited and happened only at a late stage (the prosecutor initially prohibiting this), the corporate investigators felt they had established good contact with the police. For a long time, the corporate investigators were in the dark regarding the police investigations (the same being also true the other way around). The corporate investigators did not volunteer all of their information, because, as one investigator explained, "it is not in the client's interest to have law enforcement access all the information from the much broader corporate investigations". Such access might have led to an indictment of the organisation, as there were major flaws in the control structures of the organisation.

Mention of minor mutual information sharing is far less prevalent than private to public information transfer in the observations, case studies and the interviews. Section 4 of this chapter focuses specifically on the issue of mutual information sharing. This is a pivotal point in much private/public relationships and a source of frustration on both sides. When information is shared by law enforcement authorities,

it usually remains at the limited level described in this subsection, exemplified by case study 1. However, more extensive information sharing also occurs – in this chapter this is called 'coordination of actions'.

3.3 Type C – Coordination of actions

Although *ad hoc* contacts between public and private actors commonly remain at the level of minor information sharing in one way or another, close cooperation also exists, though it is not very common according to respondents (see also Van der Lugt, 2001). In those rare cases, law enforcement actors and corporate investigators work together to get the best results. This may mean that the prosecutor and lead police or FIOD investigators meet with the corporate investigators to talk things over.

> I think both sides can benefit from just talking to each other. And to confer, to learn to trust each other. Say a big listed company finds out at a certain point that they have a corruption issue within their company. That means the company is in trouble, they're going to have reputational issues and the stock value will react but it also has a criminal component. It also brings about an environment that we don't want to have as a society. I think, in a case like that, you can benefit greatly by coordinating with each other early on, getting the full picture, pinpointing the problem, deciding who is going to do what. I can imagine that we will focus from a criminal law perspective on that one employee who has behaved so badly and make a case out of that and that we coordinate with the company and give them the opportunity to put measures in place to prevent it in future. And to inform their stake holders. The company will definitely not be served by us running around in there, searching the whole premises without a plan and exposing them to bad press, we don't want that either. I think you gain a lot by just talking to each other early on. And that's hard, you know, it's hard for us as well, we're not used to sharing information. Or to trust that a company will cooperate. We know these companies as the bad guys. So it's a process. But for the effect you want to produce, it's best to inform each other early on. [Respondent 52 – prosecutor]

As this prosecutor indicates, close cooperation may also mean that tasks are divided between public and private actors. Police and prosecution typically only investigate what is necessary for a conviction. When, for example, fifteen instances of embezzlement have taken place, five may end up in criminal court. Corporate investigators may then – sometimes with the information which has come up during law enforcement investigations – focus their efforts on the remaining ten instances.

> So everybody can do their own thing you know. Let the police and prosecution focus on the person, on the suspect and let the private investigator record the nature and

> scope of the fraud, maybe together with the police and prosecutor especially when it comes to retrieving the assets. Then everybody is doing what they do best with respect for one-another and you just share information based on the possibilities our legal system grants you. [Respondent 13 – corporate investigator]

Case study 11 (see below) is a good example of this type of coexistence. In this case, the specialised FIOD detectives of the tax authority were investigating prior to the corporate investigators. From the beginning, there was much cooperation and coordination between the law enforcement and corporate investigators, coordinating their actions. For a large part, the criminal and corporate investigations were aligned in this case.

Case study 11 – theft of equipment and fencing

Case study 11 came to the attention of FIOD investigators by accident, through a traffic violation. It turned out that the suspect had in his possession some unusual equipment and had unexplained income. During their investigations, FIOD investigators discovered that he was an employee of Observation Company 2. The in-house security department was contacted and after details about the equipment were given, the corporate investigators found the equipment was indeed company property.

From the start, information was shared both ways and meetings were held about the case. For example, Observation Company 2 was brought up to speed prior to the moment that the premises would be searched. This seemed to be both a courtesy call and a necessity, as help from the company was necessary for an efficient search of its premises. Seized administration was investigated by both, and the corporate investigators received information they required from the prosecutor and FIOD. At the same time, the corporate investigators also investigated some matters specifically at the request of the prosecutor/FIOD. Corporate investigators followed the pace of the criminal investigations (moving slower than they otherwise would), to avoid impeding the criminal investigations. Interviews were held only after the involved persons had been arrested and released pending trial.

The corporate investigations were wider than the criminal justice investigations. At a certain point, Observation Company 2 made two official reports to the FIOD. In addition, civil action was brought against two subjects and labour action was taken against other people involved (dismissal, official warning). An audit report was made to identify and fix internal shortcomings within the organisation and (an anonymised version of) the case was published on the intranet of the organisation.

Case study 11 may be considered a rare example of *cooperation* between corporate investigators and the criminal justice system. Although many respondents provide an example of this kind of (more or less) close cooperation, they also indicate this form of public/private relations hardly ever occurs. For example, in case study 11, the prosecutor and FIOD investigators kept corporate investigators closely involved after the discovery that the equipment was indeed company property, in contrast to the usual practice of law enforcement agencies to continue with their own investigations without sharing information with corporate investigators or their client. The role of the prosecutor seems essential for this (see for more on this below). Primacy is not given to either the public or private side in such cases – both conduct their own investigations but keep in close contact and coordinate actions so as to not impair efforts of the other.

> I've had cases in which we could coordinate at the level, 'what are you investigating, what are we investigating', because if you have reported you don't want to impair their investigations. I may for example say, 'we need to finish our internal investigations so we want to interview this person but let me know whether that will be an issue for the criminal investigations right now'. [Respondent 30 – forensic legal investigator/client]

4. A closer look at information sharing

> It would be great if the sector would get a person to contact within the public prosecution office. So we could talk, with all the guarantees of confidentiality on both sides. They have some projects with private investigation firms when it comes to vehicle theft but that's more about what a report should look like to get it to the prosecution. The ultimate would be, we did our investigations, the subject has confessed, the only thing the prosecutor has to do still is to interrogate again with the formal caution. If he [the involved person] confirms that he stands by what he said to us, done deal. Efficient for everyone involved. This isn't always possible of course, sometimes they need to investigate further, use their investigative powers. But that's the ultimate thing, when they can use our report with minor effort for them. [Respondent 1 – corporate investigator]

The above typology of different kinds of coexistence, ranging from wide apart to quite close, revolves in a fair measure around the level of information sharing. For respondents, coexistence, and more specifically 'cooperation', largely revolves around information sharing, rather than cooperation in the broader meaning of the word. In practice, the process of (non) information sharing results in many frustrations on both the public and the private side. Corporate investigators for example feel they are

only providing information, without getting something in return. Contacts with law enforcement officials are often characterised by difficulties, not merely when it comes to the information flow from public to private, but also the other way around.

> Why does it have to be so difficult? Say I want to get in touch with the police detective working on the case – with whom I have talked before! – but I don't have his number. I call the general number but they won't even put me through or give me contact information. I just want to give you additional information for your case and I don't even get to talk to the right person. Why? [Respondent 48 – corporate investigator]

Chapter 3 and 4 have discussed some of the most important reasons for organisations not to report to the authorities. A lack of confidence in the expertise of law enforcement officials is a prominent reason, as is the complaint that reports of 'these types of crimes' (white-collar crime) are not being investigated by law enforcement. Although this is something the majority of corporate security respondents mentioned, some respondents also indicate that they understand why this is the case. This lawyer, who sometimes acts as a client to corporate investigators and sometimes as the investigator himself, feels that corporate investigators should not complain:

> The other day, I was at an investigation firm or something like that and they were complaining that police will not react to their reports. So I told them, of course the state won't act. Why should it care about a 1000 sunglasses that have been stolen, aren't they your sunglasses? Take care of it yourself. Make sure you lock your container properly. You can report it to the government and they can write it up but don't you tell me you expect this copper who needs to make sure senior citizens are not robbed has to go and take care of your sunglasses. And if you have a serious case and they won't act because they don't get it, well then you didn't do your job. Then you'll have to make sure your report to them is better. And that you go to the right place to report. [Respondent 32 – forensic legal investigator/client]

The above quote relates back to the question of which interests are/should be served by investigations. In chapter 4 the normative considerations involved in the corporate investigations and settlement process show that corporate investigators take more into account than the private interests of clients. Similarly, clients may feel that in a certain case, 'the public interest' is at stake and they decide to report to the authorities. As case study 13, discussed in section 3.1.1, shows, this assessment of interests involved might not be enough for the criminal justice system to take action. The general capacity of the criminal justice system is limited – and the capacity for white-collar offences is even less (Beckers, 2017).

Many public-sector respondents are sympathetic when it comes to the difficulties private parties face with regard to getting in contact with them. This public prosecutor for example states: "I can see why private investigators find it hard to get to the right people in the police. And sometimes they even are told that they can't report because they're not the victim but their client is. We really need to get rid of that kind of red tape" [Respondent 54 – prosecutor]. However, respondents also point out that the venue a private party chooses is important in this respect as well. There have been many changes in (especially) the Dutch police organisation in the last decade, which makes it difficult for corporate investigators to reach the right people (because they have been transferred to a different department, because the department was dissolved, etc.).

> We [corporate investigators] want to be informed, depending on the case this will happen. Sometimes they'll tell you nothing, sometimes you're informed when they arrest people, sometimes you read things in the newspapers, and sometimes the prosecutor informs us that the case is pending for trial or that they'll take no further action. This depends on the person of the police officer and the prosecutor. But we find that if we know them from previous cases things run much smoother. Well, we're only human in the end, aren't we? [Respondent 14 – corporate investigator]

One frequently mentioned solution to this problem is to have one central point of communication for corporate investigators (nationally or regionally organised), as also suggested by the respondent quoted at the beginning of this section. In the past, there have been multiple (regional) 'fraud contact points'. In the multiple reorganisations of the police organisation and prosecution office, most of these special points of contact have been abolished. It seems that only Rotterdam has preserved it, which is regarded as positive by respondents from both the public and the private sector.

> It's hard to find the right person within the Dutch police. For me as well. In Rotterdam, we have a central point of contact for fraud cases. They used to be everywhere but in the new police structure they did not return. Rotterdam is the only one who wanted to retain it because it proved useful. I'm sure it will come back in other parts of the country as well. Organisations and private investigators need it, I mean when they come to report and end up at the general desk – I mean the policemen there can write a report but when things get a little complicated they won't know what to do. So it's convenient if they could call a fraud contact within their force. And it goes both ways, I mean it's convenient for me as well if I know who to contact in, say, a bank for formal requests. [Respondent 56 – police investigator]

Special contact points are often mentioned in interviews as a way to improve the communication between law enforcement officials and corporate investigators. As this respondent explains, it takes much effort to get a case to the right person within the police organisation:

> But it means you have to put in a lot of effort because it starts with someone in uniform, then it gets to a department where it stays for a long time, eventually it's kicked over to a different department and every time you need to push the case, ask who is involved, who is working on it. This case ended up at the right place but is certainly not a given. [Respondent 18 – corporate investigator]

Those private sector respondents who have some experience with specialised fraud units within the police and especially with specialised agencies such as FIOD and the fraud department of the public prosecution office (*Functioneel Parket* – FP), are much more positive about these contacts and about the expertise of the public officials than those who have dealt with general police forces and prosecutors. Not only is it the case that these specialised law enforcement actors have expertise when it comes to complex financial investigations, they also tend to be more open to the private interests involved in a case and to have a more comprehensive understanding of the laws regulating public/private cooperation and information sharing. Still, the question remains what the gain in information sharing would be, should there be a central point of entry for corporate investigators. The structural problems for long-term cooperation as set out above also apply to information sharing (although maybe to a lesser extent as information sharing requires less long- to mid-term efforts for investigators). As a case in point one may regard the pilots meant to streamline the use of information generated by private investigation firms in the criminal justice process, mentioned in section 1 of this chapter. To facilitate information sharing on the cases included in pilot 2, a structure for formal, recurrent deliberation between police, prosecution and private investigators was put in place to discuss the progress of cases. The report following this pilot states that for none of the cases included in the pilot this was actually used – instead the (occasional) consultations occurred on a more informal basis (Kuin & Wilms, 2015). Van Ruth and Gunther Moor (1997: 287) have made a similar observation almost two decades earlier in their report on informal information sharing by the police, based on case studies: even for formal information sharing, (pre-existing) social networks and informal contacts are essential. Respondents furthermore indicate that the role of the individual prosecutor involved in the case is essential for whether or not information is shared both ways. The next section explores this role a bit further.

4.1 Ad hoc information sharing with the private sector: the importance of the prosecutor

Whether or not actual information sharing is possible for law enforcement is a highly debated subject. The general opinion of respondents (both public and private) seems to be that there is very little legal leeway to share information with private parties. Nonetheless, some respondents indicate that there actually is some room for information sharing with private actors (see also Blonk et al., 2017). From the interviews and case studies, a picture emerges in which the public prosecutor has a pivotal role in the sharing of information. Police forces are very wary when it comes to sharing information. Just as Van Ruth and Gunther Moor already described in 1997, police officers seem not to be very well-informed when it comes to the rules of information sharing.

> The police are being difficult with these kinds of things. In some areas they are more flexible – because the law does actually allow it when necessary for the repression of crime, the maintenance of public order or whatever, article 19 *Politiewet* ['police law']. So some police know this and know how to deal with it. But others are still: 'no way'. [Respondent 40 – corporate investigator]

The public prosecutor is the leader of any criminal justice investigation. It is, therefore, the prosecutor who should take decisions on whether or not information may be shared by the police. Respondents indicate that the willingness of a prosecutor will determine whether or not corporate investigators may receive information. This is exemplified by the role of the prosecutor in the case studies mentioned above. In case study 11, in which there was extensive cooperation and information sharing, the prosecutor was willing to look for opportunities to not only receive information from corporate investigators but also to return the favour. The journal of the private investigations of case study 11 shows many details of the FIOD investigations. As mentioned before, this situation seems to be rather exceptional. A more common attitude of the prosecutor – one of caution – may be found in case study 1. While contacts with the police were deemed 'good' by the corporate investigators and in informal conversations with the investigators of the case it was indicated to me that police were willing to share information, it was prohibited by the prosecutor. The journal shows evidence of corporate investigators being in the dark with regard to much of the police investigations, as this quote from the journal exemplifies: "[Suspect X] has been arrested, but we don't know on what grounds (it is not about […] though)".

The law regulating the way the police organisation handles information, the Wpol [*Wet politiegegevens*], dictates that in general, information may not be shared with

others than law enforcement officers (article 15). However, article 19 of this law states that there are some exceptions 'when necessary for an important public interest', one of which is the prevention and repression of crime. This will happen under auspices of the prosecutor (article 19 Wpol and article 12 *Politiewet*). In the same vein, the law regulating the use of information gathered through judicial and criminal procedures, the Wjsg [*Wet justitiële en strafvorderlijke gegevens*], indicates in article 39f that information may be shared with persons and organisations outside the criminal justice system under certain circumstances. The heads of the prosecution office, the College of Attorney Generals, have drafted a policy brief on the interpretation of article 39f Wjsg.[93] Nevertheless, the use of article 39f Wjsg is subject to differences in interpretation in practice.

> I think the police should be obliged by law to give us information based on a checklist or something. When the requirements of the checklist are met they should be able to provide information. Now, we do everything, bring them a complete case, give them all our information and we get nothing back. They just say 'we're not allowed to'. But there is a policy brief from the prosecution office which indicates that some information may be given to parties concerned. They have to take proportionality and subsidiarity into account, look whether or not the motives of the party concerned are pure, things like that. So it is possible but the police hide behind privacy regulations. They say 'wait for the court case, you can ask for the information then'. But it will take forever for a case to get to court, and that is if they even decide to prosecute. We need the information now, it's relevant now, we need to take action now. We could be wrong you know, maybe the police will find out with their powers of investigation that it wasn't him, or maybe we couldn't quite get to the truth and didn't get to an involved person in the first place. You need their information then. And they'll say 'we can't give you that, you know this, having a police background'. But it *is* possible. So I called the prosecutor and told him about this policy brief. Well, within half an hour it was in my mailbox. [Respondent 48 – corporate investigator]

The quote presented above shows that not all prosecutors are aware of the guidelines provided by the College of Attorney Generals. Although there does seem to be some legal leeway as described above, the dominant view on both the public and the private side seems to be that the possibilities are very limited. Some police professionals are even unwilling to cooperate with private actors in any way (Van Ruth & Gunther Moor, 1997). However, some respondents indicate that this might be due in part to the fear of – especially – the police to act illegally on this account. "But us police-

93 See https://www.om.nl/organisatie/beleidsregels/overzicht-0/privacy/@86303/aanwijzing-0/.

people, we're just afraid to speak you know. Police-people have the tendency to be afraid to do something out of bounds. One wrong remark to a lawyer and there's a feature in the newspapers tomorrow. So police and prosecution tend to be reluctant when it comes to sharing information" [Respondent 9 – police investigator]. Lack of specific knowledge about the rules exacerbates this reluctance – actors know there are rules but not the details of these rules, which makes them extra wary (Van Ruth & Gunther Moor, 1997: 266).[94] This reluctance is interesting in light of the arguments private sector respondents put forward on a different topic – the fact that they see a discretion deficit in the criminal justice system. As explained in chapter 4, clients and corporate security investigators feel that the sensitive information which they hand over to the criminal justice system might be volunteered to newspapers and such. On the other hand, one of the key features of the corporate security sector is its emphasis on discretion and secrecy (Williams, 2005). This highly-valued characteristic however, seems to be regarded as a bad trait in law enforcement. The fact that it is very difficult for corporate investigators to receive information from law enforcement actors is one of the major grievances of corporate investigators.

> Look, we're bound to regulation as much as they are. Maybe even more. The government has to take the law into account, we have to do that as well but in addition to Dutch law, the law of every jurisdiction we're in applies. And just looking at Dutch regulation – we can't just share information about our clients. So saying they [police] can't share anything and we can share everything is nonsense. They might get into trouble internally within the police organisation, for us it might be a hundredfold worse. So that's no argument not to share. I think we should all try to find a way. And I'm not talking about investigative information about any active cases, I don't want that. I have no use for it and don't want to run the risk of compromising a criminal investigation by knowing too much. [Respondent 10 – corporate investigator]

While there is consideration for this from the side of law enforcement, respondents simultaneously emphasise the importance of such rules, especially for law enforcement information.[95]

94 Van Ruth and Gunther Moor also point to the possibility that this vague understanding of the rules might actually lead to *more* informal information sharing because people then fall back on what they themselves feel is appropriate. The authors were writing at a different time than the one this research is examining and the growing pressure on the police organisation in the last decades might explain why I have found little evidence pointing in this direction. Respondents anecdotally indicate that informal information is now more difficult and less prevalent than before (although, it is possible, of course, that this has to be attributed to nostalgia).

95 This is not to say corporate investigators do not see the value of these rules – many of them state they understand, however they would like (limited) access, based on certain standards.

> We are bound to strict rules when it comes to information gathered through criminal investigations. Which is appropriate because we are bound to be cautious with a suspect's information, that's his right. That's why we're doing the whole criminal justice thing in the first place, otherwise we could just use vigilante justice. It's not like we find it desirable to have someone stand in the square in the scaffold for everyone to mock. That's the thing we didn't want. So those rules are important but at the same time, I do get that the corporate sector feels they are just providing information without getting anything in return. [Respondent 52 – prosecutor]

The situation, described in 2001 by Klerks, Van Meurs and Scholtes – that law enforcement professionals are not quite sure which information they may legitimately share – seems to still hold true. Law enforcement professionals tend to be overly cautious, even though there is some manoeuvre room for them. As this public prosecutor from the specialised fraud office, quoted directly above, continues:

> I am still bound by these strict regulations, but if you try to understand one another and look for each other's interests, then you'll see that there is some room. Within those rules, there are some possibilities left. One important reason for me to share information is when a company has been aggrieved. An aggrieved party has the right to do damage control. And in the context of damage control I can give them certain information, giving them the opportunity to control their damage. It's not the full record of course but at least some parts. And I can for example tell them we have seized assets, so they can try to confiscate that. We can at least give them the opportunity to get the money back in that way. [Respondent 52 – prosecutor]

Much, then, relies on the knowledge of individual law enforcement professionals with regard to the legal framework and on their willingness to cooperate or share information with private parties.

> A prosecutor *can* share information with the person or organisation affected, that's article 51 of the Code of Criminal Procedure [article 51 WvSv]. And information such as 'we found these assets', that won't hurt the suspect [in his defence]. I'm not interested in his personal circumstances, his bad childhood et cetera. So if the prosecutor doesn't want to share that with me that's ok, I don't need to know. So it's possible to share information while respecting each other's position. And I feel it's perfectly normal for a prosecutor to have certain demands, quality-wise, for the information we give them. And I have been baffled for years why this isn't working in practice. [Respondent 13 – corporate investigator]

To summarise, there are formalised opportunities to share information between public and private investigators. Much of the legal leeway in this regard rests on the rights the organisation has as the aggrieved party (in the same way that many of corporate security's investigative possibilities rest on the rights of the organisation as an employer). This provides an additional barrier as some law enforcement professionals do not regard corporate investigators as the ones who are entitled to the information, even when they are explicitly acting on behalf of their client. Discretion on the side of the criminal justice system – often claimed by corporate investigators and clients to be lacking (information is seen to be leaked to journalists) – is a frequently mentioned barrier for information sharing. Many commentators therefore, have expressed the fear that information is shared illegally, through the informal circuit. Section 4.2 focuses on such informal networks.

4.2 Informal networks

Above the importance of 'knowing the right people' has been touched upon. As a result of the law enforcement background of many corporate investigators, there are many long-term connections between corporate investigators and law enforcement professionals (Williams, 2005). The networks existing between (public and private) investigators are subject of much debate. One recurrent theme in literature is the danger of old boys' networks (see for example Hoogenboom, 1988). This concept comes down to the informal use of contacts between former police officers, now working in the private sector, and their former colleagues (Van Ruth & Moor, 1997). The term 'old boys' network' has a negative connotation and is usually used to signify the misuse of former contacts to get to information one should not have. Despite the concerns which are voiced frequently, there is little evidence of misuse of contacts occurring regularly (Klerks, Van Meurs & Scholtes, 2001).

Although it cannot – of course – be absolutely ruled out that illegitimate use of contacts takes place,[96] respondents stress the counter-productiveness of such an approach for the goal they want to reach (which is, finding a solid solution to problems). Pragmatically, the utility of any 'grey' information that might be given by police to corporate investigators would be strictly limited, as it cannot be included in any reports compiled by the latter. "Should they [the police] give us information we shouldn't have and the truth comes out, they're in trouble. Plus, it's useless to me anyway. If I get information I'm not allowed to use, well it's nice to know but what good does it do me? We both know this. So it's pointless to try and get informal information" [Respondent 15 – corporate investigator]. Although utility may be limited as a recognised source of

96 Recently, the court of Oost-Brabant has ruled that a police officer had illegally accessed police systems to gather information for a former colleague (see ECLI:NL:RBOBR:2016:7193). These kinds of cases are rare though.

information, illegitimately obtained information may still have value as a starting point or a general direction for corporate investigations. In this sense, illegitimately obtained evidence may have a purpose for corporate investigators (and law enforcement alike). From a strictly rational point of view, illegitimately sharing information may sometimes be beneficial and sometimes be harmful. Interestingly, both public and private sector respondents stress the counter-productiveness of illegitimate working on the longer term (by tarnishing their and the client's reputation) and the fact that it is 'morally wrong'. We may discern the non-contractual moral agency discussed by Loader & White (2017) and at various points in this book. The principles of law used as guidelines for corporate investigations may produce a (moral) consciousness for corporate investigators, leading them to weigh pragmatic and normative considerations at different stages of their professional activities. As this corporate investigator states: "you need to protect each other in that sense and make sure you don't do anything compromising to yourself or the other" [Respondent 40 – corporate investigator].

