VIRTUAL ACTS, REAL CRIMES?

A Legal-Philosophical Analysis of Virtual Cybercrime

Litska Strikwerda

VIRTUAL ACTS, REAL CRIMES?

A Legal-Philosophical Analysis of Virtual Cybercrime

Litska Strikwerda

Promotion Committee:

Rector Magnificus, voorzitter
Prof. dr. P.A.E. Brey, University of Twente, promotor
Dr. J.H. Søraker, University of Twente, ass. promotor
Dr. P.J. Nickel, Eindhoven University of Technology, ass. promotor

Prof. dr. ir. P.P.C.C. Verbeek, University of Twente
Prof. dr. ir. F.J.A.M. van Houten, University of Twente
Prof. dr. C.M. Ess, University of Oslo
Prof. dr. E.J. Koops, Tilburg University
Dr. M. van der Linden-Smith, Utrecht University

Printed by: Wöhrmann Print Service, Zutphen, The Netherlands
Cover image: Victor Davenschot, 1986
Cover design by: Litska Strikwerda & Mark Zaremba

VIRTUAL ACTS, REAL CRIMES?
A LEGAL-PHILOSOPHICAL ANALYSIS OF VIRTUAL CYBERCRIME

DISSERTATION

to obtain
the degree of doctor at the University of Twente,
on the authority of the rector magnificus,
Prof. dr. H. Brinksma,
On account of the decision of the graduation committee,
to be publicly defended
on Friday the 10th October 2014 at 12.45 hrs

by

Litska Strikwerda
Born on 22nd February, 1983
in Amersfoort, the Netherlands

This dissertation has been approved by promotor and assistant promotors:

Prof. dr. P.A.E. Brey, dr. J.H. Søraker and dr. P.J. Nickel

ISBN: 978-90-365-3713-1

Voor mijn ouders en grootouders

For my parents and grandparents

CONTENTS

ACKNOWLEDGEMENTS

I will have to disappoint those who enjoy reading the acknowledgements of a dissertation most, for I keep it short. I would like to thank my supervisors (Philip Brey, Johnny Søraker and Philip Nickel) for their useful comments, advice and guidance. I would also like to thank my collegues at the University of Twente and Loyola University (Chicago, USA), especially those who proofread parts of my dissertation. I will continue in Dutch.

Ik draag dit proefschrift op aan mijn ouders als blijk van dank voor hun onuitputtelijke liefde, steun, warmte en trouw. Jullie hebben mij opgevoed tot een evenwichtig mens. Ik voel mij innig met jullie verbonden.

Ik draag dit proefschrift ook op aan mijn grootouders (postuum). Ik wil jullie danken voor jullie liefde, wijsheid en betrokkenheid en weet dat jullie heel erg trots geweest zouden zijn. Het past jou in het bijzonder te noemen, oma. Ik vind het moeilijk dat je er niet bij zult zijn wanneer ik dit proefschrift verdedig, maar ik ben blij dat ik je nog heb kunnen zeggen dat ik het (mede) aan jou zou opdragen. Jij hebt nooit de kans gekregen om een universitaire opleiding te volgen, hoewel je dat zeker had gekund en graag had gewild. Door jou besef ik dat studeren een voorrecht is en dat inzicht heeft mij de kracht gegeven om dit promotietraject af te leggen. Ik ben je dankbaar voor wie je was.

Mijn broer Rense en zus Tjamke heb ik gevraagd mijn paranimfen te zijn. Daarmee wil ik tot uitdrukking brengen dat zij de steunpilaren in mijn leven zijn. Ik kan altijd op jullie bouwen en daar ben ik jullie heel erg dankbaar voor. Rense, jou wil ik daarnaast in het bijzonder bedanken voor het nakijken van mijn proefschrift en voor je kritische inhoudelijke commentaar.

Tot slot wil ik een speciaal woord van dank richten tot Mark. Jou ben ik dankbaar omdat je er altijd voor mij bent. Ik houd van je.

INTRODUCTION

The advent of computer technology has given rise to a new type of crime: cybercrime, which can be defined in broad terms as crime that involves the use of computers or computer networks. On the one hand, the use of computers or computer networks allows for new varieties of anti-social human activity that did not exist before the advent of computers and computer networks, e.g., hacking (in legal terms: illegal access), although they can in essence be seen as new, electronic versions of traditional crimes (Goodman & Brenner 2002, p. 153, 189; Clough 2010, p. 11; Tavani 2007, p. 204). Hacking or illegal access can be seen as a new, electronic version of trespass (Goodman & Brenner 2002, p. 189). On the other hand, computers and computer networks can be used as tools to commit traditional crimes in different ways, e.g., e-fraud (Goodman & Brenner 2002, pp. 152-153; Clough 2010, p. 10; Council of Europe Convention on Cybercrime, Expl. Report § 5; Tavani 2007, pp. 205-206). From a legal point of view, the main difference between these two categories of cybercrime lies in the fact that the first is brought under the scope of criminal law by the development of new laws, whereas the latter is brought under the scope of criminal law by the modification of existing law (Goodman & Brenner 2002, p. 162).

The newest generation of cybercrime is virtual cybercrime. Virtual cybercrime is crime that involves a specific aspect of computers or computer networks: namely, virtuality, which can in essence be described as computer simulation. Consider, for example, the prohibition on virtual child pornography (Council of Europe Convention on Cybercrime article 9). Virtual child pornography does not consist of photographs or film material of real children engaged in sexually explicit conduct but of computer-simulated children, for the images are photoshopped or even entirely computer-generated (Council of Europe Convention on Cybercrime, Expl. Report § 101). And in the Netherlands, for instance, several minors were convicted of theft for stealing virtual items in the virtual worlds of the online multiplayer computer games *Habbo* (2001) and *RuneScape* (2001) (Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791; Gerechtshof Leeuwarden, 10 November 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764). The latter case was ultimately decided by the highest court in the Netherlands (Hoge Raad, 31 January 2012, ECLI: NL: HR: 2012: BQ9251). A case that was never brought to court but highly debated in the media and in (legal) academic literature is the " virtual rape" (rape of an avatar, i.e., a user's virtual representation in a computer game) that was described by Julian Dibbell in the New York newspaper the *Village Voice* as early as 1993.