> I have cut my ties with former colleagues, I don't want to get anyone in trouble. Leaking information from within the force will cost them their jobs. I have a lot of friends and family there but you shouldn't ask for information they're not allowed to give you. And besides, that information is useless. I can get much more valuable information from the internet than from the informal circuits. [Respondent 48 – corporate investigator]

Many respondents stress this duality of, on the one hand finding no use for illegally obtained information, and on the other not wanting to risk the permit (in the case of private investigation firms) or more generally their own reputation. Chapter 2 has shown that many corporate investigators claim commitment to the rules as not to jeopardise their good reputation.[97] At the same time, they also indicate that they believe there are (mostly small firm) investigators who do illegally obtain information.

> If one of our investigators would obtain illegal information, that's it for him – he's done. Immediately. Leaving aside that the client wouldn't be served with it anyway, on the contrary it can only do harm. It will be no help to you. But I'm sure it happens. There are enough little investigation companies who use their old police contacts to get information. [Respondent 41 – corporate investigator]

97 In this manner, the 'non-contractual moral agency' of corporate investigators also has a more instrumental side: a good reputation is essential for the commercial survival of the corporate investigation unit.

The same goes for colleagues working in other parts of the private sector, also belonging to the (old boys') network:

> Private-private cooperation is just as interesting I think. Cooperation and information sharing are important issues there as well. There still is regulation for it of course but it's somewhat less strict than when it comes to public/private. And there is a large willingness to cooperate within the legal boundaries when you really need each other. There are a lot of people with the same background in most in-house security departments. There are many informal contacts. Some people might call it an old boys' network but I don't like to call it that. I have said from the very beginning, when I came to work here and also when I had a managerial role: I don't want us to embarrass former colleagues. It's no use and it will *always* catch up to you, it will only bring you trouble. I just don't want that. But within the legal possibilities you can still do a lot. If you know people well, when you trust them not to abuse the information you give them, you might step over the line every once in a while, into a grey area. But only when we know that the person providing the information, the person getting the information and the person whose information it is are all in agreement. For example: at a certain point I got a call from someone within our organisation, he had found a wallet and wanted to return it to its owner. But he didn't have a clue who that might be. There was a ATM card in the wallet. So I called my contact with that bank and explained why I wanted the information and asked if he could give me the address. Strictly speaking, he's not allowed to give me that kind of information because of privacy regulation. But it was obvious what we were going to do with it and because it was done in the context of service provision, he could defend his actions. And of course we'll tell the person who is involved how we got his information. He's only going to be happy with it because he got his wallet back. [Respondent 46 – corporate investigator]

Interestingly, this respondent is very critical of informal/illegal information sharing, but at the same time he admits to sharing some information with 'pure intentions'.[98] When the person with whom the information is shared is trusted and the person whose information is shared is not harmed but actually served by the action, the willingness to 'move into the grey area' seems to be greater. This may be a result of the focus of corporate investigators on normative considerations and principles of law rather than on formally defined laws: since they focus on (legal) principles, rules may occasionally be broken in order to make the principles prevail. Respondents also indicate that they sometimes warn current employers about a former employee, either in the context of a pre-employment screening or on their own account. Although the information

98 Interestingly, had the bank employee contacted the person instead of the corporate investigator of the organisation who found the wallet, there would have been no privacy issue.

shared usually stays along the lines of very vague insinuations – being careful not to actually give information – this is usually enough to set off alarm bells for the current employer. One could therefore definitely argue that this type of informal information sharing crosses the line of what might be allowed by privacy regulation. In the same vein, this police detective states that he may sometimes move into a grey area to try to help.

> In my experience, with the private investigators I have dealt with, they know how to report. Nine out of ten of these guys have been a police detective so they have the experience. I have to say, that's good. They know how things work around here. And they might come here to discuss a case kind of off the record, like what are the options, see where we stand. Their client does not always want to give the information to the police. But when they come here like that, it's confidential. And we know that there are situations which are on the edge with regard to what you share with each other. But you have to know each other then. Trust is the basis of everything. The contacts we have with private investigation firms, with banks, you know each other and at a certain moment you know that you can trust the other not to abuse the information given to him. If I say 'this is a blue cap but it is supposed to be a red cap but you shouldn't know that', they will not use that information. Because the second they do, it is done. We are restricted by laws and everyone knows that. And the other way around a private investigator might say 'I have this information and my client does not want you to know but here it is'. Because he might have to give us that information to get his case together. We won't record it then but we will try to do some things to help each other out. Within limits. [Respondent 56 – police investigator]

Interestingly, because of the general lack of knowledge on what may be legitimately shared, information that is regarded to be in the grey area, may actually be legitimately given to an organisation who is considered to be affected by the norm violation (making the information transfer, thus, legitimate). Whether information is shared legitimately or illegitimately, trust seems to be a key factor.

> [That cooperation] was also more based on contacts, [Investigator] has a police background. He indicates 'it is a small world. You share information because you know you can trust one another and you won't get each other into trouble with your actions. [That part] is not based on rules and laws or guidelines. I know what I can share with the police without giving them information that would harm their case. This is why they trust me and why we can share information. When you trust each other you put effort into it and you make it work. But we more often come across situations where nothing is shared in the name of privacy. People then say that privacy legislation

> prohibits information sharing but that's not necessarily the case, you have enough room. I call that a fear to burn yourself on cold water [CM: you're afraid you break the rules but there is no rule to break]. Then you hit a wall right from the start.' [Excerpt from observation 2 – informal conversation]

Respondents (both public and private) generally indicate they are wary of illegal information sharing. In their 1997 publication Van Ruth and Gunther Moor (1997: 152) state that their respondents feel that 'the heyday of the old boys' network is over'. The authors describe a situation in which especially police officials have become more and more careful and aware of illegitimate information sharing. This incidentally seems to work both ways: it is not merely a matter of the risk of corporate investigators trying to get easy access to classified information, but also of law enforcement professionals trying to get to private information without having to go through the (cumbersome) official criminal justice channels. This is what Marx (1987) calls the 'hydraulic principle': the outsourcing of 'dirty work' by police to the private sector.

> It works both ways – I don't want my people to just give information to the police either. The reason for this is that we are also bound to discretion to our clients. So I tell the police, you need to be careful not to sabotage your investigations in that way. So make sure you ask me for information through the formal channels and summon the information from me. But what does happen are yes/no questions, as I call them: so they might ask us 'we have found this, does it look familiar?' 'Would it be useful for us to subpoena this information?' And answering that is also sort of a grey area but still on the right side I think. But if you're strict you'd have to say without a subpoena I'm not giving you anything – which makes it a very slow process of course. But in the end and above all, you don't want to impede the police investigations on the grounds that formal procedures have not been followed. [Respondent 14 – corporate investigator]

Law enforcement agencies are regulated by the laws mentioned before when it comes to information sharing with others. This is not the case for corporate investigators, however, they do have to comply with privacy regulations and often there is a duty of confidentiality towards the client. With a formal subpoena from a law enforcement agency, these duties are overruled and corporate investigators and clients need to provide the information demanded by law enforcement. Respondents indicate that they are careful not to 'over-share': they hand over the specified information but not more than necessary (as was the case in case study 1, explained above).

Other than outright illegal information sharing, the above quote shows there are certain grey areas in which, technically, there may be no information sharing but information may still be gathered. This kind of general, or what respondents call, 'directive' information seems to be the most valued and sought after in public/private relations. For both public and private investigators, who are focused on their own investigations, it is valuable to know whether they are 'on the right track'. "We don't need operational details, it would be very helpful if they could just give us directive information. Just to let us know whether we're on the right track" [Respondent 48 – corporate investigator]. The type of information sharing 'in the grey area' referred to above generally stays within this category respondents suggest. The police detective quoted above continues:

> I think the type of information that a private investigator wants is directive. It shouldn't be cardinal information, that's just not allowed. But you may help them a little, say 'you have to go right or left'. They might ask you, 'what are your thoughts about this case'? I think you may help each other in these minor ways. But it depends who you ask. If you ask some other police detective they might tell you 'look the private investigator hands over his information [by an official report] and I will use that in the criminal justice procedure and that's that. We won't discuss it because I can't'. I guess it depends on your private beliefs as well. But I think we accomplish the most if we just discuss matters and try to trust each other. [Respondent 56 – police investigator]

Informal networks have an additional purpose, other than sharing information. Former colleagues in law enforcement agencies may be used as a point of reference for 'procedural' questions such as where to report a specific case. Having a wide network of (former) colleagues may provide both corporate investigators and law enforcement actors with an easy entrance. It is not always clear to the corporate investigator where a case should be reported:

> Or the question is, is this a police case or a FIOD case? We'll search for the best place for the case to go and yes you may use your network for that. Making contacts, having an informal conversation whether or not they might be interested in the case and whether they have the space to do it, what would be the timing of the investigations, which information do you need, what can we do for you here. But these are the bigger cases and luckily these are scarce. [Respondent 38 – client]

Above, the difficulties corporate investigators have to 'get to the right person' within for example the police organisation have been discussed. Having a former colleague there might help with that.

> It matters enormously. I still cannot enter a police station in the larger cities without running into someone I know. It makes for an easier conversation. But the same goes the other way around. Every once in a while, we help former colleagues when they run into something they don't understand. I think at a professional level there should be room for such a thing. But it doesn't mean we actually share information with each other. [Respondent 41 – corporate investigator]

In this way, both public and private actors benefit from the networks forged between them. Turning briefly to information sharing and informal contacts between (corporate) organisations, one may conclude that the same goes *within* the private sector. It may happen that multiple organisations turn out to be involved in a certain case. Case study 21 is an example of this. In such instances, it may prove very helpful for investigators to know the investigators involved at the other organisation.

> There also are contacts with other colleagues who do the same work for other companies. Not everything is black and white, there's a large grey area and it's important that you cross no boundaries. For example, I got the urgent advice from a colleague from a telecom company to tell the police they should subpoena the telephone records of a certain number because there were some interesting leads there. No sensitive information was shared but now we were able to tell the police, go and check it out. Well, it took months but they did look into it and they arrested the guy in the end. [Respondent 18 – corporate investigator]

Nevertheless, there are also plenty of reasons for private actors *not* to cooperate with each other (Hoogenboom, 1994). From a commercial point of view it is prudent not to share information with competitors. Interestingly, however, respondents indicate that they do share basic information within their informal networks. Respondents stress that no personal or specific information is shared here about individuals, however, *modus operandi* might be shared. In this way, corporate investigators may benefit from each other's experience: "I have a vast network of other security managers of other companies and we talk and now and then you hear something about drivers being robbed or something like that" [Respondent 15 – corporate investigator]. Mostly though, and similar to the information sharing between private and public, information sharing between private actors seems to be limited to a certain case in which both actors have a stake (such as case study 21).

Informal (and formal) contacts between public and private and within the private realm are thus not just important for (incidental) cooperation, but have value for the finalisation of investigations as well. Having contacts and knowing people works to create trust and 'goodwill', which are essential to get things done within large organisations (Hoogenboom,

1994). The room granted by the legal framework will still be useless if no-one is willing to make use of it. As discussed above, the willingness and knowledge about the rules of individual police and prosecutors is essential in information sharing. It is important to note at this point that one cannot simply speak of 'public law enforcement' or 'the corporate security sector' in this sense: within both the public and private sector many different opinions, interests and connections make public/private coexistence either easier or more difficult (Yar, 2011: 11).

Discussion: public/private relationships and information sharing as a source of frustration

This chapter has discussed the relationships between public and private actors in the field of corporate security, defined here in terms of coexistence rather than cooperation. Despite the good intentions which seem to be present in both the public and the private realm, there is very little actual cooperation taking place. For reasons presented earlier in this book, many organisations prefer to keep the corporate investigations within the private sphere. In those cases that public law enforcement *is* involved – either *ex officio* or by a decision from the involved organisation – the contacts between public and private often still remain very limited. This chapter has given some examples of cooperation – however, respondents indicate that usually the formal contacts between public and private go no further than corporate investigators presenting information to law enforcement agencies through a formal report to the authorities. As such the term coexistence may be better suited to the mutual relationships in most cases.

One consequence of this limited contact is that there is no clear notion within Dutch law enforcement agencies with regard to the corporate investigations sector. Neither the width of corporate security's activities, nor the number of investigations done by corporate investigators, nor even the size of the sector, are manifest to law enforcement actors. "We have to accept that we don't have insight into that. No, we don't know. We see it when people come and report, then we know. And sometimes you see it from the side lines. But that doesn't come close to a full picture" [Respondent 52 – prosecutor].

> I think, if I am being completely honest, that it is one big black hole for us (laughs]. Maybe there are people in the FIOD who think they know but I wonder how they would know. There's not a lot of [scientific] research on it. Keep in mind that we are present in two fields – you may report either to the police or to the prosecution, so there's a difference there. So we don't even know from each other [police and prosecution] how many corporate reports there are. We are involved more than usual

> because we have a close cooperation with the prosecution office [on fraud]. But I have no clue whatsoever on how much [corporate] settlements there are. No. How should I? Especially when it goes through civil court or they keep in internal. We keep an eye out in the papers and we might get a nice case through those channels. And then they [organisations] say 'but we handled it already'. Sure, but I'm going to have a look anyway. But that is through the newspapers. How else would we know? There's not much more we can do. And I have to say – we are swamped with fraud as is so we are a bit reluctant to actively search for more. [Respondent 55 – FIOD investigator]

Law enforcement respondents generally only have some experience with corporate investigators, in specific cases. Their overall opinion of the corporate security sector may be considered to be rather positive.[99] "My experience is that their investigations are good. I don't think they just speak to the liking of their client. They know that that'll be the end of them getting assignments" [Respondent 9 – police investigator]. However, this is based on only very limited contact with corporate investigators.

Partly, this may also be caused by the scattered nature of the corporate security sector and the low level of control that is exercised by the state, as described in chapter 2. All of this has some consequences for the public/private relationships (which are often characterised by frustration rather than cooperation) but also for the use of information from corporate investigations in criminal justice procedures. Although reports and other information from corporate investigators may be used in criminal court, not all law enforcement actors feel comfortable doing this. As shown above, the pilots aimed at simplifying the use of this type of information by the police did not prove overly successful. Although public law enforcement respondents are generally rather positive about corporate investigators, they remain wary when it comes to the information gathered by them. "Those private investigators, they don't have to follow rules. We can use the information because it's handed to us, we don't have to wonder whether it's obtained legitimately. Of course, [if we're going to use it] we check the evidence, whether it holds up to the burden of proof in a criminal case" [Respondent 21 – police investigator]. This quote refers to the situation that criminal justice officials may make use of information provided to them even if this information is gathered in an illegitimate way (Blonk et al., 2017). This is discussed in more detail in chapter 4. Even though illegitimately gathered information may therefore *formally* be used in the criminal justice procedure, many law enforcement respondents do not feel comfortable with this. The consequence of this attitude is that in most cases, much effort is put into checking the information provided by corporate investigators. Often, respondents suggest, a full-

99 Possibly this is a rather new development, as literature often shows a negative stance from law enforcement professionals towards the private sector (c.f Hoogenboom, 1994). See with regard to the image of the private security industry more in general *inter alia* Thumala, Goold & Loader (2011).

blown criminal investigation follows, which repeats much investigative efforts by the corporate investigators in the context of criminal law. Many corporate investigators have expressed their frustration about this, as they believe it is unnecessary. Public-sector respondents on the other hand indicate that they are concerned that possible illegal actions of corporate investigators are being used to obtain information. This is a concern voiced in the literature as well (see for example Hoogenboom, 2006). The case law leaves room for the use of illegally obtained evidence: illegally obtained evidence may be used, as long as police and prosecution have not been involved in the gathering thereof.[100] Regardless of the admissibility in court, many law enforcement professionals feel uneasy when they have no insight into how the evidence is gathered, leading them to either dismiss the information from corporate investigators or to reproduce it 'the right way'. "Sometimes I get a private dossier, you know when a case has been investigated by a private investigator, and we will see what they have done. Often we need to repeat the entire investigation to give it the proper legal grounds" [Respondent 22 – police investigator]. This will take a lot of time and because many corporate investigators are quite pessimistic regarding police expertise when it comes to white-collar crime, corporate investigators often feel it is a waste of time and resources. This, adding the fact that the case, once reported, is out of their hands makes for an uneasy relationship between public and private in many cases.

Interestingly, one of the assets valued most by clients when used by corporate investigators, the use of discretion, is a source of frustration for corporate investigators and clients when used by law enforcement professionals. Information sharing is often a rather awkward process and the direction is one-sided: from private to public. Corporate investigators and clients complain that once a case is being handled within the criminal justice system, it will become public knowledge – the criminal justice system is seen to suffer from a discretion deficit (Williams, 2005). However, in public/private information sharing, corporate investigators complain that law enforcement professionals use *too much* discretion in the sense that the information sharing from public to private is often minimal to non-existent. This focus on discretion on both sides complicates public/private relationships further.

On the public side of things, law enforcement actors often also feel frustrated with public/private interactions. Many corporate investigators, having a law enforcement background, think they know police procedures but actually end up harming

100 See for example ECLI:NL:GHSHE:2006:AY1071 (ruling of the Court of Appeal Den Bosch). In its ruling the Court decided that as the police had not been involved in the gathering of evidence, they did not have a directive role in the actions of the private investigators. It is noteworthy that in this case the evidence was not obtained illegally but the legal representation of the defendant expressed concerns because his client had not been interrogated by the police but interviewed by private investigators (leading him to be protected by less legal safeguards).

the criminal investigations by being too proactive. An example of this is that the documents provided by the corporate investigators may have a certain classification of the offence, while the prosecutor wants to indict the suspect for something else (e.g. because that will provide a stronger case).

> What I don't want them to do is to qualify the behaviour for me. They might think the case is about falsifying documents but I might want to charge the suspect with something else. So I'd say stick to what you know, you see that this person has wrongfully taken money, let me worry about what crime it is. [Respondent 51 – prosecutor]

When all documents provided by corporate investigators contain an (erroneous) legal qualification of the conduct, this may present the prosecutor with problems in court as the defence may use this against the prosecution, respondents suggest.

In the same vein, law enforcement respondents indicate that although they mostly think corporate investigators cooperate quite well with them, they sometimes volunteer only certain information and 'are being difficult' with other information.

> When they themselves report, they'll cooperate because they want the case to be investigated soundly. But if we stumble upon something, for example in another investigation, their interests might be different and information 'might get lost'. They might not want to report the case to us officially and then it gets more difficult to get your information from them. [Respondent 21 – police investigator]

Under circumstances, this may lead to a feeling of being used for a private agenda and as a tool to get certain information through the use of law enforcement's investigative powers. As stated before, corporate investigators and clients might not always volunteer all information in a certain case. Law enforcement might still subpoena the information – but for that to be possible, the prosecutor must be aware of the existence of the information.

> What we volunteer to the outside world is not necessarily the full story of course. It also depends on in which country it all takes place, on the reach of legal privilege etc. Part of our strategy is answering the following questions: what should be the role of our lawyers and when should we use them and what exactly is protected? That doesn't mean that in certain countries you may not be forced to hand everything over anyway. And of course you don't want to write down any nonsense but you also don't want to for example involve people who were only at the side-lines in all of this and get them into trouble. [Respondent 37 – client]

The distance and misunderstandings between law enforcement actors and corporate investigators hampers cooperation, as much relies on trust and familiarity. Pre-existing contacts are important, not just to get information from one-another but also to 'get things done'. Knowing the right people in the police and prosecution organisations means for corporate investigators that they may find a capable person who is willing to take on their case. For law enforcement officials it means that they are more ready to trust the information provided to them. Additionally, relationships of mutual trust help to cut red tape on both sides of the fence. Of course, the danger of moving into a grey area or even outright abuse of (informal) networks is a real possibility in this context. However, only anecdotal information about such abuses can be found. Respondents do indicate that they sometimes move into the grey area ('with good intentions') and that they are sure some illegal information sharing exists. None of the respondents could point out a specific example of this though.[101]

A conclusion of this chapter is thus that even in those instances where public and private meet on a *ad hoc* basis, the prevailing situation is that of coexistence rather than cooperation: once a report *has* been made, that does not necessarily mean that cooperation will occur. Many instances of what respondents call 'cooperation' are more accurately defined as private actors handing over information to public actors ('type A' discussed in section 3 of this chapter). The pilots discussed earlier come to the same conclusion: "in practice there is no cooperation. (…) Specifically, the 'cooperation' is about investigative reports being handed over by private investigation firms to the police' (Friperson et al., 2013: 48). Cooperation in the sense of coordination of actions and mutually sharing of substantial information remains the exception. First, it is made rather difficult by law on the public side, and by law and by codes of conduct on the private side. Additionally, the forms of information that might potentially be shared may practically be usable only within the context in which they were generated. Finally, contradictory time-orientations and attitudes to ensuing publicity of on the one hand corporate security as defined by its clients (valuing a quick resolution and limiting publicity and potential reputational damage) and of public law enforcement (wanting a watertight case and quite tolerant of publicity, for reasons including deterrence) on the other, limit the opportunities for working in tandem (Gill, 2013). The reluctance of law enforcement officials to share information with corporate investigators (while sharing the case with the general public in the end through a public court case) further hampers cooperation.

101 Of course, it is impossible to tell whether respondents tell the truth about this sensitive subject. However, there are very few court cases involving illegal information sharing between corporate investigators and law enforcement professionals and in the observation settings – in which I had full access – no evidence of such abuses was found. This nevertheless does not necessarily mean that it never occurs.

In this chapter we have seen that efforts to cooperate in a structural manner are scarce when it comes to internal norm violations. Additionally, those efforts that do exist seem to be quite unsuccessful. The reasons for this may be found in structural and cultural characteristics of the corporate security market. Most notably, the fragmented nature of the corporate security market, the diffuseness of interests involved and the fact that, in the end, it is the client who decides about involving the authorities, make long-term cooperation very difficult. Corporate security as a market thrives by the grace of its use of flexibility in the framing of economic crime; secrecy, discretion and control; and legal flexibility and responsiveness to clients' needs (Williams, 2005; Meerts & Dorn, 2009). The market exists *because* of the possibility of separation from and coexistence with (and sometimes strategic use of) law enforcement. Indeed, corporate security professionals consider the criminal justice system to be unable to provide solutions to the problems at hand: bringing in law enforcement serves a purpose (from a private point of view) only when a client feels that it has been so much hurt that there is a need for retribution, *over and above* the (otherwise more efficient) corporate settlements available. Additionally, in some cases there are strategic advantages which make a report to the authorities an appealing option. Generally speaking however, respondents do not seem to have high hopes with regard to the criminal justice system. As shown in chapters 3 and 4 this is one of the reasons for the existence of a corporate security sector: corporate security can coexist with law enforcement agencies because it markets services which only partly overlap with the criminal justice system.

Similarly, law enforcement respondents have indicated they would like more cooperation. At the same time they are generally pleased with the work of corporate security and the existence of the sector. Although most would like to be informed, this does not have to be shaped as a formal report. A well-substantiated corporate investigation report may make police investigations significantly easier, especially in cases involving complicated financial matters. Nonetheless, certain actions based on their powers of investigation remain necessary for law enforcement actors – for example to interrogate the suspect within a formal interrogation setting. Formal, long-term cooperation with corporate investigators would provide considerably additional work for a police (and prosecution) organisation not very well equipped to deal with the kinds of norm violations corporate security deals with, without necessarily yielding successful results.[102]

102 The special fraud department of the prosecution office (*Functioneel Parket)* and the investigative service of the tax authority (FIOD) are the exceptions here. However, there also is a limit to the amount of cases these agencies may handle. Furthermore, more cases brought to trial would also increase the pressure on the courts and judges to both handle more cases and get specialised knowledge.

To conclude, both the public and the private security sectors seem to put much emphasis on 'cooperation' but contacts generally remain at the level of coexistence.[103] Although this was not a specific focus of this PhD research, interviews with public and private sector respondents seem to point towards a certain ambivalence in this regard. Following the train of thought of Thumala, Goold and Loader (2011), one might put this in the context of a search for legitimacy. Although the authors are writing about the private security sector more generally, some of their observations might hold true for corporate investigations as well. In its search for legitimacy, corporate security uses "symbolical borrowing as a (self) legitimating device" (ibid.: 295). The authors furthermore state that "the importance of this [public/private] partnership narrative lies in its implication that all members of the extended police family share similar values and can draw on the same reservoir of public support. The fact that the industry offers post-retirement employment to many ex-police officers reinforces this idea" (ibid.: 294). Interestingly, many corporate security providers try to steer clear of any analogies with the public police, as we have seen in chapter 3. This mechanism might therefore be less pronounced than in the wider private security sector.[104] However, when it comes to public/private relations it is striking that the public/private partnership narrative seems on the one hand quite tenacious but on the other does not yield any tangible 'results'.

103 See also the 2017 New Years' blog of the president of the NVb mentioned in chapter 1 (http://www.veiligheidsbranche.nl/blog_voorzitter_nl.html).

104 Corporate investigators for example do not have identifiable uniforms which mirror those of the police. See also White (2014).

Chapter 6

Conclusion and discussion

Revisiting the state-centric discourse

Introduction

The purpose of this research is twofold. First, it aims to take the corporate security sector out of its state of relative invisibility by describing its day-to-day activities, the rules regulating corporate investigators' professional behaviour and the composition of the field. Second, the research focuses on public/private relations. In doing so, it provides an alternative to the state-centric discourse used in most criminological literature by focusing on the semi-autonomous role of the corporate security sector. The research brings extensive qualitative empirical material into confrontation with a number of theoretical perspectives that have been articulated within criminology about private security – most notably, junior partner theory, loss prevention theory, nodal theory and the anchored pluralism perspective – and finds the closest 'fit' to be with what Canadian criminologist James Williams (*inter alia* 2005) has described as the commodification of the dark number of economic crime (Williams' 'juridification thesis'). Underlying all those criminological streams of work we can discern both a focus on the state as the (implicit) point of theoretical departure, and a common commitment to democracy and transparency. Although the former is not part of the perspective used in this research, the latter is. This research advances those values by interrogating the practices and values of the corporate security industry, making recommendations for reform. The corporate security sector acts with a high degree of flexibility within the semi-autonomous social field, both in relation to investigative activities and in relation to other actors. In this context, the state remains a key player, by adding a normative ('retribution') dimension to corporate settlement solutions and as the source of democratic control over the market. My perspective may, then, be regarded to be a reconsideration of the state-centric discourse, one that takes the semi-autonomous position of corporate investigators as the point of departure, while also being sensitive to the role of the state.

From the descriptions based on the research data, some cross-cutting themes emerge. This concluding chapter takes a closer look at these, while answering the research questions and, additionally, explores some directions future research on corporate investigations and corporate settlement might take. To reiterate, the research questions motivating this research were as follows:

Central research question

What is corporate security, how can its shifting relationship with law enforcement be conceptualised and what is its significance for the wider society?

In particular:

1. What are the raison d'être and methods of corporate security in providing corporate justice?
2. How does this stay within – or breach – regulatory/legal frameworks?
3. How wide, in practice, is the sphere of discretion for corporate security, either to act alone, without informing public law agencies, or to inform and possibly to task them?
4. When, how and why does separate working change into case-sharing? How does this reflect the public and private interests at stake?
5. What are the consequences of the flexible relationship that corporate security has with law enforcement?

The first section of this chapter focuses on answering the research questions. In doing so, this chapter starts with summarising the most important findings of the research as related to the research questions. From this discussion of the research questions, some themes emerge which deserve some special attention. These cross-cutting themes emerging from the research are discussed in sections 2 through 7. Section 2 starts with an reflection on the (semi-)autonomous role corporate investigators may take in their investigations and (assistance with) settlements. Section 3 goes on to focus more in-depth on the importance of forum shopping in the context of the corporate security market. The issue of limited control over the activities of corporate investigators and their clients is the subject of section 4. Section 5 moves beyond the semi-autonomous social field of corporate investigators, to reflect upon public/private relations. The way in which corporate investigators deal with different interests, guided by normative and pragmatic considerations, is discussed in section 6. It is argued that in the commercial context of corporate security provision, there is some room for non-contractual moral agency. Section 7, then, takes this argument and discusses the issues of legitimacy and the role of the common good in the face of private interests.

From the discussion of the answers to the research questions in section 1 and the cross-cutting themes presented in section 2 through 7, policy implications emerge. Section 8.1 discusses the implications this research may have for attempts to govern the corporate security market. Section 8.2 specifically focuses on the more theoretical

implications of the research, by arguing that public/private relations within the setting of the investigation of internal norm violations in organisations are more correctly seen as coexistence, rather than cooperation. It is expected that a focus on cooperation by policy makers will not be effective in producing the desired results. Section 9, finally, suggests some possible strains of future research, following from the research.

1. The research questions

Research question 1 – The modus vivendi of the corporate security market

The corporate security sector exists of four main groups of investigators – in-house security departments, private investigation firms, forensic accountants and forensic legal investigators. Although the market is fragmented based on professional background and legal frameworks, fieldwork suggests that corporate investigation units tend to diversify their employees, thus combining the expertise of multiple professional groups to meet the demands of clients. Corporate investigators do not have access to the same information as law enforcement authorities, because corporate investigators lack formal powers of investigation. Within the limits of what is allowed, corporate investigators may act efficiently and swiftly to gather a considerable amount of information through the investigation of internal documentation, internal systems, open sources and personal communications. Acting as an extension of an organisations' management, corporate investigators have access to much information regarding employees. Although corporate investigators cannot enforce cooperation, and may thus be said to be reliant on voluntary cooperation, the client *can* enforce cooperation by using its status as an employer. The voluntary nature of employee cooperation should therefore be assessed critically. The *raison d'être* of the corporate investigation sector lies primarily in the fact that a customised solution to internal norm violations is provided to clients, which is designed to provide an efficient solution without causing additional harm and which takes client interests as a central point of reference. Because of the possibility to work across jurisdictions, corporate investigators can be flexible with regard to the types of behaviour they investigate (which is not necessarily criminal), the investigative methods they employ and in the solutions towards which they work.

Research question 2 – Legality: the legal frameworks

In general terms, no corporate investigator is allowed to break the law. In addition, the law regulating the use of personal data applies to all investigations. Specific legal frameworks, however, differ from investigator to investigator. Interestingly, an overview

of the legal frameworks applicable to the different corporate investigators reveals that the legal context does not align with the tendency of corporate investigation units to simultaneously specialise and generalise their services. While most corporate investigator-respondents indicate that they work with corporate investigators with different professional backgrounds, the regulations remain dispersed and unclear to most of the people involved. The fact that only private investigation firms are obliged to get a permit by the Wpbr (the law regulating private security companies and private investigation firms) is seen as peculiar by many respondents. In practice, corporate investigators with different professional backgrounds seem to broadly follow the rules defined by the Privacy code of conduct for private investigators, either by applying it directly to their investigations, or by following the broader principles of law which are codified in the Privacy code of conduct. In this way, corporate investigators broadly follow the same norms, in spite of the absence of generally applicable rules. Respondents stress the importance of principles of law such as proportionality, subsidiarity and fair play as guiding norms for their investigations. There are little indications of corporate investigators breaking the rules or the normative guidelines they use, however respondents indicate that they assume that laws and (self-)regulations are occasionally broken (by others). The differences in legal frameworks furthermore create room for forum shopping – also making it unnecessary to break or bend the rules, because of the room created by the differences in the legal contexts.

Research question 3 – Autonomy and strategic tasking

Within the private legal sphere corporate investigators enjoy a high degree of autonomy. Corporate investigations are guided by an assignment from a client and within that assignment (and the limits of – mostly – privacy regulation), investigators may use the methods they deem fit. When searching for a solution to the norm violation, corporate investigators and clients draw upon multiple jurisdictions. By forum shopping among public and private legal systems, optimal solutions may be provided to clients. Solutions may be found in criminal law (a report to the authorities), private law (a civil suit based on tort or a settlement agreement), labour law (termination of the labour contract) and internal regulations of the employing organisation (multiple forms of internal disciplinary action). In many instances, the choice for a corporate settlement may be made autonomously by a client, with the aid of corporate investigators. In some cases, there is not much room for such a choice, for example because authorities are already involved. In other instances, the choice whether or not to report does remain in the private field and pragmatic and normative considerations may compel an organisation to report the case to law enforcement authorities. By presenting the case in a certain manner to the authorities, corporate investigators may be able to give some direction to the criminal justice investigations and (possible) prosecution. The decision what to investigate and prosecute lies with law enforcement authorities, however, corporate investigators may sway these decisions in a certain direction. In many cases, law enforcement authorities are reliant in part on corporate investigators (without a report, law enforcement

authorities often remain unaware of the norm violation and corporate investigators are specialised investigators with regard to complicated financial investigations). Therefore, there is a considerable sphere of discretion for corporate investigators and clients to either act alone or to involve law enforcement authorities. A criminal justice solution may be deemed desirable to supplement a corporate settlement solution (which reasoning essentially reverses the argument of the junior partner theory of Kakalik and Wildhorn).

Research question 4 – Public/private relations and the interests involved

Private and public interests are both involved in corporate investigations and they are both considered in a decision to involve law enforcement authorities. Private interests of the client are leading and considerations such as efficiency and damage control often lead to a solution outside the criminal justice system. However, pragmatic considerations such as the need for powers of investigation and a wish to avoid harsher punishment elsewhere, may lead to an official report to law enforcement authorities based on private interests. Although a commercial actor, corporate security also takes public interests into account. Normative considerations, such as a sense of responsibility towards society or towards the market, and a perceived need for retribution, may lead corporate investigators and clients to report a case to the authorities. In more general terms, public interests are taken into account in purely private solutions as well. Procedural rights of the involved person are less pronounced in corporate investigations, but the normative considerations corporate investigators use as a guide for the investigations do lead them to focus on principles of law such as proportionality, subsidiarity and fair play. Corporate investigators also indicate they are wary of being used for indecent purposes by a client.

When public/private relations occur in a case, this is done on an *ad hoc* basis. Although many informal contacts exist between corporate investigators and law enforcement professionals, cooperation efforts aimed at the longer-term have proven to be unsuccessful. A typology of coexistence – ranging from private to public information transfer, through (minor) mutual information sharing to coordination – can be used to accurately describe public/private coexistence. Only in the case of coordination, one may legitimately speak of cooperation. However, respondents indicate that coordination is rare. Coexistence usually does not surpass the level of information transfer from corporate investigators to the criminal justice system.

Research question 5 – Theoretical and practical consequences of public/private coexistence

Practical consequences of the considerable autonomy of corporate investigators and of their relative distance to the criminal justice system may fall upon clients,

involved individuals and upon (Dutch) society. Using corporate investigative services, organisations may solve their norm violations efficiently in multiple ways, through multiple legal venues, without having to cede control or risk much openness. The corporate security market may provide organisations with both investigative services and assistance in settlements. From discovery to solution, a norm violation may thus remain entirely out of sight of the criminal justice system. Strategic use of public resources may furthermore lead to a higher probability of getting a case investigated and prosecuted by the criminal justice system if that is desired. Another practical consequence, which may be of more relevance to the involved individuals and society in general, is that there is very little insight in and control over the corporate security sector by law enforcement agencies. This may have practical consequences for the involved person, as his procedural protection is rather limited in a setting of corporate investigations and settlements. From a rule-of-law point of view, such a situation may be problematised. Corporate investigators display some measure of non-contractual moral behaviour and tend to apply general principles of law (thus protecting the involved person this way). However, this is based on the normative considerations of individual corporate investigators and clients and even though there are possibilities to enforce compliance with rules and guidelines, this relies for a large part on the active stance of the parties involved (the involved person, the client and the corporate investigator). Another practical consequence is that the criminal justice system is not clogged by cases it would most likely dismiss anyway because of a lack of capacity and a shortage of specific expertise.

Conceptually, consequences fall on the way we view public/private relationships. The high level of autonomy and the active use of the criminal justice system by corporate security actors make the state-centric discourse (whether it is used by claiming a dominant, or a diminishing state) a bad fit with the corporate security market. Instead of trying to fit the social reality of the corporate security sector into the state-centric discourse, it might be better to try to fit conceptual notions of public/private relations into the social reality by emphasising the flexibility of corporate investigations within the semi-autonomous social field. Within the corporate security market, private actors are acting for a large part independently from the state, generally not involving the criminal justice system. Much of the investigations of and reactions to internal norm violations thus remains entirely out of sight of the criminal justice system. When law enforcement actors are involved, this is usually because they are actively sought after by corporate investigators and their clients.

Central research question

To summarise, the corporate security sector is a commercial provider of investigative services, involved in the investigation and settlement of internal norm violations. The

sector largely acts as a semi-autonomous social field with a high level of discretion, flexibility and autonomy. Public/private relationships are largely *ad hoc* and occur when corporate investigators or their clients feel the need to involve the criminal justice apparatus. Cooperation is fairly rare, public/private relationships being better conceptualised as coexistence, with public and private actors meeting only on an *ad hoc* basis. This means that the state has little insight into what happens in the corporate security sector. Consequently, the private sector tends to fend for itself in instances of internal norm violations. While this has the benefit for society that the criminal justice system is spared the trouble and costs of investigating and prosecuting these matters, it also means there is little to no democratic control over the corporate security sector.

Cutting across the research questions, there are a number of themes emerging from the research which deserve some additional attention. The next six sections of this chapter discuss these in more detail.

2. Corporate security as a semi-autonomous social field within a private legal order

As many scholars have indicated, private investigations, and corporate investigations more specifically, happen in a field of mystery (see e.g. Hoogenboom, 1994). Chapter 3 and 4 describe that many of the activities of corporate investigators indeed stay within the private sphere: investigations are done by private actors and solutions are sought in private remedies (private law or, more specifically: labour law). As an extension of the employer, corporate investigators have many sources of information at their disposal. The lack of formal legal powers is not necessarily a restriction for corporate investigators. Because corporate investigators are able to use the access to information the organisation has as an employer, their practical access may even exceed that of law enforcement. Although law enforcement agencies may formally claim any information (unless protected by legal privilege), this formal power may not prove extremely useful when law enforcement does not know 'where to look' or how to interpret the findings. Modern organisations have grown so complex that even for people inside the organisation, some of its processes are difficult to understand. It may therefore prove impossible for outsiders, who are rarely trained specifically for fraud investigations or familiar with the commercial world, to interpret the information they may gather through formal powers. Even if all relevant data would be handed over by the organisation (which, as respondents suggest, is

not necessarily the case),[105] it takes skilled eyes to reconstruct what happened. Corporate investigators are in a better position to efficiently gather, interpret and use information from inside the organisation. In-house investigators may be in the best position in this respect, however external corporate investigators also get the access (and cooperation) necessary for the investigations. Employers have quite an extensive right to information regarding their employees and they may also order their employees to cooperate with the investigations. Furthermore, automated processes leave traces. Much information which is at corporate investigators' disposal is therefore 'private information'. Although there certainly are instances in which the involvement of law enforcement agencies is desired, in many cases the step to involve law enforcement agencies in an investigation is therefore not a necessary one.

There are many reasons for organisations to prefer a private solution over a criminal justice procedure and keep matters within the private legal order. These are described in chapter 3 and 4. Much specialised expertise is available in this diverse field. As noted in chapter 2, many corporate investigation units (whether they are internal to an organisation or contracted-in) now employ investigators of all four professional groups discussed as being part of the corporate security sector in this research. They therefore often have a high level of expertise and much experience with regard to the types of non-conformities that organisations are faced with (and the corresponding methods of investigation). Both investigations and solutions may be tailor-made to the organisation, disrupting normal organisational processes to a limited extent and providing swift and efficient solutions. Within its private legal sphere, corporate security may act with considerable flexibility with regard to the investigative methods and solutions. Furthermore, the orientation on the private troubles of clients rather than on criminal offences, ensures an organisation that the problem is addressed, whether it may be defined within the limits of criminal law or not. Additionally, the possibility to retain information in the private sphere (giving the organisation the chance to do damage control) and to have some measure of control over the process through an assignment agreement, is highly valued by organisations. Law enforcement, conversely, is seen as slow, inefficient and causing much additional harm by its focus on openness. The information collected in this research suggests that a criminal prosecution, when sought after by organisations and corporate investigators, is hardly ever the only resolution. Rather, it is seen as an additional step that may be taken, over and above a private corporate settlement. Respondents indicate they do not expect the criminal

105 This is not necessarily a case of 'deceit' by the organisation. Coming back to the quote of respondent 43 presented in chapter 4: the information which has been asked for is provided, but that may not necessarily be the full story. Access to an employee's laptop for example does not mean access to the internal system of the organisation. The criminal investigations of the laptop will thus in such a case be limited to the hardware of the laptop. The same goes for other types of information.

justice system to provide a solution to their problem: corporate settlements are used for that. Thus, in providing investigative results and solutions to clients, corporate investigators largely remain within their semi-autonomous social field.

Corporate investigators thus largely operate in a private legal sphere in which they market corporate investigations and corporate justice. However, the research also reveals that claiming that organisations fully stay within the private legal sphere for their solutions to internal norm violations would be a too narrow view of social reality. Apart from those instances where no choice is available (law enforcement agencies are already involved *ex officio*), pragmatic and normative considerations may open the door to law enforcement involvement in a case. A criminal justice procedure adds a normative dimension to the corporate investigations: when punishment and moral disapproval is felt to be necessary, a criminal justice procedure is deemed much more suited than a private solution. In addition, the criminal justice system may be used strategically – when information is necessary that may only be obtained by using formal powers of investigation, a report to law enforcement authorities may be made as well.

3. Forum shopping within and across a private legal sphere

The semi-autonomous social field of corporate security may on the one hand be considered 'closed' in the sense that it mostly stays within the private sphere, however on the other hand it is quite open: different legal venues are used to provide an optimum solution to a client. This flexibility may just as well lead to a public law solution as one based on internal regulations, depending on the details of the case. One of the key features of corporate security is its ability to engage in *forum shopping* (Williams, 2006a). Forum shopping occurs in multiple ways and is used by multiple actors to get to the optimal result in a specific situation.

First, the fragmented nature of the professional market for corporate security creates room for clients to forum shop for the investigator who is best suited to meet their investigational needs. Every professional group of corporate investigators has unique selling points compared to the others because of professional background, expertise and the legal framework within which the investigations take place. Although the different players in the market tend to diversify the background of their employees so to be better able to meet the investigational demands clients might have, they do market themselves along the lines of these professional advantages. Second, investigators try to find the investigative methods which will deliver the best results in a certain case, taking the principles of law of proportionality and subsidiarity

into account as well. While some investigative methods and information sources are generally used in most investigations (such as the interview with the involved person), some cases provide additional sources of information or warrant a different approach. For example, a track-and-trace device may be useful when multiple high-end items go missing in a short period of time but for a case of construction fraud a site visit may be more suitable. Third, the options of corporate settlement provide the backdrop of much forum shopping. The mere fact that corporate investigators and clients may work towards and choose from multiple legal venues for a settlement of the norm violation creates a high level of flexibility. Within the different jurisdictions (public or private law or internal regulations), there are more choices to be made. Within the private law system for example, recourse to a civil court may be made based on tort or based on breach of the labour contract. The private law system furthermore provides the option of an out-of-court solution through a settlement agreement. Corporate settlements may be combined, making the choices for different forums even wider.

When it comes to the decision whether or not to involve law enforcement authorities, multiple pragmatic and normative considerations may come into play. The need for investigative powers may be one pragmatic consideration, another may be that the organisation runs the risk that it will be prosecuted in a harsher national jurisdiction than the Dutch. Although the principle of law of double jeopardy is not internationally recognised, chances of severe punishment for the organisation are reduced by such an action because even if prosecuted again, the prosecutor (and judges) in the second jurisdiction are likely to take the prior punishment into account. The extensive use of forum shopping thus means that while most of corporate investigators' activities remain within the private legal sphere, moving towards the public legal environment may provide an optimal solution in certain cases as well.

The above should make clear that stating that corporate security is a semi-autonomous social field should not be taken as a statement that it is a *homogenous* field: it is indeed highly fragmented and fluid, both in its composition and in its service provision. The fragmentation of the field (many different corporate security actors, working for many different clients, with many different interests) makes it furthermore difficult to get comprehensive insight into or exert effective control over corporate investigators' activities. The different rules applicable to the different actors make for a field which is "fragmented, almost chaotic even" (Hoogenboom, 1994: 263). Adding to this that most of the activities never reach the criminal justice system, it is not surprising that there is no clear view within law enforcement agencies of what 'corporate security' actually is in practice. In many cases, forum shopping options make it rather easy for corporate investigators and clients to keep law enforcement authorities at bay.

4. Control and accountability in the context of a semi-autonomous corporate security sector

Many commentators express a certain degree of uneasiness with regard to the existence of this private legal order (see e.g. Abrahamsen & Williams, 2011). From a rule-of-law standpoint, the (very) limited control over and insight in the day-to-day practices within the corporate security sector may be considered to be problematic. Corporate investigations can have a large effect on the people and organisations involved and there is a potential for abuse: there is little democratic control over the private legal sphere in which corporate investigators operate. As we have seen in chapter 2, extensive access and lack of formal powers do not lead to a situation in which 'anything goes'. The legal restraints put upon corporate investigators are indeed less stringent than those put upon police. As Stenning (2000: 337) argues, however, it would be incorrect to assume that (democratic) control over police organisations is more effective for this reason alone.

> Those who argue that the public police are highly accountable and the private police hardly accountable at all, usually arrive at this conclusion because they only consider the kinds of accountability to which public officials are subject and, not surprisingly, find that private police are nowhere near as accountable *in these ways* as are the public police. (…). They frequently overstate the effective public accountability of the public police by focusing on the ways in which they are theoretically accountable while not paying sufficient attention to the very real (and well documented) limitations of the effective accountability which is able to be accomplished through these mechanisms in practice.

The research that provides the foundation for this book did not focus on police accountability and neither will this concluding chapter. It is important, though, while discussing the limited amount of public control over the corporate security sector, to keep in mind that democratic control over police organisations does not automatically lead to effective accountability either. In addition, the lack of public control does not mean there is no legal framework in place or no control over corporate investigators' activities. Many (informal/self) regulations are guiding corporate security's actions. The nature of these frameworks is often not that of a legally binding rule, rather they are used as guidelines. Respondents suggest that they are generally guided by the principles of law behind the guidelines – all corporate investigators who have been interviewed or observed in this research (claim to) abide to certain leading principles of law – most notably proportionality, subsidiarity and fair play. Additionally, civil (or even criminal) liability serves as a fall-back option for those who are wronged by corporate security's activities.