The field of virtual cybercrime is largely unexplored. Only a handful of virtual cybercrimes have been brought under the scope of criminal law; they include the production, distribution, and possession of virtual child pornography and theft of virtual items. In addition, there are a couple of putative virtual cybercrimes that have been discussed in the media or (legal) academic literature; they include the above-mentioned example of virtual rape. This dissertation will explore the field of virtual cybercrime, mainly from a philosophical point of view but other viewpoints (i.e., a legal-economic, a pragmatic, and a constitutional viewpoint) will also briefly be taken into account. It will focus on the question when virtual cybercrime should be brought under the scope of criminal law and aims to answer that question. For clarification purposes I want to emphasize that I am not concerned with the moral justification of (putative) virtual cybercrimes but with the applicability of penal provisions and the moral norms which, as I will argue, underlie them.

The structure is as follows. This dissertation is divided into three parts: an introductory chapter (part I), three case studies (part II), and a reflection (part III). In total there are five chapters and an epilogue. The first chapter is the introductory chapter, the three case studies form chapter 2, 3, and 4 and, finally, the reflection constitutes chapter 5.

The first chapter, which forms the first part of this dissertation, consists of a legal-ontological study of virtual cybercrime. Ontology is the study of being, which is a branch of philosophy that is concerned with the questions of which kinds of things exist and how they are categorized according to their differences and similarities. Legal ontology is an applied form of ontology that is specifically concerned with the question of how things are (to be) categorized *under law*. This chapter will specifically be concerned with the question when the relatively new phenomenon of virtual cybercrime should be categorized as crime under law, i.e., when it should be brought under the scope of criminal law. In order to answer the aforementioned question, this chapter will provide an descriptive exploration, a philosophical analysis, and a moral evaluation of virtual cybercrime.

The first section will be concerned with the descriptive exploration. In this section, I will first study how cybercrime is treated within existing legal systems, provide a definition of cybercrime, and determine the scope of the term. Then, I will study the different meanings of the term “virtual” and define the term so that it can be explained what the new generation of virtual cybercrime entails. At last I will examine how, if at all, virtual cybercrime is treated within existing legal systems, provide a definition of the term virtual cybercrime and determine its scope.

The second section will be concerned with the philosophical analysis. In this section, I will analyze what necessary and sufficient conditions are for virtual cybercrime in order to count as a crime under existing law from the point of view of social ontology (as developed by the American philosopher Searle) and legal philosophy. I will establish that a virtual cybercrime must necessarily have an extravirtual consequence (a consequence outside the virtual environment) in order to count as a crime under existing law. I will add that not any extravirtual consequence suffices; it needs to be of such a nature that it can legitimate an interference with the liberty of citizens by means of criminal law on the basis of one of the liberty-limiting principles as they have been developed by the American philosopher Feinberg in his well-known work *The Moral Limits of Criminal Law* (1984, 1985, 1986, 1988). These liberty-limiting principles are: the harm principle (which originally derives from Mill 1865), the offense principle, legal paternalism, and legal moralism.

The third section will be concerned with the moral evaluation. In this section I will examine when the extravirtual consequence(s) of virtual cybercrime are of such a nature that (one of) the above-mentioned liberty-limiting principles are applicable. I will conclude that they apply when a virtual cybercrime results in (extravirtual) harm to others, offense, harm to the self, or evils of other kinds. I will provide many examples of virtual cybercrimes that result in the aforementioned consequences.

The second, third, and fourth chapters, which constitute the second part of this dissertation, aim to test whether or not the three specific instances of virtual cybercrime that were mentioned before: namely, theft of virtual items, virtual rape, and the production, distribution, and possession of virtual child pornography, satisfy the necessary and sufficient conditions for criminalization as they were established in the first chapter. These three instances of virtual cybercrime were chosen, because they can function as stress tests. They are controversial and have given rise to a great deal of debate, among legal scholars and philosophers in particular but also in society in general. Each of them raises particular issues, which will briefly be explained below.

The second chapter is a case study of theft of virtual items. I will take the Dutch convictions for theft of virtual items in the virtual worlds of the online multiplayer computer games *Habbo* (2001) and *RuneScape* (2001) mentioned before as a starting point. These convictions have led to a lively debate among lawyers, in- as well as outside the Netherlands, on the question of whether or not virtual items should count as “objects” that can be “stolen” under existing criminal law (e.g., Hoekman & Dirkzwager 2009; Moszkowicz 2009; Rijna 2010; Brenner 2008; Kerr 2008). Some of them are convinced that virtual items are “mere illusions” to

which “real world law” does not apply; others see them as a new form of property deserving legal protection (Ibid.). Applying the general findings from the first chapter, I will argue that virtual items should count as objects that can be stolen if the act of stealing them results in (extravirtual) harm and can, therefore, be brought under the scope of the harm principle (i.e., Feinberg’s first liberty-limiting principle). I will establish that the act of stealing virtual items results in (extravirtual) harm if these virtual items can be considered property worthy of (pecuniary or hedonistic) value in the non-virtual world, for the act of stealing them then results in an economic or emotional loss.

The third chapter is a case study of virtual rape. As early as 1993, Julian Dibbell described in the New York newspaper *The Village Voice* how a user of the virtual world of *LambdaMOO* (1990) took control over two other users’ avatars and made them appear to engage in sexual activities the users did not consent to (Dibbell 1993). Dibbell's story gave rise to a heated debate among philosophers, mainly computer ethicists, which merely focused on the question of whether or not the behavior he described should count as rape or another crime under criminal law. In 2007, fourteen years after Dibbell's story was published, new life was put into this debate when Belgian newspapers announced that the Belgian Federal Police would investigate a virtual rape, the precise facts of the event are unknown, which had occurred in the virtual world of *Second Life* (2003) (Durankse 2007a). This chapter will deal with the aforementioned question whether or not virtual rape should count as rape or another crime under criminal law. In this chapter, I will not only study present instances of virtual rape in a virtual world such as the ones described before but I will also explore the possibilities for virtual rape that virtual reality environments will most probably provide in the near future. A virtual rape in a virtual reality environment would entail that one user takes control over another user's sex toy or sex robot, which is plugged into a computer and connected to the Internet, and gives that user sexually laden sensory feedback to which s/he did not consent through his or her device.