Whether or not 'problematic', control over corporate investigators by the state is limited. Just as is the case with most investigations and settlements, most safeguards and controls also stay within the private (legal) sphere. Only private investigation firms are obligated to get a licence from the Ministry of Security and Justice, and as we have seen in chapter 2 the control over the licences is purely administrative. The scattered nature of regulations (different investigators having to comply with different legal frameworks) furthermore creates a rather ambiguous legal context. There are two interesting circumstances that may be noted in this regard. The first is formed by the confusion about the applicability of the permit system of the Wpbr: some forensic accountant-respondents do have a permit and some do not. Forensic accountants are not obliged by law to get a Wpbr-permit. Secondly, there is a pervasive fallacy in the corporate investigation profession that forensic accountants are the investigators who are most strictly regulated. As chapter 2 shows, this is not the case as forensic accountancy rules are based on (non-binding) guidelines and principles of law (which are, however, used in disciplinary proceedings). Another pervasive fallacy around regulation is that of the (im)possibilities of public/private information sharing: many (mostly public-sector) respondents are not aware of the opportunities within the legislation for information sharing. The legal context of the corporate investigations field is thus not entirely clear to the professionals working in it. Because much of corporate investigators' activities stay within the private legal sphere, the criminal justice system is furthermore not in a position to exert much control. All of this adds to the state's lack of insight in and knowledge about the corporate security sector. The control over corporate investigators' activities is thus largely located in the private legal sphere as well.

The system of safeguards in place for corporate security's actions has a different rationale than the one in place for the criminal justice system. Where the safeguards within the criminal justice system are mostly focused on protection of the (relatively powerless) citizen against (abuse of power by) the state (representing vertical relationships), the private law-rationale of the Civil Code implies a certain level of equality between parties (representing horizontal relationships). Authors such as Meershoek and Hoogenboom (2012: 20) remark that "as long as citizens have access to a judge and non-judiciary institutions of appeal, elementary civil liberties are guarded". This may be true, however, such a view glosses over the differences in ability to effectuate these possibilities for control. If you have been harmed by corporate security's actions there are private law remedies available to you – but these require an active stance from involved individuals. Furthermore, the equality-of-parties argument can be considered unhelpful in this context. In the case of corporate investigations and corporate settlements, a definite power imbalance may be discerned between the organisation (employer), corporate investigators

and legal council on the one hand, and the involved person(s), possibly with legal representation, on the other (Piret, 2005). The commercial interests and professionalism of corporate investigators protects against gross abuses of power in most cases according to respondents (see also Berndtsson, 2012). There are, however, concerns about the protection of the involved person and the power imbalances within the private legal sphere. These are fair concerns. Private organisations and corporate investigators attempt to counter these issues by taking general principles of law into account, and by prescribing procedural guarantees in the investigations and settlements, however the possibility of abuse still remains.[106] In addition, the market for corporate investigations and corporate settlements exists by virtue of the mobilisation of symbolic capital. This means that the reputation of the sector as providing a legitimate professional service, convening authority, is essential to its professional existence. For the sector to be successful in its commercial endeavours, it is thus vital that it is viewed as a legitimate actor beyond the private legal sphere in which it mostly operates (see also below). It is therefore important to note that the private legal sphere exists by virtue of "the legitimacy afforded by the public sphere and the ability of industry practitioners to mobilize formal legal sensibilities, rights and obligations and to invoke public modes of recourse in circumstances in which they are warranted" (Williams, 2006b: 219).

5. The myth of public/private turf wars – the matter of competition versus separation

Above, the activities of corporate investigators were placed within a semi-autonomous social field. This contradicts the state-centric discourse commonly used for crime control (Van der Lugt, 2001). A thought-provoking observation by Hoogenboom (1994) in this light is that private investigations affect the exclusive position of the state on crime reduction. This is a reasonable argument, which follows from the idea that the state is the leading actor when it comes to crime control, and that involvement of other actors serves as an impeachment of said monopoly (Van der Lugt, 2001). This is the starting point of most theoretical arguments about public/private relations within the security field. The junior partner theory claims that private actors are junior partners to the state, advancing the state's objectives by their actions and acting as a fall-back option for the services the state cannot (fully) provide. When defined in this way, Hoogenboom (1994) argues, the private sector is no threat to the legitimacy of the law enforcement system as it serves as a

106 They still are present in police investigations as well – however there the control and procedural guarantees are more strictly regulated.

supplement to this system. The activities of the private sector are thus considered to be different from those of the police.

Interestingly, public-sector respondents interviewed in this research have voiced no significant concerns with regard to the argument of breach of, or threat to, the monopoly on crime control (White, 2014). In 2001 Van der Lugt already expressed his wonder about the lack of concern by law enforcement professionals with regard to the role of private investigators, compared to the uneasiness they feel when it comes to the role of private security guards. This is in line with the argument of (in)visibility that White uses to explain why the most visible forms of private security are regulated in the UK, while other types of private security that are less visible, are not. Those private security actors who move in a private sphere are not regarded as posing a threat to the repression-monopoly held by the state, in the same way that parents may discipline their offspring without posing such a threat. Interestingly, corporate investigations may move out of the private legal sphere into the public sphere but even then, public and private may still be regarded as functionally separate. The failed pilot projects discussed in chapter 5, aiming to streamline the use of information gathered through corporate investigations in criminal justice proceedings, may be regarded as an indicator that the rationale within corporate and criminal justice investigations is too different to streamline in one go.

One might argue, then, that the public/private separation (in Williams' (2005) words, 'bifurcation') which has often been renounced by scholars focusing on private security, remains a relevant concept for the corporate security sector. Instead of a blurring between public and private into some kind of hybrid entity, as is so often argued to happen in other forms of private security (see Johnston, 1992), there are boundaries between public and private, with corporate security mostly remaining within its private legal sphere. This separation is based on multiple characteristics of the public and private sectors. First, the cases corporate investigators deal with are not necessarily the same as those that end up in the criminal justice system. For one, not all cases investigated by corporate security involve criminal behaviour. These are breaches of internal regulations, business standards or other norms. In those cases, there is no functional overlap between corporate investigations and criminal justice investigations. There is, however, also a large category of norm violations that *may* be defined as criminal (as they are criminalised in the penal code) but *are not* defined as such for various reasons (see chapter 4).

Secondly, it can be argued that there is a difference in *rationale* between corporate investigations and criminal justice investigations – and not just in the sense that commercial parties are focused on loss prevention and state actors are focused on crime reduction (Hoogenboom, 1994). The fact that most of corporate investigators' activities are within a commercial context, within the private law system, makes the cases they investigate, and the legal frameworks that are used for those investigations, follow the rationale of the private sector. Within the private law system equality

of parties is generally assumed, as is the agreement on 'facts' (unless contested). Although elements of criminal justice (such as the adherence to procedural justice) are inserted in corporate investigations and corporate settlements, the dominant rationale is that of the private law system. Problems are solved as efficiently as possible, defined as a business or labour conflict and dealt with accordingly. Whether or not the behaviour is (also) criminal is often an after-thought.

Thirdly, different interests are served by private and public-sector investigations. Although questions may be asked about the validity of such a claim, state-led investigations essentially serve public interests (Loader & White, 2017). The Dutch criminal justice system defines crime primarily as a dispute between the offender and the state: the (legal) person affected by the norm violation is no party to this dispute.[107] As such, there is little room for the inclusion of his private interests.[108] Conversely, corporate investigators focus mostly on the private interests of clients, keeping them central to all their proceedings (while also taking public interests into account when possible). This leads to a difference in approach to both the investigations and the solutions provided.

While there seems to be a tendency to 'cooperation talk' in both the public and the private sector, not much seems to come of it. As described, the nature of the sector (fragmented) and of the activities (focused on private interests) and the high level of autonomy within the private legal sphere, together with a difference in rationale and focus between the public and private sectors are likely to make any form of structural, long-term cooperation between law enforcement and corporate investigators very difficult. But, although the cooperation narrative is pervasive, very few (public and private sector) respondents seem to have an issue with this tendency to separation. Many respondents indicate that they feel corporate investigators are fully capable of providing their clients with the kinds of results the criminal justice system does not offer. As shown in this book, the services of corporate security go beyond criminally defined behaviour. Additionally, there is a focus and client-centeredness in corporate security's work which makes corporate investigators and settlements – although at times overlapping – essentially different from criminal justice investigations and procedures. One of the findings of the research is thus that there is no competition between public and private in the sense of nodal theory (see *inter alia* Wood & Shearing, 2007; more on this below). The competition-argument implies, as does the loss prevention theory mentioned by Hoogenboom (1994), that police and private investigators' activities are similar and that in such a sense, public and private are

107 However, in recent years the position of the victim has been strengthened, for example by the formal right to speak in court (see for example Pemberton & Reynaers, 2011).

108 Although individual law enforcement professionals may take private interests into account as well.

basically interchangeable. Although the activities in themselves may be regarded as similar,[109] the context in which they are executed (the private or the criminal justice sphere) ensures a continuation of the public/private bifurcation. This is not a rigid or unchangeable separation – indeed, as we have seen, there are many possible forms of overlap – however, it is the 'default position' of the sector.

Fundamentally, a shift needs to be made from a public-sector oriented gaze (or state-centric discourse) to one that recognizes the autonomy of corporate security actors. Hoogenboom has long argued for such a shift in the criminological gaze (e.g. 2007). As we have seen, there is simultaneously an overlap between and a difference in the activities by the public and the private sector in this field. Crucially, the difference is not the one as described in the junior partner theory – in most cases it is not a question of the corporate investigations industry being supplementary (or 'junior partner') to law enforcement activities. Rather, fieldwork suggests that the criminal justice system is seen as the supplement to corporate settlement solutions. Whether or not an internal norm violation is reported as a crime to the criminal justice authorities is in most instances an afterthought for the organisation involved. Chapter 4 has shown that even in cases where a report to the authorities is made, this is mostly done in addition to a private solution. There may be moral or pragmatic considerations for such a decision (see chapter 4) but it is often seen as the extra step, not the main solution. All of this makes the hierarchical view of crime control as a state-mandated activity, or alternatively as a "common regulatory enterprise" within a networked reality (with all actors having the same implicit interests, goals and objectives) one that is hard to maintain (Williams, 2006b: 212). Rather, one should recognise the multitude of actors, interests and professional backgrounds influencing the investigative and settlement activities within the private legal order (ibid.).

Throughout this book, relations between corporate investigators and law enforcement actors have been presented as the exception rather than the rule. In chapter 5 the term 'coexistence' is introduced as a better-suited term than 'cooperation' and a typology of co-existence is presented, ranging from a more or less one-sided action from private actors (type A – 'private-public information transfer'), through more or less mutual but limited information sharing (type B – '(minor) mutual information sharing') to what one may term actual cooperation (type C – 'coordination of actions'). In most cases in which criminal justice actors get involved, private to public information sharing occurs (type A). Often, as respondents indicate, the

109 An important side note here is that although the activities are largely similar, they are not interchangeable. The fact that corporate investigators do not have powers of investigation means that they cannot perform all the activities law enforcement professionals could in the same situation. Similarly, corporate investigators can provide their clients with services law enforcement agencies do not provide (such as asset recovery and the improvement of compliance systems).

information received from corporate investigators needs to be thoroughly checked by (mostly) full-blown criminal justice investigations to make it fit into the rationale of the criminal justice system. As a bare minimum, the suspect will be interrogated by the police with all the procedural cautions but fieldwork shows that in most instances police will 're-do' the investigations entirely.

6. Normativity and pragmatism in corporate investigations and settlements – a case of non-contractual moral agency?

Above, the different foci of rationale in corporate investigations and criminal justice investigations were discussed. This is not to say that there is no room for 'the rationale of the criminal justice system' within corporate justice. Many corporate investigators have a criminal justice background and their way of approaching their work incorporates some parts of the criminal justice rationale. This manifests itself in multiple ways and is aptly termed 'non-contractual moral agency' in a wider context by Loader and White (2017): the actions of corporate investigators which cannot be said to be contractually mandatory but are done because they are 'right'. Some of these are made contractually mandatory – because corporate investigators have inserted them into their code of conduct – others are not. Non-contractual moral behaviour that is made mandatory for part of the sector is the use of certain principles of law. In the Privacy code of conduct, which is binding to private investigation firms, the most important of these principles of law are codified. The same goes for the guidelines used by forensic accountants. Other investigators tend to also use these principles of law, in an effort to ensure due process. Moreover, more stringent rules and additional principles of law may be inserted in the individual codes of conduct of corporate investigation units. The use of these principles of law – most notably proportionality, subsidiarity and fair play – is meant as a safeguard to counter the power imbalance between employer and employee and to strengthen the formal position of the latter. The use of said principles of law and broader normative considerations works to enhance the legitimacy of corporate investigations as well. In this sense, it is a reputational matter for corporate investigation units. The interviews and observations in this research indicate that in addition to this commercial incentive to 'play fair' (which is more a practical, strategic consideration than a normative one), many corporate investigators also do so out of normative considerations. They are aware of the power they represent in the investigations and although they make use of that power (by putting pressure on an involved person to cooperate, by demanding information, et cetera), they seem to try to do so 'responsibly' (see chapter 4).

Non-contractual moral agency may be most apparent in situations in which the moral behaviour goes against commercial interests. This may be the case when corporate investigators hand back an assignment because they believe they are being used by a client in an illegitimate way or because the investigations are in danger of not being independent and objective. This is a loss of income on the short term and will most likely lead the involved client to take his business elsewhere in future.[110] Another manifestation of non-contractual moral agency is the *pro bono* work some respondents do. Corporate investigators do not get paid for these cases (or they might use a heavily reduced rate). *Pro bono* work is reserved for cases in which corporate investigative services are very welcome but the client is not able to pay for them (for example when a norm violation is discovered in a small-business environment).

The general principles of law many corporate investigators claim to take into account, constrain them in general terms from using illegitimate means of investigations. However, it may under circumstances lead to behaviour which is considered 'right' even though it is not allowed. The instances which were mentioned by respondents concerned minor (privacy) violations which benefited the person whose privacy was violated (see chapter 5). Additionally, corporate investigators and clients may find themselves in a grey area by acting in a way which they think is right towards other market players. An example of this is one employer giving another employer a warning sign about a (future) employee.

In advising clients whether or not to report a norm violation to the authorities, corporate investigators may insert normative considerations as well. When the norm violation is deemed too severe (mostly cases involving physical harm) or when a need for retribution is felt by the client, corporate investigators may advise the client to make an official report. Indicative of this is that the corporate investigator respondents, as well as the clients who were interviewed in this research, point out that they do not expect much from a report to the authorities: they often do so because they believe it is the right thing to do.

Thus, the focus on normative considerations and principles of law as guidelines for corporate investigators' activities fits within the non-contractual moral agency Loader and White (2017) would like to introduce into private security more generally. As we have seen in chapters 2 to 4, corporate investigators tend to place great value on principles of law as guidelines for their professional action. Additionally, their (and their clients') introduction of normative considerations into the process of investigating and settling, may be said to go beyond what is needed in their contractual relationship with clients. In this way, the non-contractual moral agency

110 However, because it might boost the reputation of the involved corporate investigators, it might be a commercially smart move in the long run.

of corporate investigators may ensure the (partial) inclusion of public interests into the setting of private corporate investigations and settlements. However, as long as the adherence to this principles of law and inclusion of other than strictly private interests is based on voluntary action, the potential problem of non-compliance remains present.

7. Legitimacy and the common good

The legitimacy of private security has been a recurrent theme in literature. In their article about the private security sector more generally, Thumala, Goold and Loader (2011) suggest that there is a moral ambivalence in this sector about the industry's condition and legitimacy. Although many of the claims made by the authors do not necessarily fit with the fieldwork reported upon in this book, the authors do raise some interesting points.[111] With regard to the need for justification of the market for private security, the authors state: "the industry may exist to make money. But making money selling security does not seem like justification enough". Like my respondents, the professionals interviewed by Thumala et al. "crave a wider worth and credibility, long to be well-regarded and thought of as an activity which is socially valuable" (2011: 297). When asked about their general opinion about the existence of a corporate security field, many public-sector respondents indicated that they felt a bit conflicted: on the one hand, they seemed to agree with the widely-held (but often implicit) opinion in criminology that crime should be dealt with by the state (which may be said to be a normative stance). On the other, they express the opinion that corporate investigators are generally better equipped to deal with these specific matters without public sector involvement (which is a more pragmatic approach). Interestingly, corporate investigator-respondents tend to not just point to arguments based on the market while justifying their work – such as that there is a demand for their services and that it is a legitimate business (Hoogenboom, 1994). Instead, respondents stress their role in the provision of a service which serves not merely the private interests of clients, but also adds to the common good (for example by correcting the lack of interest by police and the justice department and by providing a customised service). When talking to corporate investigators, a frequent comment is that the criminal justice system is not focused on the types of crimes organisations are concerned with. A consequence is that on the one hand reports to the authorities are not very often made, and on the other,

111 The authors refer for example to problems of poor quality of staff, 'cowboy traders' and a connection to (organised) crime. These issues are less pronounced in the corporate security sector: the quality of staff for example is regarded as higher than in the public sector (although, as chapter 2 shows, there is no uniform system of education or quality markers available).

that many cases which *are* reported are not prioritised by law enforcement agencies and thus either investigated at a late point in time or not at all. Additionally, the position of the (legal) person affected by the crime is rather peripheral in Dutch criminal law. A crime is primarily seen as a crime against *society*. This means that the way a crime is investigated and handled in the criminal justice system does not fit very well with the interests of those directly involved: police and prosecution often only investigate what they need for a conviction, while the organisation needs the complete picture. Furthermore, the criminal justice process is very slow and no 'solution' is provided to the problem at hand (see chapter 4).

Corporate investigators view themselves as providing a (public) service by offering a (professional) answer to the organisation's problem. Because of their background and experience, corporate investigators are well-suited to do the investigations and help with the settlement, it is argued. In this way, the interests of the client are served, society is served because redress is made and professional procedures are in place to ensure the people involved in the investigation are treated fairly.

> You may wonder whether the criminal justice system is always the best way to go to get to the classic goals of the penal system. Internal investigations are often much faster and more effective. The company is corrected and restored, the person is fired, so the legal order is restored. In the end, that's the most important goal of our legal system, isn't it? So actually, internal investigations serve a lot of the classically intended purposes of criminal law. [Respondent 28 – forensic legal investigator/client]

The above comment may also be interpreted as a legitimising effort of the corporate security sector. Both within the sector and across it, legitimising efforts are made by stressing the inability of the criminal justice system to meet the demands and needs of organisations when faced with internal norm violations. In this way, corporate investigators position themselves as professional (and importantly, independent) experts in their field, combining this symbolic capital with a commodification of trust (Williams, 2006b).

Corporate investigators thus see their general role as providing a service to their clients, but at the same time transcending the mere private interests as well. When it comes to the common good and the role corporate investigators may play in its constitution (for the better or the worse), some issues may be identified. Above, the power imbalance between employer and employee has been discussed. Even though corporate security providers indicate that they try to put systems in place to ensure due process, this power imbalance continues to exist within corporate settlements. In those cases that do not reach a court for reasons of private interests (such as efficiency and reputation) the control over the process lies with the investigators and

the client. Because their private interests are served with the corporate settlement, there is a real possibility of abuse. In addition, even without breaking any rules or regulations, investigators and others involved may pressure the involved person to cooperate with the investigations and settlement, for example by threatening to report the matter to the police even though they do not intend to do so. In such a case, the values of the rule-of-law in a democratic state may come under pressure. These values tend to be taken into account, but might suffer from their collision with the private interest of the client.

The above represents the question of the role of public interests (or 'the common good') within the private legal sphere. Loader and White (2017) discuss models to ensure public interests in private security provision, concluding that it is not enough to cleanse the market from unruly security providers through regulation and quality standards, or to communalise the market by the redistribution of tax payer money so as to ensure equal access to the private security market. Cleansing and communalising the private security market fall short in ensuring public interests in so far as they leave no room for non-contractual moral agency of security providers. Although both models provide a solution to what they see as the problem with regard to the public interest (respectively 'cowboys' and unequal access), they are essentially neo-liberal in their approach in as far as they consider the market as essentially 'good' (Loader & White, 2017). According to the authors, public interests are involved in more ways than that. Loader and White therefore propose to 'civilise the private security market' by adding to the abovementioned cleansing and communalising models, the use of principles of law: "embedded in these settings, principles invite and mutually orient all actors who make up regulatory space" (2017: 179). The authors envision an 'inclusive deliberation' between stake-holders to ensure social solidarity in the provision of private security. For this, public and private institutions are essential. Police and trade associations are mentioned as obvious choices: "in the civilizing model, police forces are viewed not as top-down regulators of private security, but as one side of a public-private partnership, which rests upon, and, therefore deepens the principles of inclusive deliberation and social solidarity" (2017: 180).

While the focus on principles of law described above fits well with the realities of the Dutch corporate security market, the proposition of a public/private partnership (in the widest sense of the word) deliberating and putting into action the use of such principles does not. This book has shown the inward focus of the Dutch corporate security market, only rarely stepping outside its private niche to involve law enforcement actors such as the police. The statement that private security aspires to be police-like which gives the police considerable power to "communicate the importance of public values and commitments to the industry" (Loader & White, 2017: 180), has already been dismissed in several places in this book. Corporate security

respondents seem, on the contrary, to stress the non-police-like nature of their activities, preferring not to be seen as private police. The distance that exists with public law enforcement – notwithstanding the transfer of personnel and knowledge between the two – makes such a view hard to maintain.

Similarly, the role of trade associations is rather limited within the Dutch corporate security sector. Many respondents indicate they are not member to a trade association, and if they are it is one that is specific to their professional background (e.g. (forensic) accountant). Just as there is no overarching legal framework for all corporate investigators in the Netherlands, there is no overarching trade association (although, initiatives have been made in this regard, see chapter 2). Any role trade associations would play in the advertising of public interests through principles would necessarily remain limited to their members. However, intervention into the market by either police or a trade association would not only seem impractical, but it can be said to be superfluous as well. The next section of this chapter focuses on some alternative options which may provide a more practical solution to the issues of limited control possibilities over the corporate security market. The formulation of generally applicable principles of law, as suggested by Loader and White (2017) seems not to be necessary as corporate investigators seem to adhere to the same principles of law already. In doing so, and in their awareness of effects of their work beyond the specific private interests of the client, corporate investigators seem to endeavour to add in a positive way to the constitution of the common good. However, the question may be posed whether such an approach, using normative considerations and principles of law, is solid enough as a legal framework guiding corporate investigators' activities as the possibilities of control over the sector remain limited in this way.

8. Policy implications

8.1 Governing corporate security – looking forward

In his 2006 article, James Williams discusses some of the fundamental issues related to regulating the corporate security sector (2006a). Some of the key characteristics of the sector produce barriers, not only to structural forms of public/private cooperation, but also to attempts to regulate or govern the sector. The relative invisibility of corporate investigations and settlements, the large potential for forum shopping and strategic use of legal venues, the multiple interests involved and the fragmented nature of the sector in terms of professional actors and legal frameworks, all make comprehensive control very difficult. Be that as it may, corporate investigators also share common characteristics. One important commonality is the work itself: although corporate

investigations and settlements are tailor-made and client-centred, the investigative activities largely align within the sector. The tendency within the sector to combine the expertise of corporate investigators from multiple professional backgrounds in one corporate investigation unit adds to the common ground between corporate investigators. Furthermore, a common focus on principles of law as guidelines for professional behaviour seems to open up possibilities for regulation.

While there seems to be sufficient common ground for the governance of the sector based on an overarching legal framework, this research shows that such a framework is currently lacking. One might pose the question whether this is problematic. The premium corporate investigators put on principles of law may be a protection against misconduct – however, as long as the application of such principles is based on voluntary action by individual investigators and as long as the legal frameworks are unclear and only limited control is exercised over the sector, the possibility of misconduct and abuse of power still lurks. In this light, a useful analogy might be made with the 'principles-based' approach to (financial) regulation that has been applied pre-financial crisis. This Anglo-Saxon term for public control over private self-regulation within a broad public regulation framework (focusing on 'principles' rather than on prescriptive rules), in practice came down to de-regulation. Many commentators have linked this form of regulation to the financial crisis of 2008. In hind-sight it has become clear that this type of 'light-touch regulation' is vulnerable (Black, 2011). A crisis-trigger such as was available in the financial markets is not available in the context of corporate investigations and, as mentioned, there are few indications of gross abuses or major problems. However, the analogy with the 2008 credit crunch and the role of regulation in this, does alert us to vulnerabilities of such an approach. The focus on principles of law as guidelines for investigatory activities may be seen as a useful common ground to build upon in regulating the corporate security market. In absence of a widely-applicable permit system, much relies on the willingness of individual corporate investigators (and clients) to follow these principles of law and act upon a breach of said principles.

I would therefore suggest making the Wpbr [Law on Private Security Companies and Private Investigation Firms] and the Privacy code of conduct for private investigation firms applicable to all investigators who deal with individuals in their day-to-day business. This implies a shift by making the nature of the activities and the potential for breach of privacy of the subject of investigations the defining measure in asserting the applicability of the law, instead of the position of the investigators in relation to the client (CBP, 2007). This would mean that forensic accountants, forensic legal investigators and in-house investigators would all become required to get a permit. This is not a magic bullet in the sense that problems still remain. For example, the role of legal privilege should be determined, although case law seems to point in the

direction of non-applicability for investigative actions (see chapter 2). Another issue that still remains is the control over the permit holders. In the current system, the control of permits and compliance to the conditions of these permits is virtually non-existent. One of the reasons for this is that the police cannot spare the resources to provide effective control. This issue will be exacerbated when more investigators would be required to get a permit. I would suggest to both change the conditions of control – re-introducing some form of control on content, for example the yearly report private investigation firms had to submit in the past – and to place the control in the hands of another regulatory body. My suggestion would be the Dutch Data Protection Authority [*Autoriteit Persoonsgegevens* (AP)] as much of the applicable regulation is focused upon the WBP, the Dutch privacy law.

From the standpoint that corporate investigators are not a form of privatised police, placing the control in the hands of the Data Protection Authority makes more sense than the current situation in which the police organisation is responsible for control. The research shows that police/corporate investigator relations are *ad hoc* and often rather cumbersome. It would alleviate the pressure on police without being detrimental to their information position, since the current control system is virtually non-existent. *Ad hoc* relations between corporate investigators and police would continue to exist in cases in which pragmatic or normative considerations bring an incentive to corporate investigators and clients to involve law enforcement authorities in a case. For the Data Protection Authority such a change would provide a large workload. However, since the AP is involved with corporate investigators already, in approving the Privacy code of conduct, it would in my opinion be the most efficient and effective solution. Most of the concerns uttered about corporate investigators' activities are *not* about criminal acts (the realm of law enforcement) but about *breaches of privacy* (the realm of the AP). Furthermore, in a 2007 advisory letter to the Dutch government, the AP (at the time still called CBP) itself has suggested that it may be involved to a greater extent in the control over the permit system, stating that: "the CBP would gladly enhance the current cooperation[112] with regard to the permit system by being in charge of the control over compliance with the norms set in the Privacy code of conduct, although the CBP is currently lacking the capacity to do so" (CBP, 2007: 1). It would, therefore, be necessary to provide the Data Protection Authority with the additional resources required to act as an efficient regulator for the Wpbr-permit system.

Tightening control over corporate investigations and settlements in this way does produce more administrative work for corporate investigators. This was one of the reasons to exclude in-house corporate investigation units from the permit system (State secretary of justice & minister of the interior, 2009). In its search for legitimacy,

112 This cooperation is formed by the advice the Data Protection Authority provides to the minister of security and justice when a request for a permit is being assessed.

the corporate security sector seems to ask for a better system of control – at least the corporate security respondents in this research do. In addition, in the current situation many of those corporate investigators who are not obliged to have a permit either do have a permit or act like a permit holder by using the Privacy code of conduct. I would therefore not expect much resistance from the corporate security sector – indeed a wider and more effective permit system would be beneficial to the legitimacy of the market. Additionally, from a level playing field perspective, the new situation should benefit the market as a whole.

The above suggestions might mitigate some of the issues identified in this research, they will not abolish them completely. Much still depends on the willingness of individual corporate investigators and clients to use the principles of law such as protection of the involved persons as part of their non-contractual moral agency (Loader & White, 2017; see also section 6 above and chapter 4 and 5). The Privacy code of conduct is a useful tool but non-compliance to it will not lead to any consequences for the investigator as long as no-one knows about it. The changes in the control system suggested here would not lead to very extensive knowledge of individual cases: a very detailed description of every action in every investigation, or a standard mandatory insight in the investigation reports would be impractical and I believe, undesirable as well. As we have seen, the corporate security sector exists by virtue of its marketing of some strategic advantages (the use of secrecy, discretion and control; its legal flexibility (forum shopping) and the way economic crime is framed). If these characteristics cease to exist because of stringent regulation, clients would find different solutions, moving away from the professionalised and regulated corporate security market. It is not only corporate investigators who engage in forum shopping and strategic use of legal venues – the same may be said about their clients. Forum shopping is not undesirable per se (for the reason that it may just involve a search for an optimal outcome without negative side effects) – but it might lead to a situation in which either investigators or clients look for a specific context in which they are not regulated or accountable, which situation is objectionable from a rule-of-law point of view.

The nature of the professional activities of corporate investigators produces a focus on their private niche, which is not necessarily detrimental to public or private interests but it does lead to a sphere of obscurity. It is essential that a context is provided in which all who are involved may trust the quality of corporate investigations. This goes for the people investigated, for organisations using the services of corporate investigators (clients), for other corporate investigators, for law enforcement authorities and for the judicial system. In those instances in which law enforcement is involved, law enforcement actors should be able to rely on the professionalism of corporate investigators. As we have seen, trust is essential to public/private coexistence. Cooperation is possible

within the limits of the law, however the room for manoeuvre that exists is not much used because of trust issues (among other things). Non-compliance with the Privacy code of conduct may currently be corrected by legal representatives of the people involved, by law enforcement professionals, by a (civil or criminal) court and by clients. This however depends for a large part on the assertiveness of the involved person and the moral agency of clients. Only for private investigation firms, it may currently lead to loss of livelihood through forfeiture of the permit.

8.2 Revisiting the cooperation mantra

Extensive, long-term public/private cooperation is not realistic in the field of corporate security because of the structural characteristics of the market, as referred to above. It would therefore be wise to let go of the emphasis on public/private cooperation and focus on the social reality of public/private separation. In doing so, room will be created to value both the criminal justice system and the corporate security sector in their own right. The junior partner-perspective remains pervasive in public/private cooperation-talk but this research shows that the social reality is much more complicated than that. Efforts to streamline private cooperation in criminal justice procedures have as of yet been unsuccessful – maybe it is time to introduce a new approach.

Respondents (both private and public-sector) indicate that in the *ad hoc* contacts they have, trust and familiarity are important. The fraud contact points that have disappeared after a reorganisation of the Dutch police organisation are mentioned as being beneficial to the value of *ad hoc* contacts. Letting go of the emphasis on cooperation does not mean that *ad hoc* coexistence will cease to exist. Normative and pragmatic considerations from the corporate side, and (from the law enforcement perspective) criminal investigations in which corporate investigators are investigating as well, will continue to lead to *ad hoc* contacts. This research has introduced three general types of *ad hoc* contacts: private to public information transfer, (minor) mutual information sharing and coordination of actions. For all these types of coexistence, the reinstatement of (fraud) contact points would be beneficial. It would not solve the problem of different logics guiding the investigations; law enforcement officials may still feel the need to reproduce (part of) the investigations by using their powers of investigation in many cases. However, law enforcement respondents also suggest that in some cases they (would like to be able to) make only minor efforts before presenting the privately generated information to the court in a criminal justice procedure – if that information is useful and trustworthy. Familiarity between (public and private) investigators and mutual trust may make this more likely.[113] Similarly, the

113 Too much familiarity is not to be aspired either, since that may lead to collusion and informal (illegitimate) information sharing. As of yet, this does not seem to be a major concern in corporate investigator/police relations. However, it would be wise remain wary of the possibility.

information flow from public to private that may ensue in some cases may benefit from the (fraud) contact points. Currently, few law enforcement professionals seem to be aware of the possibilities for information sharing with corporate investigators and much is reliant on the willingness of individual prosecutors and investigators. Having a formal contact point, specialised in contacts with corporate investigators and clients, would potentially remove some of the hesitation. It would provide both public and private sector professionals with a point of entry based on contacts, when they are in need of one in a specific case. Furthermore, a knowledgeable point of reference may be valuable for both public and private sector professionals.

The above should be placed in the context of *ad hoc* coexistence rather than longer-term cooperation efforts. Corporate investigators and law enforcement professionals largely stay in their own sphere of action but meet on an *ad hoc* basis. Stating that we need to let go of the cooperation mantra does not mean that no form of cooperation will ensue in specific cases. However, it is not necessarily something to aspire to on a structural level.

9. Reflections – this research and beyond

Through this research I have endeavoured to shed light on the market for corporate investigations and corporate settlements. The research adds to criminological knowledge, both about the market itself and about public/private relations. The methodological approach chosen has allowed me to give a rich description and analysis of the subject, which was the goal of the research. A qualitative research approach, combining different methods through triangulation, has the advantage that it allows the researcher to explore the subject matter in-depth. The approach is also necessarily (and purposively) selective as it focuses on certain parts of the field. Here, the focus has been on the four main groups of corporate investigators – in-house security departments, private investigation firms, forensic accountants and forensic legal investigators. Because their day-to-day business was central to the research, a choice was made to select the majority of respondents from corporate investigators. For future research, it would be interesting to focus more specifically on the upcoming profession of forensic legal investigators. This research has consciously focused on the corporate security market in the broad sense of the word. Differences between the corporate investigator groups have been found, but there are enough similarities to claim that they are part of the same professional market and therefore, that they should be answerable to the same legal framework. Future research focusing on investigators with a specific professional background could provide even richer information on the day-to-day activities of corporate investigators. In doing so, one

might also focus on specific specialisations such as the ever more relevant corporate cyber investigations.

Furthermore, an emphasis in future research on clients, in the form of HR managers and general management, would be interesting, and may provide a deeper understanding of the choices made in corporate settlement procedures. Some practical issues may be attached to such an approach, since it is difficult to find clients of corporate investigative services (not much is publicised in for example the newspapers on corporate investigations), who are also willing to participate in such a research (as corporate investigations are based on discretion). In this research, clients were contacted using the snowball method by asking corporate investigators for contacts. Such an approach may prove effective in future research as well. Another innovative angle for research on corporate justice would be to focus on the involved people who have been subject to corporate investigations and corporate settlements. This is likely to be a hard-to-reach group. First of all, since corporate investigations and settlements are often not publicised, it is difficult to find involved people. Through contacts with corporate investigators and clients, names might be found but the focus on discretion and privacy regulation would make them unlikely to volunteer such information. Second, since there may be little or no linkage between potential respondents – unless they turn out to involve one or more 'rogue' corporate security providers or organised groups – snowballing from one such respondent to another would be impractical. Another way to receive information on involved persons would be to use case law of criminal or civil court cases in which internal investigations have (also) been done. This would, however, severely limit the scope of the research, as only a limited amount of cases in which corporate investigations have been done end up in court.

In addition to the new angles suggested above, it would be interesting to supplement the information retrieved through this research by a quantitative study. Although saturation was achieved in this research in the sense that no additional information or respondents resulted from the research after a certain point and this may be taken as an indication that the information gathered is valid and reliable, a quantitative study may provide specific information which cannot be derived from qualitative research methods. Such a study could map the number, skill-sets and technical resources of corporate investigators; how many organisations make use of their services; and which cases end up in the criminal justice system. For this, it may be very helpful if the permit system is expanded to all corporate investigators, since that would provide an overview of the scope of the corporate security market in the Netherlands. Such a research may thus have to be postponed until the time when the permit system is altered to include all professional corporate investigators.

This research is focused on corporate investigations into and corporate settlement of internal norm violations. Because the norm violations are internal, there are more options

to react to the norm violation than in cases in which the norm violation is external to the organisation. In addition, internal norm violations are often claimed (*inter alia* by respondents) to be more dangerous to an organisation than external threats (which may be reflected in the higher level of reports to the authorities for external crimes, see for example PwC, 2014). It would be interesting to compare the two types of norm violations in future research. In addition, a similar comparison could be made between criminal and non-criminal norm violations: is there a difference in the way organisations react to the different types of norm violations?

For reasons discussed in chapter 1, the role of regulatory agencies in the field of corporate security has not been a subject of this research. The aim of the research – to provide an overview of the Dutch corporate security sector – makes the inclusion of all (potentially relevant) regulatory agencies impractical. The fact that corporate investigators are used in a wide variety of (economic) sectors, means that in different situations a multitude of regulators may be involved. However, it would be possible (and interesting) to focus more specifically on the relationships between the regulatory agencies and corporate investigators within a specific sector. Examples may be the relationships corporate investigators may have with the Radio Communications Agency [*Agentschap Telecom*] when working in the context of the telecommunications sector, or the role of the Dutch Healthcare Authority [*Nederlandse Zorgautoriteit*] in relation to the health care sector. Especially if control over a renewed permit system would come to be exerted by the Data Protection Authority, therefore making that authority the regulator for the entire corporate security sector, it would be very interesting to look at the relations between this regulatory agency and corporate investigators. With regard to the extended role the Data Protection Authority would take in the control over the more elaborate permit system as suggested here, it would be relevant to do an impact study in future, to assess the way in which the changes would affect the different stake-holders.

One last strain of research that would be important to pursue is more international in nature. This is relevant because corporate investigators move across multiple national jurisdictions. The forum shopping activities (as discussed in chapter 4, section 1.2.1), choosing the most agreeable jurisdiction to be prosecuted (if the organisation itself is to blame), provide an example of the ease with which corporate investigators move across national boundaries (in stark contrast to the difficulties law enforcement agencies have with this). Finally, as noted in chapter 2 above, it would be useful to deploy a comparative perspective in order to explore to what extent the specific (regulatory) history of the Netherlands has affected the way in which the corporate security market has developed.

The strains of future research proposed here may build upon the insights provided in this research. Most importantly, it would be necessary to approach the corporate security sector as a semi-autonomous social field, without using the lens of a top-down state-centric discourse. The discourse promoted in this research theoretically

assesses corporate investigators as semi-autonomous actors, while also taking into account the role of the state as a key player – one that adds a normative ('retribution') dimension to corporate settlement solutions (when involved in that), and one that is the source of democratic control over the market. In further exploring the social realities of the corporate security market – and the coexistence of corporate investigators with law enforcement agencies and other state actors within it – it is important to stay clear of stereotypical portrayals of 'public' and 'private'. The non-contractual moral agency of corporate investigators, be that to provide themselves with legitimacy or out of normative concerns, creates space for other than purely commercial considerations. A key word describing the corporate security market is flexibility – it plays a pivotal role in the services provided, the legal frameworks applied, the interests served and in the relationships with public actors. It would be wise to bear this in mind in future work.

References and legislation

References

A

Abrahamsen, R. & Williams, M.C. (2011). *Security beyond the state. Private security in international politics.* Cambridge: Cambridge University Press.

Advocatie.nl (2015, September 9). *NS-onderzoek De Brauw inhoudelijk juist, schijn van partijdigheid niet opgeheven.* Retrieved from http://www.advocatie.nl/ns-onderzoek-de-brauw-inhoudelijk-juist-schijn-van-partijdigheid-niet-opgeheven.

AFM (2014). *Uitkomsten onderzoek kwaliteit wettelijke controles Big 4-accountantsorganisaties.* Amsterdam: Autoriteit Financiële Markten.

AFM (2015). *Dashboard 2015 voor Accountantsorganisaties*. Retrieved from https://www.afm.nl/nl-nl/professionals/doelgroepen/accountantsorganisaties/publicaties/dashboard.

AFM (2016). *AFM legt boetes op aan Big 4-accountantsorganisaties voor niet naleven zorgplicht.* Retrieved from https://www.afm.nl/nl-nl/professionals/nieuws/2016/mrt/boete-big4.

Almelo, L. van (2007). 'Wta is windowdressing'. Henk de Graaff en Marcel Pheijffer in discussie. *De Accountant, 2007*(4), 34-36.

Almelo, L. van (2013). De advocaat als investigator. *Advocatenblad, 93*(9), 25-27.

Almelo, L. van (2016). *Uitglijders. Lessen uit accountantstuchtrecht.* Amsterdam: NBA.

Almelo, L. van & Schimmel, P. (2014). *Feiten maken het recht. Een studie van Grant Thornton Forensic & Investigation Services naar een goed forensisch accountantsonderzoek*. Rotterdam: Grant Thornton.

AMS Advocaten (2015). *Enquêteprocedure*. Retrieved from http://www.amsadvocaten.nl/de-rechtsgebieden/ondernemingsrecht/de-enqueteprocedure/.

Aon (2017). *Global Risk Management Survey 2017*. Basel: Aon Global Risk Consulting.

B

Baarda, D.B., Goede, M.P.M. de & Meer-Middelburg, A.G.E van der (1996). *Basisboek Open interviewen. Praktische handleiding voor het voorbereiden en afnemen van open interviews.* Groningen: Stenfert Kroese.

Balter, R. & Bellissard, L. (2003). *A ScalAgent Distributed Technologies White Paper. Scalable and Flexible Mediation Infrastructure for Networked Smart Devices.* Échirolles: ScalAgent Distributed Technologies.

Batelaan, H. & Bos, J. (2003). *De particuliere beveiliging bewaakt? Evaluatie regelgeving particuliere beveiligingsorganisaties. Eindrapport.* Amsterdam: Regioplan beleidsonderzoek.

Beck, U. (1992). *Risk society: towards a new modernity*. London: Sage.

Beckers, J.J.H. (2017). *Tussen ideaal en werkelijkheid. Een empirische studie naar de strafrechtelijke aanpak van organisatiecriminaliteit in Nederland.* Rotterdam: Erasmus universiteit Rotterdam.

Beltzer, R.M. (2005). Ontbinding en WW: The show must stop. In R. Hansma (Ed.), *De ontbinding van de arbeidsovereenkomst in tienvoud. Werkgroep Ontslagrecht 1988-2005: Gijs Scholtens neemt ontslag!* (pp. 1-12). Deventer: Kluwer.

Berndtsson, J. (2012). Security professionals for hire: Exploring the many faces of private security expertise. *Millennium – Journal of international studies, 40*(2), 303-320.

Beyens, K., Kennes, P. & Tournel, H. (2016). Mijnwerkers of ontdekkingsreizigers? Het kwalitatieve interview. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve methoden en technieken in de criminologie* (pp. 187-222). Leuven: Acco.

Bijleveld, C.C.J.H. (2009). *Methoden en Technieken van Onderzoek in de Criminologie*. Den Haag: Boom Juridische Uitgevers.

Black, J. (2011). The rise, fall and fate of principles-based regulation. In K. Alexander & N. Moloney (Eds), *Law Reform and Financial Markets* (pp. 3-34). Cheltenham: Edward Elgar.

Blink, L.P. van den (2010). Enige ervaringen van een enquêteur. In K.M van Hassel & M.P. Nieuwe Weme (Eds.), *Willems' wegen. Opstellen aangeboden aan prof.mr. J.H.M. Willems* (pp. 55-62). Deventer: Kluwer.

Blonk, G., Haen, T., Lannoy-Walenkamp, B. de & Gelder, P. van (2017). *De fraudeaangifte. Startpunt voor een succesvolle strafrechtelijke belangenbehartiging*. Deventer: Vakmedianet.

Boutellier, H., Steden, R. van, Bakker, I., Mein, A. & Roeleveld, W. (2011). *De positie van de politie: een verkennende studie voor de strategische onderzoeksagenda politie*. Apeldoorn: Politieacademie.

Bunt, H.G. van de (2015). Ethische dilemma's bij criminologisch onderzoek. *Tijdschrift over Cultuur & Criminaliteit (5)*1, 55-69.

Bunt, H.G. van de, Holvast, N.L., Huisman, K., Meerts, C.A., Mein, A.G. & Struik, D. (2011). *Bestuurlijke rapportage vastgoedfraudezaak 'Klimop'.* Rotterdam/Utrecht: Erasmus School of Law/Verwey-Jonker Instituut.

Bunt, H. van de & Swaaningen, R. (2005). Privatisering van de veiligheidszorg. In L.C. Winkel, J.J.M. Jansen, H.O. Kerkmeester, R.J.P. Kottenhagen & V. Mul (Eds.), *Privatisering van veiligheid* (pp. 5-19). Den Haag: Boom Juridische Uitgevers.

Button, M. (1998). Beyond the public gaze – The exclusion of private investigators from the British debate over regulating private security. *International Journal of the Sociology of Law, 26*(1), 1-16.

Button, M. (2002). *Private policing.* Cullompton, Devon: Willan Publishing.

Button, M. (2004). 'Softly, softly', private security and the policing of corporate space. In R. Hopkins Burke, (Ed.), *Hard cop, soft cop: Dilemma's and debates in contemporary policing* (pp. 101-113).

C

CBP (2007). *Advies over het kabinetsstandpunt inzake het rapport "Publieke bemoeienis met particuliere beveiliging en recherche".* Den Haag: College Bescherming Persoonsgegevens.

CBP (2015a). *Controle van personeel.* Retrieved from https://www.cbpweb.nl/nl/onderwerpen/werk-uitkering/controle-van-personeel#news.

CBP (2015b). *Cameratoezicht op de werkplek. Do's en don'ts voor werkgevers.* Retrieved from https://cbpweb.nl/sites/default/files/atoms/files/cbp_cameratoezicht.pdf.

CBP (2015c). *Een zwarte lijst gebruiken.* Retrieved from https://www.cbpweb.nl/nl/onderwerpen/zwarte-lijst/een-zwarte-lijst-gebruiken?qa=zwarte%20lijst&scrollto=1.

CBP (2015d). *Cameratoezicht op de werkplek*. Retrieved from https://cbpweb.nl/nl/onderwerpen/cameratoezicht/cameratoezicht-op-de-werkplek.

Cleiren, C.P.M. (2001). Waarheid in het strafrecht: niet tot elke prijs. In C.P.M. Cleiren, R.H. de Bock & C.J.M. Klaassen (Eds.), *Het procesrecht en de waarheidsvinding. Preadviezen voor de Nederlandse vereniging voor procesrecht* (pp. 9-31). Den Haag: Boom Juridische Uitgevers.

Coburn, N.F. (2006). Corporate investigations. *Journal of Financial Crime, 13*(3), 348-368.

Cools, M., Davidovic, D., De Clerck, H. & De Raedt, E. (2010). The international private security industry as part of the European Union security framework: a critical assessment of the French EU presidency White Paper. In M. Cools, B. de Ruyver, M. Easton, L. Pauwels, P. Ponsaers, G. Vande Walle, T. Vander Beken, F. Vander Laenen, G. Vermeulen & G. Vynckier (Eds.), *EU and International Crime Control. Topical Issues* (pp. 123-136). Antwerpen: Maklu.

D

De Brauw (2015). *Definitief rapport van bevindingen, 2 november 2015, bestemd voor N.V. Nederlandse Spoorwegen*. Retrieved from https://zoek.officielebekendmakingen.nl/blg-614489.pdf.

Decorte, T. (2016). Kwalitatieve data-analyse. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve methoden en technieken in de criminologie* (pp. 463-512). Leuven: Acco.

Deloitte (2012). *Rapport inzake onderzoek bij Avalex inzake (informatieverstrekking over) Resultaat 2010, ten behoeve van het Dagelijks Bestuur van Avalex 30 maart 2012*. Retrieved from http://www.politiekdelft.nl/avalex_rapport_deloitte_20120330.pdf.

Dijk, F. Van & Waard, J.J. de (2001). De markt voor private opsporing; vraag en aanbod. *Justitiële Verkenningen, 27*(4), 25-41.