I will study the present and future instances of virtual rape mentioned above in light of three categories of legal philosophical theories on rape. In a nutshell, they all agree that rape should be prohibited because it causes harm, but each theory defines rape and the harm it causes differently. I will establish that a virtual rape in a future virtual reality environment involving a haptic device or robotics fulfills the requirements of the crime of rape as it is viewed under the liberal theories dominant under current law. A surprising finding will be that virtual rape in a virtual world like the one Dibbell described, re-actualizes the conservative view of rape that used to dominate the law in the Middle Ages and fulfills the requirements of the crime of rape as it is viewed under the feminist theories that criticize current law. However, virtual rape in a virtual

world cannot count as rape under current criminal law, because it does not fulfill the requirements of the crime of rape as it is viewed under the liberal theories that currently dominate the law. Ultimately, I will suggest qualifying virtual rape in a virtual world as the crime of sexual harassment instead.

The fourth chapter is a case study of virtual child pornography. As mentioned above, the production, distribution, and possession of virtual child pornography are commonly prohibited. The legitimacy of their prohibition is contested, however. That is because the production of virtual child pornography, as opposed to the production of *non*-virtual child pornography, does not involve children really engaged in sexually explicit conduct, for virtual child pornography consists of either photoshopped pictures of real children or entirely computer-generated images. It is, therefore, often claimed that virtual child pornography does, contrary to *non*-virtual child pornography, not result in (extravirtual) harm and can, therefore, not be brought under the scope of the harm principle. A US law that prohibited virtual child pornography on the ground that it is harmful to children was even declared unconstitutional by the US Supreme Court (*Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002)).

In this chapter I will study whether or not virtual child pornography results in (extravirtual) harm. For reasons that will be explained in the chapter, I will highlight the question of whether or not entirely computer-generated child pornography results in harm as intended by the harm principle. I will suggest that the production, distribution, and possession of entirely computer-generated child pornography is a victimless crime. According to the American philosopher Bedau, the criminalization of victimless crimes is based on either legal paternalism or legal moralism (Bedau 1974). Therefore, I will study whether legal paternalism or legal moralism can legitimate the prohibition of entirely computer-generated child pornography. Ultimately drawing from the positions of virtue ethics and feminism, I will argue that the prohibition of entirely computer-generated child pornography can be legitimated on the basis of legal moralism.

In the fifth chapter, which constitutes the third and last part of this dissertation, I will argue that the question of when virtual cybercrime should be brought under the scope of criminal law does not only have the philosophical dimension that has been discussed so far but also a legal-economic, a pragmatic, and a constitutional dimension. In the first section of this chapter, I will summarize the findings from the previous chapters. In the second section, I will study the legal-economic dimension of the question of when virtual cybercrime should be brought under the scope of criminal law. I will reflect on the costs and benefits of using criminal law for the regulation of virtual cybercrime relative to non-criminal instruments. Since virtual cybercrime

often takes place in the virtual environments of computer games, specific attention will be paid to the rules of games as an alternative for criminal law in the regulation of virtual cybercrime.

In the third section, I will study the pragmatic dimension of the question of when virtual cybercrime should be brought under the scope of criminal law. The aforementioned dimension has to do with the overall capacity of the criminal justice system; as a rule, the criminalization of conduct should not overload the criminal justice system. This is of particular importance with regard to virtual cybercrime, because it involves the use of ICTs, which have a couple of features that facilitate crime and hamper law enforcement. Therefore, the regulation of virtual cybercrime via criminal law can be expected to impose a heavy burden on the criminal justice system.

In the fourth section, I will study the constitutional dimension of the question of when virtual cybercrime should be brought under the scope of criminal law. Under constitutional law, the restriction of citizens' liberties always needs justification. It will turn out that this dimension greatly overlaps with the legal-economic and pragmatic dimension of the aforementioned question. Therefore, it is not in need of further discussion.

The findings of sections one, two, and three will respectively be concretized into philosophical, legal-economic, and pragmatic criteria for the criminalization of virtual cybercrime, which can be used to decide on actual cases. These criteria will be negative criteria, which means that they will indicate when virtual cybercrime should *not* be brought under the scope of criminal law. I will make a distinction between absolute negative criteria, which will indicate when criminalization of virtual cybercrime should be omitted, and relative negative criteria, which will be contraindications for criminalization; the more of these criteria are applicable, the less appropriate it is to criminalize the virtual cybercrime concerned. I will explain that the philosophical, legal-economic, and pragmatic criteria are not conflicting but that they complement each other: one should test a particular instance of virtual cybercrime against the total of all criteria if one wants to answer the question of whether or not it should be brought under the scope of criminal law.

In the last section, the instances of virtual cybercrime that have been discussed throughout this dissertation will be tested against the above-mentioned criteria. I will conclude that the philosophical and legal-economic negative criteria for criminalization do often not apply to the aforementioned instances of virtual cybercrime but that the pragmatic criteria usually do. I will also briefly discuss possible solutions to that problem.

In the epilogue, I will formulate forward-looking policies with regard to virtual cybercrime. I will propose to use the framework of absolute and relative negative criteria for criminalization that I will set up in this dissertation to decide whether or not a particular instance

of virtual cybercrime should be brought under the scope of criminal law. In order to check whether or not my framework functions satisfactorily, I will test two (putative) instances of virtual cybercrime that have not been discussed in the dissertation against the aforementioned criteria and decide whether or not they should be brought under the scope of criminal law. Finally, I will state suggestions for future research.