Dorn, N. & Levi, M. (2009). Private – Public or Public – Private? Strategic Dialogue on Serious Crime and Terrorism in the EU. *Security Journal, 22*, 302-316.

Dorn, N. & Meerts, C. (2009). Corporate security and private settlement: An informal economy of justice. In J. Shapland & P. Ponsaers (Eds.), *The Informal Economy and Connections with Organised Crime: The Impact of National Social and Economic Policies* (pp. 113-129). Amsterdam: Boom Publishers.

Dubbeld, L. (2015). Duizelingwekkend opleidingsaanbod voor security manager. *Security management, 2015*(februari). Retrieved from http://www.securitymanagement.nl/een-duizelingwekkend-opleidingsaanbod-voor-de-security-manager.

E

Eerste Kamer der Staten-Generaal (2014). *Memorie van Antwoord. Wijziging van verschillende wetten in verband met de hervorming van het ontslagrecht, wijziging van de rechtspositie van flexwerkers en wijziging van verschillende wetten in verband met het aanpassen van de Werkloosheidswet, het verruimen van de openstelling van de Wet inkomensvoorziening oudere werklozen en de beperking van de toegang tot de Wet inkomensvoorziening oudere en gedeeltelijk arbeidsongeschikte werkloze*

werknemers (Wet werk en zekerheid), Kamerstukken I, 2013-2014, 33818, C.

Erp, J. van, Huisman, W., Bunt, H. van de & Ponsaers, P. (2008). Toezicht en compliance. *Tijdschrift voor Criminologie, 50*(2), 83-95.

Eski, Y. (2016). *Policing, Port Security and Crime Control An Ethnography of the Port Securityscape*. Abingdon, Oxon: Routledge.

F

Faber, W. & Nunen, A.A.A. van (2002). *Het ei van Columbo. Evaluatie van het project financieel rechercheren*. Oss: Faber organisatie vernieuwing.

Falk Moore, S. (1973). Law and Social Change: The Semi-Autonomous Social Field as an Appropriate Subject of Study. *Law & Society Review, 7*(4), 719-746.

Fijnaut, C.J.C.F. (2002). Bedrijfsmatig georganiseerde particuliere opsporing en (het Wetboek van) s/Strafvordering. In M. Groenhuijsen & G. Knigge (Eds.), *Dwangmiddelen en rechtsmiddelen* (pp. 689-750). Deventer: Kluwer.

Fijnaut, C.J.C.F., Muller, E.R., Rosenthal, U. & Van der Torre, E.J. (Eds.) (2007). *Politie; studies over haar werking en organisaties.* Deventer: Kluwer.

Friperson, R., Bouman, S. & Wilms, P. (2013). *Samen opgespoord? Eindrapport "Pilot samenwerking particuliere onderzoeksbureaus met politie en OM"*. Den Haag: WODC.

Functioneel Parket (2014, November 12). *SBM Offshore N.V. betaalt US$ 240.000.000 wegens omkoping* [Press release]. Retrieved from https://www.om.nl/actueel/nieuwsberichten/@87202/sbm-offshore-betaalt/.

G

Garland, D. (2001). *The Culture of Control; Crime and Social Order in Contemporary Society.* Chicago: University Press.

Gemeente Rotterdam (2017). *Eindrapport enquêtecommissie Boompjeskade.* Rotterdam: Gemeente Rotterdam.

Gill, M. (2013). Engaging the corporate sector in policing: Realities and opportunities. *Policing, 7*(3), 273-279.

Gill, M. & Hart, J. (1997). Exploring investigative policing: A study of private detectives in Britain. *British Journal of Criminology, 37*(4), 549-576.

Gill, M. & Hart, J. (1999). Private security: Enforcing corporate security policy using private investigators. *European Journal on Criminal Policy and Research, 7*(2), 245-261.

Graaff, H.J. de (2007). *De juridische positie van forensisch accountants in Nederland.* Rotterdam: Erasmus Universiteit.

Grant Thornton (2010). *Grant Thornton Forensic & Investigation Services B.V. Reglement onderzoekswerkzaamheden*. Rotterdam: Grant Thornton.

Grant Thornton (2012). *Eindrapportage voor de gemeente Eindhoven inzake de totstandkoming van verhuis- en schadevergoedingen woonwagenbewoners Tongelresche Akkers en daarbij mogelijk opgetreden plichtsverzuim*. Retrieved from https://eindhoven.raadsinformatie.nl/document/184307/1/Bijlage_5_Grant_Thornton_eindrapport_TA.

Gunther Moor, L. & Vijver, C.D. van der (2001). Privatisering van opsporing; een kader voor normering. *Justitiële Verkenningen, 27*(4), 77-86.

H

Hagenaars, P.M.M. & Bonnes, J.M. (2014). *De kracht van privaat-publieke samenwerking. Succesfactoren in veiligheidsprojecten in het digitale tijdperk.* Den Haag: Boom Lemma uitgevers.

Henry, S. (1983). *Private justice. Towards integrated theorising in the sociology of law.* London: Routledge & Kegan Paul.

Hoffmann (2015). *Managementbrief II nr. 2140607, betreft onderzoek o.i.v. Gemeente Urk te Urk*. Retrieved from http://www.omroepflevoland.nl/SiteFiles/Doc/Rapport_onderzoek_naar_lek_E48A8C53F9EC9A01C1257DE400371DDF.pdf.

Hoogenboom, A.B. (1988). *Particuliere recherche: een verkenning van enige ontwikkelingen*. 's-Gravenhage: SDU uitgeverij.

Home Office (2013). *New regulation of private investigators to be introduced.* Retrieved from https://www.gov.uk/government/news/new-regulation-of-private-investigators-to-be-introduced.

Hoogenboom, A.B. (1988). *Particuliere recherche: een verkenning van enige ontwikkelingen*. 's-Gravenhage: SDU uitgeverij.

Hoogenboom, A.B. (1990). Rechtseconomie en particuliere beveiliging. 'Policing for profit' als voorloper van strafrechtelijke hervormingen? *Ars Aequi, 39*(10), 721-732.

Hoogenboom, A.B. (1994). *Het politiecomplex. Over de samenwerking tussen politie, bijzondere opsporingsdiensten en particuliere recherche.* Arnhem: Gouda Quint.

Hoogenboom, A.B. (2006). Grey intelligence. *Crime Law and Social Change, 45*(4-5), 373–381.

Hoogenboom, A.B. (2007). Grijs gebied tussen publiek en privaat bedreigt veiligheid. *Christen Democratische Verkenningen, winter 2007*, 58-65.

Hoogenboom, A.B. (2009). *De publiecke saeck; politie en veiligheid in een verwilderde wereld*. Den Haag: Boom Juridische Uitgevers.

Hoogenboom, A.B. & Muller, E.R (2002). *Voorbij de dogmatiek: publiek-private samenwerking in de veiligheidszorg*. Den Haag: COT.

I

Inspectie Openbare Orde en Veiligheid (2009). *Kwaliteit in particuliere veiligheid?! Politietoezicht op de particuliere beveiligingsorganisaties en recherchebureaus*. Den Haag: Inspectie Openbare Orde en Veiligheid.

Inspectie Veiligheid en Justitie (2005). *Naar samenwerken aan veiligheid. Onderzoek naar de uitvoering van de korpscheftaken in het kader van de Wet particuliere beveiligingsorganisaties en recherchebureaus*. Den Haag: Ministerie van Veiligheid en Justitie.

J

Janssen, J. (2011). Politie en wetenschap. *Tijdschrift voor Criminologie, 53* (2), 163-172.

Jennen, B.C.G. & Biemond, H.J.TH. (2009). Het interne fraudeonderzoek: enkele juridische overwegingen. *Tijdschrift voor de Ondernemingsrechtpraktijk, 4*(2), 57-61.

Johnston, L. (1992). *The Rebirth of Private Policing.* London: Routledge.

Jones, T. & Newburn, T. (1993). *Private Security and Public Policing*. Oxford: Oxford University Press.

Jones, T. & Newburn, T. (2006). Understanding plural policing. In T. Jones & T. Newburn (Eds.), *Plural policing. A comparative perspective* (pp. 1-11). Abingdon, Oxon: Routledge.

K

Kerkmeester, H.O. (2005). Privatisering van veiligheid: economische aspecten. In L.C. Winkel, J.J.M. Jansen, H.O. Kerkmeester, R.J.P. Kottenhagen & V. Mul (Eds.), *Privatisering van veiligheid* (pp. 79-93). Den Haag: Boom Juridische Uitgevers.

Keupink, B.J.V. & Tillema, A.J.P. (2013). Ontwikkelingen in het verschoningsrecht. *Ondernemingsrecht, 60*(8), 307-310.

Klerks, P. (2008). Terughoudend toezicht op omvangrijke private recherche. *Tijdschrift voor veiligheid, 7(*4), 9-19.

Klerks, P. & Eysink Smeets, M. (2005). *Particuliere recherche; uitbreiding van de reikwijdte van de wet? Eindrapportage.* Apeldoorn: Politieacademie.

Klerks, P., Meurs, C. van & Scholtes, M. (2001). *Particuliere recherche: werkwijzen en informatiestromen.* Den Haag: ES & E.

Klerks, P. & Scholtes, M. (2001). Particuliere recherche; een informatiemarkt in ontwikkeling. *Justitiële Verkenningen, 27*(4), 9-24.

Koevoets, M.M. (2004). Onrechtmatig verkregen bewijs in het arbeidsrecht. *Arbeidsrechtelijke annotaties 3*(3), 39-58.

Kolthoff, E. (2015). Publiek integriteitsonderzoek door private partijen. In P. Ponsaers, E. De Raedt, L. Wondergem & L. Gunther Moor (Eds.) *Outsourcing policing. Cahiers Politiestudies 2015-3, nr.36* (pp. 163-176). Antwerpen: Maklu uitgevers.

Kuin, M.C. & Wilms, P.J.M. (2015). *Publiek-private opsporing: vele handen maken licht werk? Eindrapport Evaluatie vervolgpilot samenwerking particuliere onderzoeksbureaus met politie en Openbaar Ministerie*. Den Haag: WODC.

L

Laenen, F. Vander & O'Gorman, A. (2016). Ethische aspecten van het kwalitatief onderzoek. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve methoden en technieken in de criminologie* (pp. 555-586). Leuven: Acco.

Leys, M. Zaitch, D. & Decorte, T. (2016). De gevalsstudie. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve methoden en technieken in de criminologie* (pp. 161-186). Leuven: Acco.

Loader, I. (1997). Thinking Normatively about Private Securtity. *Journal of Law and Society, 24*(4), 337-394.

Loader, I. & Walker, N. (2006). Necessary virtues: the legitimate place of the state in the production of security. In J. Wood & B. Dupont (Eds.), *Democracy, Society and the Governance of Security* (pp. 165-195). Cambridge: Cambridge University Press.

Loader, I. & White, A. (2017). How can we better align private security with the public interest? Towards a civilizing model of regulation. *Regulation & Governance, 11*(2), 166-174.

Lugt, B.W.M. van der (2001). Waarborgen voor private opsporing. *Justitiële verkenningen, 27*(4), 65-76.

M

Maesschalk, J. (2016). Methodologische kwaliteit in het kwalitatief onderzoek. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve methoden en technieken in de criminologie* (pp. 131-160). Leuven: Acco.

Mascini, P. & Erp, J. van (2014). Regulatory governance: Experimenting with new roles and instruments. *Recht der werkelijkheid, 35*(3), 3-11.

Marx, G.T. (1987). The interweaving of public and private police in undercover work. In C.D. Shearing & P.C. Stenning (Eds.), *Private policing* (pp. 172-193). Newbury Park, CA: Sage Publications.

Meershoek, A.J.J. & Hoogenboom, A.B. (2012). Drieënvijftig tinten grijs. Afnemende verantwoording van en controle op hybride politiewerk. *Justitiële Verkenningen, 38* (5), 10-23.

Meerts, C. (2013). Corporate security – private justice? (Un)settling employer-employee troubles. *Security Journal, 26*(3), 264-279.

Meerts, C. (2014a). Over pragmatisme en strategie. *Tijdschrift voor Criminologie, 56*(4), 115-137.

Meerts, C.A. (2014b). Corporate security: Governing through private and public law. In K. Walby & R. Lippert (Eds.), *Corporate security in the 21st century. Theory and practice in international perspective* (pp. 97-115). Basingstoke: Palgrave Macmillan.

Meerts, C.A. (2016). A world apart? Private investigations in the corporate sector. *Erasmus Law Review, 9*(4), 162-176.

Meerts, C.A. & Dorn, N. (2009). Corporate security and private justice: danger signs? *European Journal of Crime, Criminal Law and Criminal Justice, 17*(2), 97-111.

Minister of security and justice (2013). *Brief van de minister d.d. 28-02-2013*, nr. 352870.

Minister of security and justice (2015). *Antwoorden kamervragen over de rol van advocaten en accountants bij fraudeonderzoeken*, Kamerstukken II, 2014–2015, Aanhangsel, nr. 2098.

Minister of security and justice (2016). *Brief van de minister van Veiligheid en Justitie*, Kamerstukken II, 2015–2016, 29279, nr.334.

Ministry of Social Affairs and Employment (2015a). *Informatie voor werkgevers. Ontslag wegens verwijtbaar handelen of nalaten van de werknemer.* Den Haag: Ministerie van Sociale Zaken en Werkgelegenheid.

Ministry of Social Affairs and Employment (2015b). *Informatie voor werkgevers. Ontslag wegens verstoorde arbeidsverhouding.* Den Haag: Ministerie van Sociale Zaken en Werkgelegenheid.

Ministry of Social Affairs and Employment (2015c). *Informatie voor werkgevers. De werkgever ontslaat de werknemer op staande voet.* Den Haag: Ministerie van Sociale Zaken en Werkgelegenheid.

Mortelmans, D. (2016). Het kwalitatieve onderzoeksdesign. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve methoden en technieken in de criminologie* (pp. 81-130). Leuven: Acco.

Mr. Online (2016). *Gedragsregels advocaat toe aan opfrisbeurt*. Retrieved from http://www.mr-online.nl/juridisch-nieuws/29721-gedragsregels-advocaat-toe-aan-opfrisbeurt.

N

Nalla, M. & Morash, M. (2002). Assessing the scope of corporate security: Common practices and relationships with other business functions. *Security Journal, 15*(3), 7-19.

NBA (2014). *Verordening gedrags- en beroepsregels accountants.* Amsterdam: NBA.

NBA (2016). *Regelgeving en wettelijke eisen PE.* Retrieved from https://www.nba.nl/Voor-leden/Permanente-educatie/Algemene-informatie-PE/.

NIVRA/NOvAA (2010). *NBA-handreiking 1112. Praktijkhandleiding persoonsgerichte onderzoeken voor accountants-administratieconsulenten/registeraccountants.* Amsterdam: Koninklijke Nederlandse Beroepsorganisatie voor Accountants.

Noaks, L. & Wincup, E. (2004). *Criminological research. Understanding qualitative methods.* London: Sage publications.

NOS (2016, October 24). *Een cyberaanval kan je beter stil houden*. Retrieved from http://nos.nl/artikel/2139346-een-cyberaanval-kan-je-beter-stilhouden.html.

NRC (2017, May 11). *Onderzoek VW moet openbaar.* Retrieved on 03-08-2017 from https://www.nrc.nl/nieuws/2017/05/11/onderzoek-vw-moet-openbaar-8776397-a1558098.

NRC (2015, June 30). *Zeven NS-medewerkers gestraft voor fraude bij aanbesteding Limburg.* Retrieved from http://www.nrc.nl/nieuws/2015/06/30/zeven-ns-medewerkers-gestraft-voor-onregelmatigheden-ov-aanbesteding-limburg-a1415088.

NVb (2014). *Informatie-uitwisseling politie en particuliere beveiliging.* Gorinchem: Nederlandse Veiligheidsbranche.

NVb (2015). *Privacygedragscode sector particuliere onderzoeksbureaus van de Nederlandse Veiligheidsbranche.* Gorinchem: Nederlandse Veiligheidsbranche.

NVB (2016). *Factsheet Veiligheid en fraude.* Amsterdam: Nederlandse Vereniging van Banken.

O

Ontslag.nl (2014). *Wat is een pro forma ontbindingsprocedure en waar dient deze procedure voor?* Retrieved from https://ontslag.nl/ontslagprocedure-bij-kantonrechter/wat-een-pro-forma-ontbindingsprocedure/.

P

Pemberton, A. & Reynaers, S. (2011). The controversial nature of victim participation: therapeutic benefits in victim impact statements In E. Erez, M. Kilchlinh, & J.J.M. Wemmers (Eds.), *Therapeutic jurisprudence and victim participation in justice: International perspectives* (pp. 229-248). Durham, North Carolina: Carolina Academic Publishing.

Perry, J. & Fontnouvelle, P. De (2005). *Measuring reputational risk: The market reaction to operational loss announcements. Working paper.* Boston: Federal Reserve Bank of Boston.

Peters, F.M. (2006). Who is afraid of the Ondernemingskamer. *Corporate Finance jaargids 2006,* 1-8.

Piret, J.M. (2005). Privatisering van veiligheid: ideologische en rechtsstatelijke aspecten. In L.C. Winkel, J.J.M. Jansen, H.O. Kerkmeester, R.J.P. Kottenhagen, & V. Mul (Eds.), *Privatisering van veiligheid* (pp. 39-54). Den Haag: Boom Juridische Uitgevers.

PwC (2014). *Economic crime survey Nederland 2014*. Amsterdam: PricewaterhouseCoopers.

PwC (2017). *Economic crime survey Nederland 2017.* Amsterdam: PricewaterhouseCoopers.

R

Radar (2015). *Woekercompensatie onder het tapijt geveegd.* Retrieved from https://radar.avrotros.nl/uitzendingen/gemist/26-10-2015/woekercompensatie-onder-het-tapijt-geveegd/.

Reemst, L. van (2016). A theoretical framework to study variations in workplace violence experienced by emergency responders. *Erasmus Law Review, 9*(3), 135-145.

Rense, J.F. (2004). De private onderzoeker; (ver)plicht tot hoor en wederhoor? *Maandblad voor Accountancy en Bedrijfseconomie, 78*(3), 76-80.

Reynaers, A. & Graaf, G. de (2014). Public values in public-private partnerships. *International journal of public administration, 37*, 120-128.

Rijksoverheid (n.d.) *Factsheet convenanten.* Retrieved from https://www.kcwj.nl/kennisbank/integraal-afwegingskader-beleid-en-regelgeving/6-wat-het-beste-instrument/61/convenant?cookie=yes.1502366816373-1475345741.

Rijksoverheid (2011). *Convenantsamenwerking en informatie-uitwisseling Electronic Crimes Task Force.* Retrieved from https://www.rijksoverheid.nl/documenten/convenanten/2011/03/15/convenant-samenwerking-en-informatie-uitwisseling-electronic-crimes-task-force.

Roks, R.A. (2016). *In tha H200d. Een eigentijdse etnografie over de inbedding van criminaliteit en identiteit.* Rotterdam: Erasmus Universiteit Rotterdam.

Rovers, G.B. & Vries Robbé, E. de (2005). *Interne criminaliteit in de logistieke sector*. 's-Hertogenbosch/ Den Haag: Bureau voor Toegepast Veiligheidsonderzoek/Boom Juridische uitgevers.

Ruth, A. van & Gunther Moor, L. (1997). *Lekken of verstrekken? De informele informatie-uitwisseling tussen opsporingsdiensten en derden.* Ubbergen: Uitgeverij Tandem Felix.

S

Schaap, C.D. (2008). *De private forensisch fraudedeskundige. Een feitelijke en juridische positionering*. Nijmegen: Wolf Legal Publishers.

Schaap, C.D. (2013). Vergeten componenten? *Tijdschrift voor Sanctierecht & Compliance, 2013*(2/3), 57-61.

Schimmel, P. (2011). *Fraudebeheersing; een leidraad van preventie tot detectie.* Deventer: Kluwer.

Shearing, C.D. (1992). The Relation between Public and Private Policing. *Crime and Justice, 15*, 399-434.

Shearing, C.D & Stenning, P.C. (1981). Modern Private Security: Its Growth and Implications. *Crime and Justice, 3*, 193-245.

Shearing, C. & Stenning, P. (1983). Private Security: Implications for Social Control. *Social Problems, 30*(5), 493-506.

South, N. (1988). *Policing for profit: the private security sector.* London: Sage.

Staatscourant, 6 juli 2000. *Selectielijst handelingen Minister van Justitie en onder hem ressorterende actoren op beleidsterrein weerkorpsen en beveiligingsorganisaties.*

Staatscourant, 2 oktober 2006, nr. 191. *Wijziging regeling particuliere beveiligingsorganisaties en recherchebureaus.*

Staatscourant, 1 april 2014, nr. 9654. *Beleidsregels particuliere beveiligingsorganisaties en recherchebureaus*.

State secretary of justice and minister of the interior (2009). *Brief van de staatssecretaris van justitie en de minister van binnenlandse zaken en koninkrijksrelaties.* Kamerstukken II, 2008-2009, 29 279, nr.93.

State secretary of security and justice, 2016 (2016). *Kamerbrief met beleidsreactie op rapporten van de Inspectie Veiligheid en Justitie naar uitvoering korpscheftaken Wwm en Wpbr*. Kamerstukken II, 2015–2016, 29 628, nr. 629.

Steden, R. van (2009). Burgerparticipatie in lokale veiligheidsnetwerken: over 'nodale sturing' en 'verankerd pluralisme'. *Justitiële Verkenningen, 35*(1), 29-42.

Steden, R. van & Huberts, L. (2006). The Netherlands. In T. Jones & T. Newburn (Eds.), *Plural policing. A comparative perspective* (pp. 12-33). Abingdon, Oxon: Routledge.

Steenhuis, D.W. (2011). *Particulier onderzoek in strafzaken; An offer hardly to be refused*. Gorinchem: Nederlandse Veiligheidsbranche.

Stenning, P. (2000). Powers and accountability of private police. *European Journal on Criminal Policy and Research, 8*(3), 325-352.

Sutherland, E.H. (1940). White-Collar Criminality. *American Sociological Review, 5*(1), 1-12.

T

Thumala, A., Goold, B. & Loader, I. (2011). A tainted trade? Moral ambivalence and legitimation work in the private security industry. *The British journal of sociology, 62*(2), 284-303.

TNS Nipo/WODC (2011). *Monitor criminaliteit bedrijfsleven 2010. Feiten en trends inzake aard en omvang van criminaliteit in het bedrijfsleven.* Amsterdam: TNS Nipo.

V

Verhoeven, M. (2015, September 30). De togacolumn: Met deze recherche valt geen fraude op te sporen. *NRC Handelsblad.* Retrieved from https://www.nrc.nl/nieuws/2015/09/30/de-togacolumn-met-deze-recherche-valt-geen-fraude-op-te-sporen-a1480980.

Vries Robbé, E. de, Cornelissens, A. & Ferweda, H. (2009). *Ambtscriminaliteit aangegeven? Een onderzoek naar het opvolgen van en kennis over de wettelijke verplichting tot aangifte van artikel 162 Sv misdrijven*. Arnhem: Advies- en Onderzoeksgroep Beke/WODC.

W

Walby, K. & Lippert, R. (Eds.) (2014), *Corporate Security in the 21st Century: Theory and Practice in International Perspective*. Basingstoke: Palgrave Macmillan.

Weber, M. (1946). Politics as a Vocation. In H.H. Gerth and C. Wright Mills (Eds.), *From Max Weber: Essays in Sociology* (pp. 77-128). New York: Oxford University Press.

Werkgroep toekomst accountantsberoep (2014). *In het publiek belang. Maatregelen ter verbetering van de kwaliteit en onafhankelijkheid van de accountantscontrole.* Amsterdam: NBA.

White, A. (2014). Beyond the regulatory gaze? Corporate security, (in)visibility, and the modern state. In K. Walby & R. Lippert (Eds.), *Corporate security in the 21st century. Theory and practice in international perspective* (pp. 39-55). Basingstoke: Palgrave Macmillan.

Whytock, C.A. (2010). The evolving forum shopping system. *Cornell Law Review, 96*(3), 481-534.

Wijk, J. van, Huisman, W., Feuth, T & Bunt, H.G. van de. (2002). *Op deugdelijke grondslag. Een explorerende studie naar de forensische accountancy*. Zeist: Uitgeverij Kerckebosch.

Williams, J.W. (2005). Reflections on the private versus public policing of economic crime. *British Journal of Criminology, 45*(3), 316-339.

Williams, J.W. (2006a). Governability matters: the private policing of economic crime and the challenge of democratic governance. *Policing and Society, 15* (2), 187-211.

Williams, J.W. (2006b). Private legal orders: professional markets and the commodification of financial governance. *Social & Legal Studies, 15*(2), 209-235.

Williams, J.W. (2014). The Private Eyes of Corporate Culture: The Forensic Accounting and Corporate Investigation Industry and the Production of Corporate Financial Security. In K. Walby & R. Lippert (Eds.), *Corporate Security in the 21st Century. Theory and Practice in International Perspective* (pp. 56-77). Basingstoke: Palgrave Macmillan.

Wood, J. & Shearing, C. (2007). *Imagining security.* Devon: Willan Publishing.

Y

Yar, M. (2011). From 'the governance of security' to 'governance failure': refining the criminological agenda. *Internet Journal of Criminology, 2011*, 1-19.

Z

Zaitch, D., Mortelmans, D. & Decorte, T. (2016). Etnografie en participerende observatie. In T. Decorte & D. Zaitch (Eds.), *Kwalitatieve methoden en technieken in de criminologie* (pp. 255-319). Leuven: Acco.

Legislation

Advocatenwet
[Law on the legal profession]
Bpbr – Beleidsregels private beveiligingsorganisaties en recherchebureaus
[Decree on Private Security Companies and Private Investigation Firms]
Bta – Besluit toezicht accountantsorganisaties
[Decree on the Control over Accountants]
BW – Burgerlijk Wetboek
[Civil Code]
Politiewet
[Police Law]
Rpbr – Regeling private beveiligingsorganisaties en recherchebureaus
[Regulation on Private Security Companies and Private Investigation Firms]
Rv – Burgerlijk procesrecht
[Code of Civil Procedure]
Verordening op de advocatuur
[Ordinance on the Legal Profession]
Verordening op de beroepseed voor accountants
[Ordinance on the Professional Oath for Accountants]
Wab – Wet op het accountantsberoep
[Law on the Accountancy Profession]
WBP – Wet bescherming persoonsgegevens
[Data Protection Act]
Wed – Wet op de economische delicten
[Law on Economic Crimes]
Wft – Wet op het financieel toezicht
[Law on Financial Institutions]
Wjsg – Wet justitiële en strafvorderlijke gegevens
[Law on Judicial Data]
Wob – Wet openbaarheid van bestuur
[Law on Governmental Transparency]
Wpbr – Wet particuliere beveiligingsorganisaties en recherchebureaus
[Law on Private Security Companies and Private Investigation Firms]
Wpol – Wet politiegegevens
[Law on Police Data]
Wta – Wet toezicht accountantsorganisaties
[Law on the Control over Accountants]

Wtra – Wet tuchtrechtspraak accountants
[Law on Disciplinary Proceedings for Accountants]
WvSr – Wetboek van Strafrecht
[Criminal Code]
WvSv – Wetboek van Strafvordering
[Code of Criminal Procedure]
Wwft – Wet ter voorkoming van witwassen en financieren van terrorisme
[Law Preventing Money Laundering and the Funding of Terrorism]

Case law[114]

ECLI:NL:GHSHE:2006:AY1071 [Court of Appeal of Den Bosch]
ECLI:NL:TADRSHE:2012:YA2502 [Council of Discipline Den Bosch]
ECLI:NL:TAHVD:2013:33 [Disciplinary Court of Appeals Lawyers]
ECLI:NL:HR:2014:942 [Supreme Court of the Netherlands]
ECLI:NL:RBDHA:2015:248 [Court of The Hague]
ECLI:NL:HR:2015:3714 [Supreme Court of the Netherlands]
ECLI:NL:TACAKN:2016:49 [Accountancy Chamber]
ECLI:NL:CBB:2016:118 [Court for Trade and Industry]
ECLI:NL:RBOBR:2016:7193 [Court of Eastern-Brabant]

114 The abbreviation 'ECLI' means European Case Law identifier. The abbreviation following that denotes the country, in this case the Netherlands ('NL'). The abbreviations that are presented after the country code identify the type of court. The explanations of these abbreviations are given above.

Summaries

Summary

This research answers the following central research question in relation to the market for corporate investigations in the Netherlands: *What is corporate security, how can its shifting relationship with law enforcement be conceptualised and what is its significance for the wider society?* To answer this question, information was gathered with the aid of qualitative research methods. Fieldwork consisted of interviews, observations and case studies. 59 semi-structured interviews were conducted with corporate investigators (33), law enforcement professionals (16) and clients (10). The two (full-time) observations were done to get to a better understanding of the daily activities of corporate investigators. The first observation took place with a private investigation firm and lasted seven weeks. The second observation took place with an in-house security department and lasted six weeks. Additionally, 21 case studies were analysed as a result of the observations. In this summary, the key findings of the research are discussed as reported in the main text.

The corporate security sector consists of professionals, providing specialised and tailor-made 'high-end' security services to their clients. Although corporate investigators may be involved in additional activities (such as pre-employment screenings and drafting and implementing integrity codes), this research focuses on the investigative activities of corporate investigators: mainly forensic accountancy, (private) investigations more generally, IT-investigations, asset tracing, and (assistance with) settlement and prevention tactics. There are four main groups of corporate investigators in the Netherlands: private investigation firms, in-house security departments, forensic accountants and forensic legal investigators. The research focuses on the activities of corporate investigators in relation to internal norm violations (within the employee/employer relationship).

One of the main concerns of this research is the conceptualisation of the corporate security sector. The junior partner theory and loss prevention theory provide us with two competing arguments: on the one hand the private security sector is seen as a subordinate to a dominant public sector, complementing this sector when necessary (junior partner theory). On the other, the private security sector is seen as the private equivalent of the criminal justice system, doing the same types of investigations and providing private justice to its clients; a strict distinction between public and private cannot be made (loss prevention theory). The ideas related to nodal theory may also be relevant to the corporate security market. In short, nodal theory suggests that that security is provided by a range of different providers, from which security consumers may choose. The state is seen as one of these providers but not as the primary one. In addition to the nodal perspective on security, another pluralistic perspective is that of

anchored pluralism, which similarly holds that the security market is characterised by fragmentation and pluralism but contrary to the nodal standpoint, it does prioritise the state over other venues of security. The anchored pluralism stance is that the state still has a vital role to play as the main provider of justice, and as the legal 'anchor' of security provided by private actors.

The above theories all (implicitly or explicitly) use the state as the theoretical point of departure. Whether it is a matter of privatisation and responsibilisation (conscious acts by the state) or a matter of (unintentional) growth of mass private property, the assumption remains that the state was present in a dominant way and that this presence is diminishing. As will be apparent from what follows below, the role of the state is better conceptualised by its *absence*, when it comes to internal norm violations within organisations. Many internal norm violations never reach the criminal justice system. When the norm violation is reported to law enforcement authorities, this report is often used as a supplement to a corporate settlement solution (which effectively reverses the argumentation of junior partner theory) and corporate investigators and law enforcement actors should be viewed as functionally different for several reasons (which effectively refutes the argument of loss prevention and pluralistic perspectives that there is interchangeability and competition between public and private (corporate) security actors). The growth of the market for corporate investigations should rather be seen as a commodification of the dark number of internal norm violations. The perspective taken in this research is that the corporate security sector acts with a high degree of flexibility within a semi-autonomous social field, both in relation to investigative activities and in relation to other actors. In this context, the state remains a key player, by adding a normative ('retribution') dimension to corporate settlement solutions and as the source of democratic control over the market. The perspective in this book may, then, be regarded to be a reconsideration of the state-centric discourse, one that takes the semi-autonomous position of corporate investigators as the point of departure, while also being sensitive to the role of the state.

The legal bases of corporate investigations are found in multiple legal frameworks. Other than general laws such as the Criminal Code and the Data Protection Act, an overarching legal framework is not available to corporate investigators. Only for private investigation firms does a specific law exist in the form of the Law on Private Security Companies and Private Investigation Firms [Wpbr], and most notably the Privacy code of conduct which is attached to that law. As a consequence, only those corporate investigators who work in a private investigation firm are obliged to get a permit. For forensic accountants and forensic legal investigators, the general legislation applies which is created for the professions of accountant and lawyer.

In addition, guidelines for person-oriented investigations (which are based on principles of law) are available to forensic accountants. In-house investigators are predominantly regulated by internal regulations. Even though the legal frameworks of the various corporate investigators differ, in practice most corporate investigators seem to follow the Privacy code of conduct for private investigation firms. Corporate investigators also stress the importance of principles of law and normative considerations as guiding norms, applying principles of law such as proportionality, subsidiarity and fair play to their day-to-day activities. The different legal frameworks provide clients and corporate investigators with the possibility of forum shopping. The control over corporate investigators' activities is limited and relies for a large part on involved individuals, corporate investigators and clients. Examples of abuse by corporate investigators are rare; however, the lack of effective (democratic) control and the fragmented nature of legal frameworks create possibilities for such abuse.

Partly as a result of the differences in legal frameworks, the various groups of investigators identified in this research have specific selling points relative to the others. In-house investigators' strong suit is that they are highly knowledgeable with regard to the client organisation. Private investigation firms, on the other hand, are more general in their services and because they are external to the organisation, they are regarded to be more independent. Forensic accountants are independent as well, and in addition they are the experts on financial investigations. Forensic legal investigators, finally, add legal knowledge to the investigations, providing a client with a legal interpretation and assistance with settlements. Although the various investigators lay emphasis on these differences, thus taking commercial advantage of the dissimilarities, corporate investigation units tend to diversify the background of employees, combining the different professional groups to be able to respond to clients' investigative demands. Corporate investigators tend to also set themselves apart from law enforcement authorities, by using different language (avoiding criminal justice terminology). Corporate investigators do not view themselves as a private police force.

With regard to the corporate investigation process, some generalities may be discerned. Corporate investigations start with an assignment from the client. In this assignment, corporate investigators try to ensure that their investigations will be executed independently and objectively. Investigations remain dependent on the client though: the client determines the scope of the investigations and his private interests are central to the investigations. Furthermore, much information used in corporate investigations is information that is available to the client as an employer – and by extension, to corporate investigators. In this way, corporate investigators have many investigative possibilities, in spite of the fact that they lack the powers of investigation

granted to law enforcement officials. As a consequence, corporate investigators are to a considerable extent reliant on the cooperation of the organisation and the individuals involved. Cooperation by the involved person is only voluntary to a certain extent, as the organisation may use its position as an employer to pressure an involved person into cooperating. While choosing the methods of investigation, corporate investigators tend to apply the principles of law of proportionality, subsidiarity and due process. The most commonly used sources of information by corporate investigators are internal documentation (financial administration, contracts); internal systems (communications systems such as email and telephone; data carriers such as computers; and employee systems such as entrance registration); open sources (databases, (social) media); and personal communications (the interview). Other sources such as observations, site visits or information derived from a criminal justice procedure may also be used. The interview with the involved person is generally done at the end of the investigations. In this way, investigators are able to confront the involved person with the information already gathered. In line with the adversarial principle, the interviewed person is given the opportunity to react to the interview report. After the investigations have been finalised, a draft report is made, and, in accordance with the adversarial principle, provided to the involved person. After the subjects of the investigations have had the opportunity to react to the draft report, the final report is submitted to the client.

After the report has been finalised, a settlement of the matter is often sought. Several reasons may be identified which make the use of corporate investigators with regard to both investigations and settlements appealing to organisations. Corporate investigators are not bound to the definitions of behaviour given by criminal law, nor by the (often slow and bureaucratic) structures of the criminal justice procedure. As a result, they may offer a high level of flexibility in investigative methods and solutions. Secondly, the orientation in corporate investigations is on the client and the private troubles the client may have, rather than on criminal acts (which are defined in the Dutch criminal justice system as being against society). This means that whatever norm violation is deemed harmful by an organisation may be investigated by corporate investigators (and the assignment may also be limited to that specific norm violation). Thirdly, corporate investigations provide an organisation with a high level of discretion and a certain measure of control over the process and information flow. These circumstances combine to make corporate investigations and corporate settlements appealing to organisations: organisations tend to prefer not to report to law enforcement authorities.

Considerations against reporting to law enforcement authorities are, then, a loss of control over information and over the process; the (limited) scope of behaviours that fall within the reach of criminal law; the limits to solutions provided by the criminal justice system; and a low level of confidence in the problem-solving capabilities of

the criminal justice system. However, a report to the authorities may still be made as an addition to a corporate settlement, based on pragmatic (strategic behaviour) and normative considerations. Powers of investigation may be necessary to retrieve valuable information. Another pragmatic consideration may be provided by forum shopping possibilities, based on the use of the *ne bis in idem* principle: being prosecuted in the Netherlands may prove beneficial to an organisation because it may soften prosecutors and judges in jurisdictions which are regarded to be harsher with regard to white-collar crime. A need for retribution or a sense of obligation towards society constitute examples of normative considerations. Corporate settlements may be provided through different legal venues. In addition to the option of using the criminal justice system by reporting to law enforcement authorities, the private law system may be used by filing a civil suit to reclaim damages or to terminate the labour agreement, by going through a *pro forma* procedure or by initiating a process with the Enterprise court. In addition, the private law system may be used to end the labour contract through a settlement agreement. Internal regulations may be used to discipline the employee, ranging from administering a warning to a summary dismissal.

The nature and composition of the corporate security sector, and the types of norm violations corporate investigators deal with (internal, white-collar norm violations), make long-term cooperation between private and public actors fundamentally difficult. As a result, public/private relations are better conceptualised as (*ad hoc*) coexistence than cooperation. Most notably, the fragmented nature of the corporate security market, the diffuseness of interests involved and the fact that, in the end, it is the client who decides about involving the authorities, make long-term cooperation very difficult. Corporate security as a market thrives by the grace of its use of flexibility in the framing of economic crime; secrecy, discretion and control; and legal flexibility and responsiveness to clients' needs. The market exists *because* of the possibility of separation from and coexistence with (and sometimes strategic use of) law enforcement. Two pilots, meant as a way to formalise the participation of corporate investigators in criminal justice investigations, were not very successful as a result of the above reasons. A conclusion, then, is that public/private relationships are not easily captured within existing theories of private security. A typology of *ad hoc* coexistence, rather than cooperation, is introduced, ranging from 'private to public transfer of information' (type A), through '(minor) mutual information sharing' (type B) to 'coordination of actions' (type C). Type A, private/public information transfer, may either occur as a sequence (law enforcement authorities being involved only after corporate investigators have finished their investigations) or may run parallel (law enforcement authorities being the initiator of the investigations, or corporate investigators inviting law enforcement authorities in at an early stage). When

investigations occur as a sequence, corporate investigators are usually not involved beyond providing criminal justice authorities with the corporate investigations report through an official report. When investigations run parallel, mutual information sharing may ensue but more commonly the public and private investigations remain separate – and again the involvement of corporate investigators (begins and) ends with the transfer of privately generated information through an official report to the authorities. Type B, minor mutual information sharing, includes information flowing not just from private to public, but also in the other direction. This type of information sharing is less prevalent according to respondents. In most instances, the majority of information still flows from private to public; however corporate investigators may also receive something in return. This information is often rather general, being more about investigative activities than investigative results (for example corporate investigators may be informed of a search on the premises or that a certain suspect will be taken into custody). Type C, coordination of actions, is quite rare according to respondents. In those cases, law enforcement actors and corporate investigators work together to get the best results. This may mean that the prosecutor and lead-police or FIOD [tax] investigators meet with the corporate investigators to talk things over. Information is shared both ways, investigative actions are coordinated and a division of labour may evolve, in which corporate investigators and law enforcement actors share information about the matters they themselves will not pursue, but are relevant to the other.

Public/private relations largely revolve around information sharing. This is often a source of frustration for corporate investigators because of a perceived lack of expertise and willingness by law enforcement officials. Many law enforcement professionals seem to be unaware of the possibilities for information sharing within the criminal justice system. Respondents indicate that the position individual prosecutors take with regard to information sharing is crucial to what will be possible in practice. Relative to general police forces and prosecution offices, corporate security respondents and clients highly value specialised fraud units within the police, FIOD investigators and the specialised prosecutors of the *Functioneel Parket* (FP). Respondents from both the public and private sector would welcome the (re) institution of central contact points within the police organisation and the prosecution office. Respondents indicate they are wary of informal information sharing, however it does exist. The utility of illegitimately obtained information may be limited in most cases but it may be used as directive information (to guide the investigations in a certain direction). Non-contractual moral activity may lead corporate investigators to avoid the illegal sharing of information (because it is 'wrong'), but it may simultaneously lead them to actually share information 'in a grey area' (because it is 'right'). Breaches of privacy law mentioned by respondents occur with regard to

directive (and often general) information, rather than them being gross abuses of privacy law. Informal networks serve more purpose with regard to entrance into the criminal justice system, respondents suggest. Former colleagues in law enforcement agencies may be used as a point of reference for 'procedural' questions such as where to report a specific case. Having a wide network of (former) colleagues may provide both corporate investigators and law enforcement actors with an easy entrance.

To summarise, the corporate security sector is a commercial provider of investigative services, involved in the investigation and settlement of internal norm violations. The sector largely acts as a semi-autonomous social field with a high level of discretion and autonomy. Corporate investigators and clients use forum shopping within and across the private legal sphere to get to the optimal outcome. This means that the state has little insight into what happens in the corporate security sector. While this has the benefit for society that the criminal justice system is spared the trouble and costs of investigating and prosecuting these matters, it also means there is effectively little to no democratic control over the corporate investigation sector. As an important implication of the research, it is suggested that a Wpbr-permit should be made obligatory to all four corporate investigator groups. The control over such a permit-system should be given to the Data Protection Authority.

The tendency of corporate investigators to stay *within* the private legal sphere, and *outside* of the criminal justice system, does not limit the sector to a purely commercial rationale. Through (non-)contractual moral activity, normative considerations influence the corporate investigation and settlement processes in addition to pragmatic and commercial considerations. Public/private relationships are largely *ad hoc* and occur when corporate investigators or their clients feel the need to involve the criminal justice apparatus. Cooperation is fairly rare, public/private relationships being better conceptualised as coexistence, with public and private actors meeting only on an *ad hoc* basis. The commonly used state-centric discourse has proven to be unhelpful to conceptualise public/private relations between law enforcement and corporate investigators. Rather than putting emphasis on cooperation, we should investigate the corporate security sector in its own right. Most importantly, it is necessary to approach the corporate security sector as a semi-autonomous social field, without using the lens of a top-down state-centric discourse. The discourse promoted in this research theoretically assesses corporate investigators as semi-autonomous actors, while also taking into account the role of the state as a key player (be it on the background) – one that adds a normative ('retribution') dimension to corporate settlement solutions (when involved in that), and one that is the source of democratic control over the market. In further exploring the social realities of the corporate security market – and the coexistence of corporate investigators with law

enforcement agencies and other state actors within it – it is important to stay clear of stereotypical portrayals of 'public' and 'private'. The non-contractual moral agency of corporate investigators, be that to provide themselves with legitimacy or out of normative concerns, creates space for other than purely commercial considerations. A keyword describing the corporate security market is flexibility – it plays a pivotal role in the services provided, the legal frameworks applied and the interests served and in the relationships with public actors.

Samenvatting

Normovertredingen begaan door werknemers van organisaties worden vaak onderzocht en afgehandeld door corporate onderzoekers. Het doel van dit onderzoek is de corporate onderzoeksector in Nederland en zijn relaties met het strafrechtelijk systeem inzichtelijk te maken. De onderzoeksvraag die leidend is geweest voor dit onderzoek luidt: *Wat is corporate onderzoek, hoe kan de wisselende relatie van corporate onderzoekers met politie en justitie worden geconceptualiseerd en wat is de relevantie voor de Nederlandse maatschappij?* Deze vraag is beantwoord aan de hand van empirisch materiaal, verzameld met behulp van kwalitatieve onderzoeksmethoden. 59 semigestructureerde interviews vormen de basis van het onderzoek, waarvan er 33 zijn gehouden onder corporate onderzoekers, 16 onder professionals uit het strafrechtelijk systeem en 10 onder opdrachtgevers van corporate onderzoeksdiensten. Daarnaast zijn twee observaties uitgevoerd, gericht op corporate onderzoekers. De eerste observatie is uitgevoerd binnen een particulier onderzoeksbedrijf en had een duur van zeven weken. De tweede observatie is uitgevoerd binnen een interne veiligheidsafdeling van een groot Nederlands bedrijf en had een duur van zes weken. Tenslotte zijn er 21 particuliere onderzoeksdossiers geanalyseerd, voortvloeiend uit de twee observaties. Deze samenvatting geeft de belangrijkste resultaten weer van het onderzoek.

De corporate onderzoeksector bestaat uit professionals die zich bezighouden met het aanbieden van gespecialiseerde en op maat gemaakte diensten op het gebied van forensisch onderzoek. Hoewel de professionele diensten meer omvatten (bijvoorbeeld het uitvoeren van *pre-employment screenings*), richt dit promotieonderzoek zich op de forensische onderzoeksactiviteiten van de corporate onderzoeksector, bestaande uit forensisch accountancy-onderzoek, cyber onderzoek, particulier onderzoek meer in zijn algemeenheid, het opsporen van vermogen, (assistentie bij) de afhandeling van de normovertreding en het treffen van uit onderzoek voortvloeiende preventiemaatregelen. Het promotieonderzoek richt zich op de werkzaamheden van corporate onderzoekers in relatie tot interne normovertredingen (binnen de werknemer/werkgever relatie). In Nederland zijn er vier (beroeps)groepen die zich bezighouden met dit soort onderzoeken – particuliere onderzoeksbureaus, interne veiligheidsafdelingen, forensische accountants en forensische juridische onderzoekers.