PART I: INTRODUCTORY CHAPTER

CHAPTER 1 VIRTUAL CYBERCRIME: A DESCRIPTIVE EXPLORATION, PHILOSOPHICAL ANALYSIS, AND MORAL EVALUATION

A shorter version of this chapter was presented as a paper at the 4th International Conference on Digital Forensics & Cyber Crime (Lafayette, USA, 25-26 October 2012), where it won the Best Paper Award. The paper was published under the title "When Should Virtual Cybercrime Be Brought under the Scope of Criminal Law?" in Marcus K. Rogers and Kathryn C. Seigfried-Spellar (Eds.), *Digital Forensics and Cyber Crime (LNICST), Vol. 114* (pp. 109-143). Berlin: Springer-Verlag (2013).

Introduction

This first chapter provides a legal-ontological study of virtual cybercrime. Ontology is the study of being, which is a branch of philosophy concerned with the questions of which kinds of things exist and how they are categorized according to their differences and similarities. Legal ontology is an applied form of ontology specifically concerned with the question of how things are categorized *under law*. Legal ontology does not only study how existing things are categorized under law but also how new things should be categorized under law (Koepsell 2003, p. 33). This chapter will be concerned with the question when the relatively new phenomenon of virtual cybercrime should be categorized as a crime under law, i.e., when it should be brought under the scope of criminal law.

In order to answer the above-mentioned question, the following three steps need to be taken:

STEP 1	*Descriptive exploration*: what is virtual cybercrime and how, if at all, is it treated within existing legal systems?
STEP 2	*Philosophical analysis*: what are necessary and sufficient conditions for virtual cybercrime in order to count as crime under existing law?
STEP 3	*Moral evaluation*: when does virtual cybercrime meet these conditions?[1]

Table 1 Three steps of a legal-ontological analysis of virtual cybercrime

The first section of this chapter will be concerned with the first step. In this section I will study how cybercrime is treated within existing legal systems, provide a definition of

[1] These steps are based on Koepsell 2003, pp. 38-39.

cybercrime, and determine the scope of the term. Then, I will study the different meanings of the term "virtual" and define the term so that it can be explained what the relatively new legal phenomenon of virtual cybercrime entails. Finally, I will examine how virtual cybercrime is treated within existing legal systems, provide a definition of the term virtual cybercrime, and determine its scope.

In the second section of the chapter, I will establish what the necessary and sufficient conditions are for virtual cybercrime to obtain in order to count as a crime under existing law, which is the second step. I will analyze what necessary and sufficient conditions are for virtual cybercrime in order to count as a crime under existing law from the point of view of social ontology (as developed by the American philosopher Searle) and legal philosophy. I will establish that a virtual cybercrime must necessarily have an extravirtual consequence (a consequence outside the virtual environment) in order to count as a crime under existing law. I will add that not any extravirtual consequence suffices; it needs to be of such a nature that it can legitimate an interference with the liberty of citizens by means of criminal law on the basis of one of the liberty-limiting principles as they have been developed by the American philosopher Feinberg in his well-known work *The Moral Limits of Criminal Law* (1984, 1985, 1986, 1988). These liberty-limiting principles are: the harm principle (which originally derives from Mill 1865), the offense principle, legal paternalism, and legal moralism.

In the third section I will examine when the extravirtual consequence(s) of virtual cybercrime are of such a nature that (one of) the aforementioned liberty-limiting principles can be invoked. This is the third step. Ultimately, I will come to the conclusion that virtual cybercrime should be brought under the scope of criminal law when it results in extravirtual harm to others, offense, harm to the self, or evils of other kinds.

1.1 Legal positioning, definition, and scope of virtual cybercrime

In this section, I will examine what virtual cybercrime is and how, if at all, it is treated within existing legal systems. I will start with a description of the developing field of cybercrime. Against this background, I will provide a definition of cybercrime and determine the scope of the term. Then, I will define the term "virtual" and explain what the new legal phenomenon of virtual cybercrime entails. Next, I will examine how virtual cybercrime is treated within existing legal systems. Finally, I will provide a definition of the term virtual cybercrime and determine its scope. Note that I will define (virtual) cybercrime in general terms so that in principle the definition applies to any country or jurisdiction worldwide.

1.1.1 Background: the developing field of cybercrime

Crime is generally understood as a human act (or omission) prohibited by law. The prefix "cyber" refers to the use of computers or computer networks; it means "computer-mediated" (Brenner 2008, p. 52; Clough 2010, p. 10; Council of Europe Convention on Cybercrime, Expl. Report, § 8). Cybercrime thus consists of any computer-mediated human act that is prohibited by law.

Cybercrime poses a challenge, because the use of computers and computer networks allows for "new and different forms of (…) [human] activity that evade the reach of existing criminal law" (Goodman & Brenner 2002, p. 153). On the one hand, the use of computers or computer networks allows for new varieties of anti-social human activity that did not exist before the advent of computers and computer networks (new crimes, new tools), e.g., the spread of computer viruses (Ibid.; Clough 2010, p. 11; Tavani 2007, p. 204). On the other hand, computers and computer networks can be used as a tool to commit traditional crimes such as fraud, in different ways (old crimes, new tools) (Goodman & Brenner 2002, pp. 152-153; Clough 2010, p. 10; Council of Europe Convention on Cybercrime, Expl. Report § 5; Tavani 2007, pp. 205-206). The following diagram might clarify this distinction further:

New crimes, new tools	**Old crimes, new tools**
E.g., the spread of computer viruses	E.g., e-fraud.

Table 2 New crimes, new tools vs. old crimes, new tools

Legislators continuously need to determine which of the new and different forms of human activity for which the use of computers and computer networks allows have to be prohibited and which not. They have to enact new legal prohibitions in order to prohibit new forms of human activity that computers or computer networks allow for, or make existing legal prohibitions sufficiently broad to include the different forms of human activity that computers and computer networks allow for. Mostly, the enactment of new penal provisions or the extension of existing penal provisions takes place at a national level. Which new and different types of human activity involving the use of computers and computer networks are outlawed precisely, varies significantly according to national legal systems but there is common ground (Goodman & Brenner 2002, p. 165).

The most familiar and most important international initiative to develop criminal law aimed at cybercrime is the Convention on Cybercrime, which has been ratified by most of the member states of the Council of Europe and some other states, i.e., the USA, Australia, and Japan. It is the only binding international instrument on this issue to have been adopted to date (Council of Europe Convention on Cybercrime, Summary). The Convention on Cybercrime establishes "a common minimum standard" of relevant crimes (Council of Europe Convention on Cybercrime, Expl. Report § 33). It defines nine types of new and different human activities involving the use of computers or computer networks. State Parties to the Convention agree to establish the aforementioned human activities as crimes under their domestic law, if they have not yet done so (Ibid.). The Convention on Cybercrime thus provides a list of behaviors considered to be cybercrime worldwide.

The first crime category listed in the Convention on Cybercrime is illegal access or "hacking", which is the unauthorized intrusion into the whole or any part of a computer system (Council of Europe Convention on Cybercrime, article 2; § 44 Expl. Report). The second crime category, illegal interception, consists of the unauthorized interception of computer data by means of tapping devices or other technical means (Council of Europe Convention on Cybercrime, article 3; § 51 Expl. Report). The third crime category, data interference, refers to the damaging, deletion, deterioration, alteration or suppression of computer data without right (Council of Europe Convention on Cybercrime, article 4). The alteration of computer data includes the input of malicious codes such as viruses (Council of Europe Convention on Cybercrime, Expl. Report § 61). The fourth crime category, system interference, can be described as "computer sabotage"; it is the serious hindering of the functioning of a computer system by means of a "denial of service attack" or the dissemination of viruses and other malicious codes (Council of Europe Convention on Cybercrime, article 5; § 65-67 Expl. Report; Goodman & Brenner 2002, p. 189). A denial of service attack consists of an attempt to make a computer or computer network unavailable to its intended users. A common method of attack is sending so many external communications requests to a computer (network) that it cannot respond or responds so slowly that it is effectively unavailable. The fifth crime category, misuse of devices, refers to the production, sale, distribution or otherwise making available of a device that is designed or adapted primarily for the purpose of committing any of the aforementioned offences (Council of Europe Convention on Cybercrime, article 6; § 71 Expl. Report).

The sixth crime category, computer-related forgery, involves the false making or altering of computer data (Council of Europe Convention on Cybercrime, article 7; § 81 Expl. Report). The seventh crime category, computer-related fraud, consists of electronic deceit, e.g., credit

card fraud (Council of Europe Convention on Cybercrime, article 8; § 86 Expl. Report). The eighth crime category, crimes related to child pornography, concerns the electronic production, distribution or possession of child pornographic images (Council of Europe Convention on Cybercrime, article 9). The ninth and last crime category, crimes related to infringements of copyright and related rights, involves the unauthorized copying of protected works such as literary, photographic, musical, and audio-visual works, on a commercial scale and by means of a computer system (Council of Europe Convention on Cybercrime, article 10; § 107 Expl. Report).

The first five crime categories (illegal access, illegal interception, data interference, system interference, and misuse of devices) concern new forms of human activity that did not exist before the advent of computers and computer networks. That is because they can only be carried out through the use of computers or computer networks. Since these crime categories concern new forms of human activity, they require signatory states to enact new legal prohibitions, if they have not already prohibited these activities (Brenner & Goodman 2002, p. 189; Tavani 2007, p. 204). They can be classified under the heading "computer crime" (Clough 2010, p. 10).

The next four crime categories (computer-related forgery, computer-related fraud, crimes related to child pornography, and crimes related to infringements of copyright and related rights) concern traditional crimes where computers or computer networks are used as a tool to commit the crime in a different way. Because states will already have criminalized these traditional crimes, these crime categories require them to make their existing laws sufficiently broad to extend to situations involving computers or computer networks if they have not already done so (Council of Europe Convention on Cybercrime, Expl. Report § 79). They can be classified under the heading "computer-facilitated crime" (Clough 2010, p. 10).

Generally, legislators will only prohibit human acts if that is consistent with existing laws and the philosophy underlying them (Goodman & Brenner 2002, p. 216). The prohibition of a computer-mediated human act is consistent with existing laws and the philosophy underlying them if the act is equivalent to an "off-line" crime, for example, because the same legal interests are at stake (Schellekens 2006, pp. 66-69). Most of the computer crimes listed in the Convention on Cybercrime, although they are new crimes, are equivalent to traditional off-line crimes, because they are in essence electronic versions of them (Goodman & Brenner 2002, p. 189).

Illegal access is often seen as the electronic version of trespass. Illegal interception can be seen as an electronic invasion of privacy crime. And data interference is an electronic property damage crime. System interference and the misuse of devices are entirely new crimes that have

no analogue in traditional crime, however (Goodman & Brenner 2002, p. 189). The prohibition on system interference protects an entirely new legal interest that has been brought about by the advent of computer systems: the interest of operators and users of computer systems to be able to have them function properly (Council of Europe Convention on Cybercrime, Expl. Report § 65). The prohibition on misuse of devices aims to prohibit the aforementioned crimes at the source, because it prohibits the production, sale, distribution or otherwise making available of tools that are needed to commit them. It builds upon the European Convention on the legal protection of services based on, or consisting of, conditional access and EU Directive 98/84/EC on the legal protection of services based on, or consisting of, conditional legal access (Council of Europe Convention on Cybercrime, Expl. Report § 71).