Een belangrijk onderwerp in dit promotieonderzoek is wijze waarop de corporate onderzoeksector theoretisch benaderd moet worden. Een aantal theorieën over publiek/private relaties kan worden besproken en beoordeeld als niet (volledig) toepasbaar. De junior partner theorie gaat uit van een relatie waarbinnen de overheid dominant is en de private sector ondergeschikt. De private sector is vanuit

dit oogpunt aanvullend aan de overheid (de 'junior partner'). De economische theorie (ook wel *loss prevention theory*) daarentegen, stelt dat publieke en private veiligheidsactoren vergelijkbaar zijn en dat zij met elkaar in competitie zijn. Een strikt onderscheid tussen publiek en privaat is vanuit deze gedachte niet te maken. De nodale benadering op veiligheid stelt dat veiligheid wordt aangeboden door een veelheid aan actoren en dat de staat daar een van is. Het verankerde pluralisme perspectief tenslotte is het eens met de stelling dat er veiligheidsnetwerken bestaan met een veelheid aan actoren, maar plaatst de staat wel in een bevoorrechte positie hierbinnen. De beschreven theoretische benaderingen nemen allen de staat (impliciet of expliciet) als uitgangspunt. Of het hierbij nu gaat om privatisering en responsabilisering (als een bewuste actie van de staat), of om een (door de staat onbedoelde) groei in grootschalig privébezit, de assumptie is dat de staat aanwezig was in het veiligheidsveld en dat deze aanwezigheid afneemt. Wanneer het gaat om onderzoek naar en afdoening van interne normovertredingen binnen organisaties, kan de positie van de staat echter beter worden beschreven als *afwezigheid*. Veel interne normovertredingen bereiken nooit het strafrechtelijk systeem. In de gevallen dat er aangifte wordt gedaan, wordt de strafrechtelijke afhandeling van de zaak vaak gebruikt als een aanvulling op een corporate afdoeningswijze (wat ingaat tegen de propositie van de junior partner theorie dat het private veld het publieke veiligheidsveld aanvult). Daarnaast kunnen corporate onderzoekers en publieke opspoorders worden gezien als functioneel afwijkend van elkaar (wat ingaat tegen de ideeën van inwisselbaarheid en competitie van de economische, nodale en verankerd pluralisme perspectieven). In plaats daarvan kan de groei van de sector worden gezien als de commercialisering van het *dark number* van interne normovertredingen. De benadering die gebruikt wordt in dit promotieonderzoek is dat de corporate onderzoeksector een grote mate van autonomie en flexibiliteit tentoonspreidt binnen een semiautonoom sociaal veld, zowel in relatie tot onderzoekwerkzaamheden als in relatie tot andere actoren. Hierbinnen is een belangrijke rol weggelegd voor de overheid, doordat het een normatieve (retributie) dimensie kan toevoegen aan het corporate onderzoek. Daarnaast is het van belang dat de overheid een rol speelt in het toezicht op en de controle over de corporate onderzoeksector. Het ingenomen theoretische perspectief kan dan ook worden beschouwd als een heroverweging van de theorieën die de staat als (impliciet) uitgangspunt nemen. De semiautonome positie van corporate onderzoekers wordt hier als uitganspunt genomen, zonder daarbij de rol van de staat uit het oog te verliezen.

De regels rondom corporate onderzoek zijn niet voor alle onderzoekers strikt vastgelegd. Alleen voor de particuliere onderzoeksbedrijven geldt een vergunningplicht onder de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr). De andere

beroepsgroepen van corporate onderzoekers hebben slechts algemene regelgeving (in het geval van accountants en advocaten), richtlijnen (in het geval van accountants) en zelfregulering (in het geval van interne veiligheidsafdelingen). Echter, de Wet Bescherming Persoonsgegevens, en andere algemene wetten zoals het Wetboek van Strafrecht, zijn van toepassing op alle corporate onderzoeken die worden uitgevoerd. Daarnaast blijken de geïnterviewde corporate onderzoekers in de praktijk de Privacy gedragscode, die is opgesteld en wettelijk bindend verklaard voor particuliere onderzoeksbedrijven, grotendeels te volgen. Het blijkt dat de verschillende onderzoekers dezelfde rechtsbeginselen en principes gebruiken in hun onderzoek, met als belangrijkst: proportionaliteit, subsidiariteit en (rechts)gelijkheid. Op deze wijze probeert men democratische beginselen uit het strafrecht, zoals het recht op een eerlijk proces, in het private onderzoek te integreren. Ondanks het commerciële karakter van het corporate onderzoeksveld wordt er op deze manier ook ruimte gecreëerd voor normatieve overwegingen. Het (democratische) toezicht op de corporate onderzoeksector is vrijwel afwezig en in de praktijk sterk afhankelijk van de inspanningen van betrokken personen, klanten en corporate onderzoekers zelf. Er zijn weinig voorbeelden bekend van grove rechtsschendingen door corporate onderzoekers, maar door de ruimte die wordt geboden is er wel potentie tot misbruik en *forum shopping*.

De gefragmenteerde aard van de regelgeving resulteert in combinatie met andere kenmerken in verschillen tussen de verscheidene corporate onderzoekers. Interne veiligheidsafdelingen zijn in een unieke positie ten opzichte van de opdrachtgever omdat zij onderdeel van de organisatie van de opdrachtgever zijn en dus veel inzicht hebben in de organisatie. Particuliere onderzoeksbedrijven daarentegen zijn extern aan de opdrachtgever en dus onafhankelijker en zij bieden algemenere diensten aan dan andere corporate onderzoekers. Ook forensische accountants worden gezien als onafhankelijker en, daarnaast, als expert op het gebied van financieel onderzoek. Forensische juridische onderzoekers tenslotte, onderscheiden zich voornamelijk door hun juridische kennis en de verdergaande mogelijkheden tot assistentie met de afhandeling van de normovertreding. Hoewel de verschillende beroepsgroepen vanuit commercieel oogpunt de nadruk leggen op de verschillen, blijkt dat de meeste corporate onderzoeksafdelingen en -bedrijven juist onderzoekers aannemen met verschillende professionele achtergronden om zo een optimale dienstverlening te kunnen aanbieden aan opdrachtgevers. Naast deze nadruk op de verschillen met andere corporate onderzoekers, worden door respondenten ook de verschillen met politie en justitie benadrukt. Dit uit zich onder andere in het vermijden van strafrechtelijke terminologie. Corporate onderzoekers zien zichzelf niet als private politie of justitie.

Corporate onderzoekers kunnen voor een groot deel zelfstandig en onafhankelijk van politie en justitie opereren bij het aanbieden van onderzoeksdiensten en bij het assisteren bij de afdoening van normovertredingen. Een corporate onderzoek wordt uitgevoerd op basis van een opdracht van de opdrachtgever; corporate onderzoekers proberen deze op zodanige wijze te formuleren dat zij binnen de grenzen van de opdracht onafhankelijk kunnen werken. Corporate onderzoeken blijven echter deels afhankelijk van de opdrachtgever aangezien deze de reikwijdte van het onderzoek bepaalt en corporate onderzoekers grotendeels afhankelijk zijn van de informatie die de opdrachtgever aanlevert. Via de opdrachtgever, tevens werkgever van de betrokken werknemer, hebben corporate onderzoekers verregaande toegang tot informatie, ondanks dat de opsporingsbevoegdheden die kunnen worden ingezet door politie en justitie niet tot hun beschikking staan. In onderzoeksmogelijkheden en oplossingen zijn corporate onderzoekers heel flexibel en kunnen zij efficiënt werken. De medewerking van de betrokken werknemers is belangrijk voor het onderzoek. Deze medewerking kan slechts tot een bepaalde hoogte als vrijwillig worden gezien, aangezien de opdrachtgever als werkgever druk kan uitoefenen om medewerking te bewerkstelligen.

Bij het bepalen van de methoden van onderzoek die worden ingezet worden corporate onderzoekers deels geleid door rechtsbeginselen zoals proportionaliteit, subsidiariteit en (rechts)gelijkheid. Informatiebronnen en methoden van onderzoek die veel worden ingezet zijn interne documentatie (financiële administratie, contracten); interne systemen (communicatiesystemen zoals email en telefoonverkeer, gegevensdragers zoals computers en werknemerssystemen zoals de registratie van toegang); open bronnen (databanken, (sociale) media); en persoonlijke communicatie (interviews met betrokkenen en getuigen). Daarnaast kunnen andere informatiebronnen worden ingezet, zoals observatiegegevens en informatie uit een (openbaar) strafrechtelijk proces. Het interview met de betrokkene vormt over het algemeen het sluitstuk van het corporate onderzoek. Op deze manier kunnen de onderzoekers de betrokkene confronteren met de verzamelde belastende informatie. De betrokkene wordt, volgens het beginsel van hoor- en wederhoor, de mogelijkheid geboden om het interviewverslag te lezen en hierop te reageren. Na afronding van het onderzoek wordt een conceptrapport opgesteld, waar de betrokkene ook inzage in krijgt (ten aanzien van de voor hem relevante delen) en waar hij op kan reageren. Tenslotte wordt het definitieve rapport aangeboden aan de opdrachtgever.

Na de afronding van het onderzoek volgt er veelal een afhandeling. Er zijn verschillende redenen waarom organisaties corporate onderzoek en particuliere afdoeningsmogelijkheden prefereren boven een strafrechtelijk aangifte. Corporate onderzoekers zijn niet gebonden aan de definities die in het strafrecht worden gebruikt, noch aan de formaliteiten en het (tijdrovende) strafrechtelijke proces. Als

gevolg hiervan kunnen corporate onderzoekers flexibeler te werk gaan. De focus op de belangen van de opdrachtgever is een tweede kenmerk dat gunstig is voor opdrachtgevers. In tegenstelling tot in het strafrechtelijk systeem, waarin niet de belangen van de organisatie, maar de belangen van de maatschappij centraal staan, kan elk gedrag dat als schadelijk wordt ervaren door de opdrachtgever worden onderzocht in de context van een corporate onderzoek (en kan de opdracht worden beperkt tot een specifiek voorval). Ten derde bieden corporate onderzoekers kun cliënten een hoge mate van discretie en controle over de informatie die naar buiten komt en (tot op zekere hoogte) over het onderzoeksproces.

Redenen om geen aangifte te willen doen bij strafrechtelijke autoriteiten zijn dan ook een verlies van controle over informatie en het proces; de (beperkte) reikwijdte van wat er kan worden onderzocht als misdrijf; de beperkte mogelijkheden tot (buiten-strafrechtelijke) afdoening; en een beperkt vertrouwen in het probleemoplossend vermogen van het strafrechtelijk systeem. Er zijn echter ook normatieve en pragmatische overwegingen die leiden tot de beslissing aangifte te doen. Pragmatische overwegingen zijn bijvoorbeeld dat de opsporingsbevoegdheden van de politie noodzakelijk zijn om tot bewijs te komen of dat het in het voorkomende geval beter is om een vervolging in Nederland te initiëren (zodat een vervolging in een andere, strengere jurisdictie kan worden vermeden of afgezwakt [*ne bis in idem*]). Dit laatste is een van de vele voorbeelden van *forum shopping* die binnen de corporate onderzoeksmarkt kunnen worden ingezet. Normatieve overwegingen zijn bijvoorbeeld dat de opdrachtgever behoefte heeft aan retributie of dat er een verantwoordelijkheid wordt gevoeld naar de samenleving toe. Deze overwegingen kunnen er toe leiden dat de afstand die normaliter bestaat tussen corporate onderzoekers en politie en justitie wordt verkleind, en dat men actief probeert politie en justitie te betrekken in het onderzoek.

Een belangrijke uitkomst van dit promotieonderzoek is dat corporate onderzoekers door middel van *forum shopping* gebruik maken van de mogelijkheden die de verschillende rechtsstelsels (strafrecht, civiel recht, arbeidsrecht en interne regelgeving binnen organisaties) bieden om tot een zo efficiënt en positief mogelijke oplossing te komen voor hun cliënt. Naast een strafrechtelijke vervolging kan men gebruik maken van het civielrechtelijke systeem door een civiele rechtszaak aan te spannen ter vergoeding van schade of ter beëindiging van een arbeidsovereenkomst, door een *pro forma* procedure te initiëren of door het initiatief te nemen tot een procedure bij de Ondernemingskamer. Daarnaast kan het civielrecht worden gebruikt door het sluiten van een vaststellingsovereenkomst ter beëindiging van de arbeidsovereenkomst. Interne regelgeving kan bijvoorbeeld worden gebruikt voor de disciplinering van de werknemer, variërend van een waarschuwing tot ontslag op staande voet.

De aard en samenstelling van de corporate onderzoeksector en het type normovertredingen waar corporate onderzoekers zich mee bezig houden zorgen er voor dat formele samenwerkingsverbanden met politie en justitie over een lange termijn moeilijk te realiseren zijn. De gefragmenteerde aard van de sector, de verscheidenheid aan betrokken belangen en het feit dat de opdrachtgever en niet de corporate onderzoeker bepaalt of er wel of niet aangifte wordt gedaan, staan hieraan in de weg. De flexibiliteit van corporate onderzoekers en de mogelijkheid om zonder inmenging van het strafrechtelijk systeem te werken zijn essentiële kenmerken voor het voortbestaan van de sector. Een belangrijke uitkomst van het promotieonderzoek is dan ook dat publiek/private relaties niet moeten worden gezien in het licht van een dominante overheid en ondergeschikte private actoren. Publiek/private relaties draaien vaak eerder om naast elkaar bestaan (co-existentie) dan om (langdurige) samenwerking (coöperatie). Convenanten en publiek/private samenwerkingsverbanden blijken in de praktijk niet goed te werken en op basis van het promotieonderzoek kan worden gesteld dat kortdurende, zaaks-gerelateerde contacten veel vaker voorkomen. De mate waarin informatie wordt uitgewisseld en wordt samengewerkt binnen deze contacten verschilt. Het promotieonderzoek introduceert een typologie voor deze *ad hoc* co-existentie, variërend van 'privaat naar publieke informatieoverdracht'(type A), tot '(beperkte) wederzijdse informatie-uitwisseling' (type B), en 'coördinatie van handelingen' (type C). Type A, privaat/publieke informatieoverdracht, kan voorkomen als een sequentie maar er kan ook sprake zijn van twee (gelijktijdige) parallelle onderzoeken. Corporate onderzoekers zijn vaak niet verder betrokken bij het strafrechtelijk onderzoek dan het overdragen van hun eigen onderzoeksresultaten via een aangifte. In het geval van parallelle onderzoeken is er meer kans op samenwerking, maar ook hier gaat het vaak slechts om informatieoverdracht. Bij type B, beperkte wederzijdse informatie-uitwisseling, wordt de meeste informatie door private partijen aan politie en justitie aangeleverd, maar in dit geval krijgt de private partij ook (in beperkte mate) informatie terug. Volgens respondenten komt dit type informatieoverdracht minder vaak voor dan type A. De informatie die met private partijen wordt gedeeld is vaak vrij algemeen en meer gericht op onderzoeksverrichtingen dan op onderzoeksresultaten (zo wordt bijvoorbeeld de informatie gedeeld dat een doorzoeking plaats zal vinden op een bepaald moment en bepaalde locatie). Type C, coördinatie van handelingen, tenslotte, komt volgens respondenten weinig voor. Bij dit type co-existentie werken corporate onderzoekers en politie, FIOD en justitie samen om de zaak tot een goed einde te brengen. Dit kan betekenen dat er regelmatig overleg plaatsvindt, dat informatie over en weer wordt gedeeld, dat onderzoekshandelingen op elkaar worden afgestemd en dat een vorm van arbeidsverdeling plaats kan vinden.

Een groot deel van de publiek/private contacten vindt plaats in het kader van informatie-uitwisseling. Doordat corporate onderzoekers de perceptie hebben dat politie en (in mindere mate) justitie expertise en bereidheid tot informatiedeling missen, is dit vaak een bron van frustratie. Veel publieke opspoorders blijken de mogelijkheden die de wet biedt om informatie te delen inderdaad niet te kennen. Respondenten geven aan dat de opstelling van de individuele officier van justitie cruciaal is om te bepalen of er informatie wordt gedeeld in een specifiek geval. Ten opzichte van de politieorganisatie en het openbaar ministerie in hun algemeenheid zijn respondenten positiever ten aanzien van gespecialiseerde fraudeonderzoekers binnen de politie, de FIOD en het Functioneel Parket. In dit kader wordt er gepleit voor (her)introductie van een (de)centraal fraudecontactpunt binnen politie en justitie ter bevordering van de onderlinge relaties in specifieke zaken. Respondenten geven verder aan terughoudend te zijn met informele informatie-uitwisseling en dat de bruikbaarheid van informeel verkregen informatie beperkt is. Normatieve overwegingen kunnen informele en illegitieme informatie-uitwisseling tegen gaan (omdat het 'verkeerd' is), maar tegelijkertijd kunnen normatieve overwegingen informele en illegitieme informatie-uitwisseling ook in de hand werken (omdat het juist 'goed' is in het onderhavige geval). Informeel verkregen informatie bevat over het algemeen slechts algemene informatie die een onderzoek in een bepaalde richting kan sturen. Op basis van dit promotieonderzoek kan worden gesteld dat het informele netwerk door zowel corporate onderzoekers als politiemensen eerder wordt gebruikt om een aanspreekpunt te vinden dan om op een illegitieme wijze aan informatie te komen.

Samenvattend kan worden gesteld dat de corporate onderzoeksector (forensische) onderzoeksdiensten aanbiedt en betrokken is bij de (advisering ten aanzien van) afdoening van interne normovertredingen binnen organisaties. De sector kan grotendeels als een semiautonoom sociaal veld opereren, waarbinnen corporate onderzoekers een hoge mate van discretie en autonomie genieten. *Forum shopping* tussen en binnen jurisdicties wordt door onderzoekers en opdrachtgevers gebruikt om tot een optimale uitkomst te komen in een specifieke zaak. Dit leidt ertoe dat er weinig zicht is vanuit de overheid op onderzoek naar en afhandeling van normovertredingen binnen organisaties. Dit betekent enerzijds dat het strafrechtelijk systeem tijd en kosten bespaart wat betreft de opsporing en vervolging van deze normovertredingen, maar anderzijds ook dat er weinig zicht en democratische controle is op wat er in de corporate onderzoeksector gebeurt. Een belangrijke aanbeveling is dan ook dat alle vier de groepen van corporate onderzoekers vergunningplichtig worden gemaakt en dat zij zich allen te houden hebben aan de Wpbr en de bijbehorende Privacy gedragscode. Verder wordt er naar aanleiding van

dit promotieonderzoek voorgesteld het toezicht op het vergunningstelsel neer te leggen bij de Autoriteit Persoonsgegevens.

Vanuit theoretisch oogpunt is het belangrijk om de corporate onderzoeksector en de relaties die er bestaan tussen deze onderzoekers en het strafrechtelijk systeem in een ander licht te beschouwen dan gebruikelijk is. In plaats van de rol van de staat te benadrukken, is het zinvol om de sector te benaderen als een (semi) autonoom veld. Binnen een dergelijke benadering is het echter ook belangrijk om de rol van de staat mee te wegen. Op momenten dat het strafrechtelijk systeem betrokken is bij een zaak voegt deze een normatieve (retributie) dimensie toe aan het corporate onderzoek. Daarnaast is het van belang dat de overheid een rol speelt in het toezicht op en de controle over de corporate onderzoeksector. De normatieve en pragmatische overwegingen die invloed uitoefenen op beslissingen binnen onderzoek en afdoening, zorgen ervoor dat het werkveld van corporate onderzoekers niet uitsluitend kan worden gedefinieerd als puur commercieel. Een sleutelwoord in relatie tot de corporate onderzoeksector is flexibiliteit – ten aanzien van de aangeboden diensten, de regelgeving, de betrokken belangen en in het kader van de relaties met publiekrechtelijke actoren speelt flexibiliteit een belangrijke rol.

Curriculum Vitae

Clarissa Meerts was born on 15 May 1986 in The Hague ('s-Gravenhage). She completed her high school ('gymnasium') education in 2004 by graduating from the Gymnasium Haganum. Clarissa continued to study Criminology at the Erasmus University Rotterdam, where she received her bachelor's degree (cum laude) in 2007. Clarissa combined her bachelor in Criminology with the interdisciplinary Erasmus honours programme, graduating in 2006. A master's degree (cum laude) in International and Comparative Criminology at Erasmus University Rotterdam followed in 2009.

From 2007 to 2009 Clarissa was a (research) student-assistant to Prof. Dr. Nicholas Dorn for a research project about corporate security in the Netherlands. After receiving her master's degree, Clarissa was employed by the Criminology department of Erasmus School of Law as a junior researcher and teacher (from 2009 to 2012). During this time, she participated in two major research projects: the *Monitor Georganiseerde Criminaliteit* and a research on a major Dutch real estate fraud (*de Vastgoedfraude*).

In 2012, the Netherlands Organisation for Scientific Research (NWO) granted Clarissa a Research Talent grant, funding her PhD research. Her PhD project, which was focused on corporate investigations and corporate settlements of internal norm violations within organisations, was supervised by Prof. Dr. René van Swaaningen and Prof. Dr. Nicholas Dorn. In addition to a dissertation, Clarissa (co)authored multiple publications on the subject of corporate investigations, corporate settlements and public/private cooperation in the security field.

Both previous to and during her PhD project, Clarissa has been involved as a lecturer in multiple courses within the Criminology education of Erasmus School of Law. During her career at Erasmus School of Law, Clarissa attended multiple (international) conferences and(co)authored multiple publications.

Clarissa is currently working at the Criminology department of the Free University Amsterdam (VU) as an assistant professor. Her research interests are corporate investigations, corporate settlements, public/private relationships, white-collar and financial crime and organised crime.

PhD portfolio

Name PhD student:	Clarissa Meerts
Erasmus Department:	Erasmus School of Law, Department of Criminology
Research School:	Monitoring Safety and Security
PhD-period:	September 2012-September 2017
Promotor:	Prof. Dr. René van Swaaningen
Co-promotor:	Prof. Dr. Nicholas Dorn

PhD training and experience		
Specific courses		
	Qualitative interviewing	2011
	Introduction in the use of Atlas.ti	2012
	Teaching course on Problem oriented learning	2012
	Academic writing (EGSL)	2013
Seminars and workshops (attended)[1]		
	EGSL lunch lectures	2012-2015
	Lunch lectures Monitoring Safety & Security	2012-2017
	Dutch Society of Criminology (NVC)	2012-2017
	Security Sessions (SSAP)	2012-2017
	European society of Criminology (ESC)	2012-2017
	Junior meetings criminology department (ESL)	2015-2017
	Publication strategies for PhD candidates (EGSL)	2015
	Career event for PhDs and Post-docs (EUR)	2016
Presentations		
	See below ((inter)national conferences)	
	PhD lunch lectures	2012
	Workshop in honour of David Friedrichs	2014
	Workshop Criminology and Investigation *Tijdschrift voor Criminologie*	2015
	Career day criminology (BOD)	2014 & 2017
Presentations given at (inter)national conferences		
	Dutch Society of Criminology (NVC)	2012-2017
	European society of Criminology (ESC)	2014-2017
	Farewell seminar Prof. Dr. Dorn	2015
	Seminar at John Moores University Liverpool	2016
	Seminar 'Understanding corporate crime: theory and methods' of European Working Group in Organisational Crime (EUROC)	2017
Teaching (2012-2016)		

	Introduction to criminology	
	Introduction to law	
	Introduction to sociology	
	Nature, prevalence and damage of crime	
	Quantitative methods of criminological research	
	Explaining crime	
	Theoretical criminology	
	Advanced quantitative research methods	
	Prevention and punishment	
	Supervision of Master theses	
	Guest lectures	
Publications during PhD		
Meerts, C.A.	Corporate Security - Private Justice? (Un)Settling Employer-Employee Troubles. *Security Journal, 26* (3), 264-279.	2013
Meerts, C.A.	Over pragmatisme en strategie. *Tijdschrift voor Criminologie, 56* (4), 115-137.	2014
Meerts, C.A.	Corporate security: Governing through private and public law. In K. Walby & R.K. Lippert (Eds.), *Corporate security in the 21st century. Theory and practice in international perspective (Crime prevention and security management)* (pp. 97-115). Basingstoke: Palgrave Macmillan.	2014
Meerts, C.A.	A world apart? Private investigations in the corporate sector. *Erasmus Law Review, 9*(4), 162-176.	2016
Meerts, C.A. & Dorn, N.	Cooperation as mantra: corporate security and public law. In R. van Swaaningen, C.G. van Wingerden & R.H.J.M. Staring (Eds.), *Over de muren van stilzwijgen - liber amicorum Henk van de Bunt* (pp.503-515). Den Haag: Boom criminologie.	2017

1 This is a selection of the most relevant seminars and workshops that have been attended during the PhD research.