The computer-facilitated crimes that are listed in the Convention on Cybercrime are consistent with existing legal prohibitions and the penal philosophy underlying them, because they relate to traditional crimes that most signatory states have already criminalized (Council of Europe Convention on Cybercrime, Expl. Report § 79). The provision on computer-related forgery creates a parallel crime to the forgery of tangible documents (Council of Europe Convention on Cybercrime, Expl. Report § 81). The provision on computer-related fraud extends the prohibition on fraud to assets represented or administered in computer systems such as electronic funds or electronic money (Council of Europe Convention on Cybercrime, Expl. Report § 86). The provision on crimes related to child pornography aims to modernize existing criminal law provisions to more effectively circumscribe the use of computers and computer networks in the commission of sexual crimes against children (Council of Europe Convention on Cybercrime, Expl. Report § 91). It also includes entirely computer-generated child pornographic images in the scope of the definition of child pornography (Council of Europe Convention on Cybercrime, article 9 (2) c; Expl. Report § 101). And, finally, the provision on crimes related to infringements of copyright and related rights extends existing prohibitions on copyright infringement to the reproduction and dissemination of protected works on the Internet (Council of Europe Convention on Cybercrime, Expl. Report § 107).

Many states that have ratified the Convention on Cybercrime have also ratified its Additional Protocol, which criminalizes four types of human acts of a racist and xenophobic nature that are frequently committed through computer systems. All of them are computer-facilitated crimes; the Additional Protocol aims to extend criminal law that already exists in most signatory states to the commission of traditional crimes through the Internet (Council of Europe Additional Protocol to the Convention on Cybercrime, Expl. Report §3). The Additional Protocol was set up, because the emergence of the Internet provides persons with modern and powerful

means to support racism and xenophobia and enables them to disseminate expressions containing such ideas easily and widely. It builds upon the International Convention on the Elimination of All Forms of Racial Discrimination and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe Additional Protocol to the Convention on Cybercrime, Expl. Report §10).

The first crime category listed in the Additional Protocol is the dissemination of racist and xenophobic material through a computer system (article 3). Racist and xenophobic material can be defined as "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors" (Council of Europe Additional Protocol to the Convention on Cybercrime, article 2). It can be disseminated through a computer system by means of, among other things, the creation or compilation of hyperlinks, the exchange of such material in chat rooms or the posting of messages in newsgroups or discussion fora (Ibid., Expl. Report § 28, 31). The second crime category, racist and xenophobic motivated threat, refers to the utterance of threats against persons through a computer system for the reason that they belong to a group distinguished by any of the aforementioned characteristics (Ibid., article 4; § 35 Expl. Report). The third crime category, racist and xenophobic motivated insult, consists of the offense of persons or a group or persons though a computer system for the reason that they belong to a group which is distinguished by any of the aforementioned characteristics (Ibid., article 5; § 36 Expl. Report).

The last crime category is denial, gross minimization, approval or justification of genocide or crimes against humanity. It refers to the dissemination of material which denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity committed through a computer system (Council of Europe Additional Protocol to the Convention on Cybercrime, article 6). There have been various cases, dealt with by national courts, where persons have expressed ideas or theories, often presented as scientific research, which aimed at denying, grossly minimising, approving or justifying the serious crimes that occurred during the World War II. The scope of this provision is not limited to the crimes committed by the Nazi regime during the World War II but also covers genocides and crimes against humanity committed by other regimes, e.g., in Yugoslavia or in Rwanda (Council of Europe Additional Protocol to the Convention on Cybercrime, Expl. Report § 39, 40).

The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, which has been ratified by most of the member states of the Council of Europe,

establishes another relevant crime category. The aforementioned Convention obliges signatory states to take the necessary legislative or other measures to criminalize the solicitation of children for sexual purposes ("grooming") through information and communication technologies (Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, article 23). Grooming usually starts with the befriending of a child; often the groomer is pretending to be another young person. The groomer will slowly draw the child into discussing intimate matters. Sometimes, pornography is shown to the child. The child may also be drawn into producing child pornography by sending compromising personal photos of him- or herself. This provides the groomer with a means of controlling the child through threats. Finally, the groomer will arrange a meeting in real life with the child (Ibid., Expl. Report § 156). The latter is an essential aspect of grooming: sexual chatting with a child alone is insufficient to incur criminal responsibility, the relationship-forming contacts must be followed by a proposal to meet the child (Ibid., Expl. Report § 157).

Grooming is a computer-facilitated crime: computers or computer networks are used as a tool to establish contacts that could also be established by means of non-electronic communications. Not all countries prohibit non-electronic variants of grooming, however, and the aforementioned provision explicitly does not include them either (Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Expl. Report § 159). It thus differs from country to country whether the provision on grooming requires signatory states to extend an existing legal prohibition or to enact a new legal prohibition. As a rule, conduct that is not prohibited "offline" is not prohibited "online" either, unless computer technology "has such an impact on the nature of the conduct or its prevalence that it necessitates criminalization" (Clough 2010, p. 16). The drafters of the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse felt it was essential to include a provision especially aimed at grooming committed through the use of information and communication technologies, because this is the most dangerous method of grooming, for it is extremely difficult to monitor, both by parents and by legal authorities (Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Expl. Report § 159).

1.1.2 Definition and scope of cybercrime

Against the aforementioned background, cybercrime can be defined as any new or different human act that is carried out through the use of computers or computer networks and is

prohibited by the enactment of a new or the extension of an existing law. It differs from country to country which behaviors involving the use of computers or computer networks are outlawed. The Convention on Cybercrime, its Additional Protocol, and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse provide a list of new and different human acts involving the use of computers or computer networks that are commonly prohibited, i.e., illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, crimes related to child pornography, crimes related to infringements of copyright and related rights, acts of a racist and xenophobic nature that are committed through computer systems, and "grooming."

1.1.3 Meaning of the term "virtual"

The adjective "virtual" has both a pre-computer, traditional meaning and a computer-based meaning (Brey 2008, p. 365). The pre-computer, traditional meaning of the adjective "virtual" is twofold. Firstly, virtual in this sense can mean "quasi" or "pseudo" (Søraker 2010, p. 20). Secondly, virtual in this sense can mean "imaginary", "make-believe", or "fake" (Brey 2008, p. 365). There is no consensus on the computer-based meaning of the adjective "virtual." There are countless definitions, each focusing on a particular context (Søraker 2010, p. 21). What the adjective "virtual" means precisely, seems to be dependent on its context. Below, I will discuss the computer-based meaning of the term "virtual" in different contexts that will prove of importance for this dissertation.

In principle, the term "virtual" can refer to "anything that is created or carried by a computer and that mimics a "real" entity", e.g., virtual memory (Brey 2008, p. 363). Virtual memory is memory that is not actually built into the computer. It is a computer simulation of physical memory and can effectively function as such (Brey 2008, p. 365). The term "virtual" can also be used in the specific context of a virtual environment. Below, I will distinguish two types of virtual environments: virtual worlds and virtual reality environments.

Figure 1 User navigating his avatar through the virtual world of a MMORPG © dantetg 2014 CCO 1.0 (Retrieved from <http://www.pixabay.com/nl/spel-de-strategie-computer-289470>).

A virtual world is an interactive, computer-simulated environment that is accessed by multiple users at the same time (Søraker 2010, p. 44). The first virtual worlds began to appear in the late 1970s. They were text-based online computer games known as MUDs (Multi-User Dungeons). MUD players created a fantasy world only using text. The next stage, graphical MUDs, started in the mid-1980s. They were image- rather than text-based fantasy worlds. In the twenty-first century graphical MUDs evolved into MMORPGs (massively multi-player online role-playing games). The increased Internet access speed and the improved computer-processing power allowed for more complicated graphics such as 3D visuals. The vast majority of MMORPGs can at this day still be described as fantasy worlds (Brenner 2008, pp. 20-23). But over the last decade a few virtual worlds have arisen that eschew the fantasy-based role-playing game play common to MMORPGs. They offer "an augmented version of reality" (Ibid., p. 32). Such virtual worlds are called "metaverses" (Ibid.). The users of virtual worlds represent themselves by means of an "avatar". In graphical virtual worlds an avatar is a graphical object, which usually has a human-like form. In text-based virtual worlds it is a nick name. Through their avatars, users interact with each other and with virtual objects. Virtual objects are merely images that represent certain physical objects such as cars.

A virtual reality environment consists, just like a MMORPG, of an interactive, computer-simulated environment with 3-D visuals. But virtual reality differs from MMORGPs in two important aspects. First of all, users do not experience the three-dimensional, interactive, computer-simulated environment through an avatar but through their own eyes and other senses. Secondly, virtual realities do not offer multi-user access yet; at least not beyond a very limited degree, so users will mainly interact with objects instead of other users (Søraker 2010, pp. 52, 55). Virtual reality is designed to exploit the sensory systems of human beings so as to produce a sense of presence in those environments (Allen 2010, p. 220).

Figure 2 Virtual reality technology: man wears a head-mounted display and datagloves © Amber Case 2009 CC BY-NC 2.0 (Retrieved from <http://www.flickr.com/photos/caseorganic/3493601806>).

Virtual reality technology first emerged in the 1980s. It consists of a head-mounted display and a dataglove or datasuit attached to a computer. As the user navigates through and interacts with the computer-simulated environment, the computer gives sensory feedback through the dataglove or datasuit (Brey 2008, p. 362). Highly advanced datagloves can, for instance, make the user feel resistance when s/he grabs a computer-simulated object in the computer-simulated environment (Søraker 2010, p. 54). Virtual reality technologies are used to simulate both real and imaginary environments. In medicine, they are for instance used to simulate anatomical structures and medical procedures, for example, for the training and education of surgeons (Brey 2008, p. 364).

In his dissertation, Søraker has done extensive research on the computer-based meaning of the term "virtual". He comes to the conclusion that "computer simulation" and "interactivity" constitute the essence of the computer-based meaning of the term "virtual" (Ibid., p. 30). Søraker provides the following generic definition of the term "virtual": a virtual x is an "interactive, computer-simulated x (or, x made possible by interactive computer simulation)" (Ibid., p. 55). This definition focuses exclusively on virtual worlds and excludes from its scope things that are created or carried by a computer and mimic a real thing such as virtual memory, because they are not interactive. Since these things should, for the purposes of this dissertation, be included in the scope of the definition of the term "virtual", I will make use of a generic definition of the term "virtual" that does not necessarily include interactivity. I will take "virtual" to mean computer-simulated or made possible by computer simulation. The computer simulation may or may not be interactive.

1.1.4 State of the art: virtual cybercrime

Applying the above-mentioned definition of the term "virtual", virtual cybercrime can be described as cybercrime that is carried out through the use of a specific feature of computers and computer networks: namely, computer simulation. It is computer-simulated crime, or crime made possible by computer simulation. Virtual cybercrime thus consists of a computer-simulated human act or a human act made possible by computer simulation that is prohibited by law.

The distinction between a computer-simulated human act and a human act made possible by computer simulation is an important one and should, therefore, be highlighted. A computer-simulated human act is an act that is virtual in itself. When someone performs a computer-simulated act, s/he acts in a virtual environment through an input device (Søraker 2010, p. 147). An example of a computer-simulated human act is gambling on a virtual slot machine in a virtual casino. Such a computer-simulated human act consists of three steps. First, a human being

performs a bodily action, e.g., the pressing of a button or the clicking of the mouse. Second, the computer simulation interprets the bodily action as a particular command, e.g., "spin the reel". Third, the computer simulation makes the changes to the virtual environment, and possibly to the non-virtual world as well, that are required by the command (Ibid., p. 137). In this case the reels of the virtual slot machine will spin and stop at a certain point. If the reels show a winning combination of symbols, the player is paid money and if they do not, the player loses money. The money may be won or lost within the virtual environment but it is also possible that it is won or lost in the non-virtual world. Depending on the situation, the computer-simulated human act of gambling on a virtual slot machine in a virtual casino thus may or may not have real financial consequences for the player.

Many countries legally restrict gambling. Gambling is illegal in these countries unless it complies with certain regulations made under law. In some countries, for example, New Zealand, individual persons who participate in illegal gambling are held liable under criminal law (§ 19 (1) (a) Gambling Act 2003). Provided that players can win or lose non-virtual money, these laws are applicable to the computer-simulated human act of gambling on a virtual slot machine.

Other examples of computer-simulated crime are only found in the media and (legal) academic literature as opposed to in actual law (see e.g., Brenner 2008; Clough 2010, pp. 16-21; Kerr 2008). Of them the virtual "rape" that was described by Julian Dibbell in a much-debated 1993 article in the New York newspaper *The Village Voice* is the best-known. Dibbell describes how a user represented by an avatar named "Mr. Bungle" took control over two other users' avatars by means of a "voodoo doll": a subprogram that served the purpose of attributing actions to avatars that their users did not consent to (Dibbell 1993). The user who represented himself by Mr. Bungle pressed buttons and clicked the mouse, and these acts were interpreted by the aforementioned subprogram as commands to attribute (sexual) activities to the avatars, without the consent of their users. As a result, the users were unwillingly confronted with sexual activities involving their own avatars on their computer screens. One of the users claimed to have experienced emotional pain in the non-virtual world due to the event (Dibbell 1993).

A human act made possible by computer simulation is an act that is not virtual in itself but that is defined in terms of a virtual object. Computer simulation is the condition of possibility for such an act and the nature of that act is partly determined by features of the computer simulation (Søraker 2010, pp. 33-34). The production, possession, and distribution of virtual child pornography are examples of human acts made possible by computer simulation. The aforementioned acts are not virtual in themselves but defined in terms of a virtual object: virtual

child pornography. Virtual child pornographic images are child pornographic images which, although realistic, do not involve a child really engaged in sexually explicit conduct. They are either photoshopped pictures of real children or entirely computer-generated images (Council of Europe Convention on Cybercrime, Expl. Report § 101). Computer simulation is thus the condition of possibility for the production and the inherent distribution and possession of virtual child pornographic images. The nature of these acts is partly determined by the features of the computer simulation, because the production, distribution, and possession of virtual child pornographic images do not involve (the profiting from) child abuse, as opposed to the production, distribution, and possession of *non*-virtual child pornographic images.

The production, possession, and distribution of virtual child pornography are commonly prohibited. The Convention on Cybercrime's prohibition on child pornography, as was discussed in section 1.1.1, includes the production, possession, and distribution of virtual child pornography in its scope (Council of Europe Convention on Cybercrime, article 9 (2) c). Not all states that have ratified the Convention on Cybercrime have criminalized the production, possession, and distribution of virtual child pornography, however (see Council of Europe Convention on Cybercrime, List of declarations, reservations and other communications). The production, possession, and distribution of virtual child pornography are thus not as commonly prohibited as the production, possession or distribution of *non*-virtual child pornography.

Some countries, e.g., the Netherlands (article 254a Wetboek van Strafrecht) and the UK (Section 63 (7) Criminal Justice and Immigration Act 2008), also prohibit the production, distribution, and possession of virtual animal pornography, i.e., pornography that realistically depicts humans engaged in sexual activities with animals. The aforementioned acts are not virtual in themselves but defined in terms of a virtual object. Just like virtual child pornographic images, virtual animal pornographic images consist of either photoshopped pictures or entirely computer-generated images. Computer simulation is thus the condition of possibility for the production and the inherent distribution and possession of virtual animal pornographic images. The nature of these acts is partly determined by the features of the computer simulation, because the production, distribution, and possession of virtual animal pornographic images do not involve (the profiting from) cruelty to animals, as opposed to the production, distribution, and possession of *non*-virtual animal pornographic images.

Dutch case law provides another example of a human act made possible by computer simulation that has been brought under the scope of criminal law. In 2009 Dutch judges convicted several minors of theft, because they had stolen virtual items in the virtual worlds of online multiplayer computer games. Three minors were convicted of theft for stealing virtual

furniture in the virtual world of the online multiplayer computer game *Habbo* (2001) (Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791). *Habbo* (2001) is a metaverse and consists of a virtual hotel where players have their own room, which they can furnish. By means of deceit (phishing) the perpetrators obtained the usernames and passwords of other *Habbo* (2001) players, so that they could access the other players' accounts and transfer their virtual furniture to their own *Habbo* (2001) accounts.

In a similar case, two minors were convicted of theft for stealing a virtual amulet and a virtual mask in the virtual world of the online multiplayer computer game *RuneScape* (2001) (Gerechtshof Leeuwarden, 10 November 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764). This judgement was confirmed by the Dutch Supreme Court (Hoge Raad, 31 January 2012, ECLI: NL: HR: 2012: BQ9251). *RuneScape* (2001) is a MMORPG and consists of a virtual medieval fantasy realm in which players earn points and items such as the aforementioned amulet and mask, through their activities in the realm. The perpetrators had violently forced another player of *RuneScape* (2001) to give them access to his account, so that they could transfer his virtual amulet and virtual mask to their own *RuneScape* (2001) accounts.

The acts of stealing in these cases were not virtual in themselves, because they involved infractions outside the game (deceit, violence). But they were defined in terms of virtual objects (the virtual items stolen). Computer simulation was, therefore, the condition of possibility for these acts. Their nature was partly determined by the features of the computer simulation, because the items stolen differed from other items that count as objects that can be stolen under criminal law, among other things because they were not tangible. There have not yet been comparable penalties in other jurisdictions (Hoge Raad, 31 January 2012, Concl. Adv.-Gen., ECLI: NL: HR: 2012: BQ9251).

I am not aware of any other examples of computer-simulated human acts or human acts made possible by computer simulation that have been brought under the scope of criminal law.[2] Remember it was established in section 1.1.3 that the term "virtual" cannot only refer to things that are created or carried by a computer and that mimic a real (non-virtual) thing, but that it can also be used in the specific context of a virtual world or virtual reality environment. Noticeably, the crimes listed above are only virtual in the first meaning. Virtual reality technologies (i.e., interactive, computer-simulated environments with 3-D visuals experienced by users through

[2] There is another example that is often brought up in the media and/or (legal) academic literature but that I do not include in the definition of virtual cybercrime. This example concerns a player of the online multiplayer computer game *Legend of Mir 3* (2004) who was convicted for killing a fellow player, because they had a fight over a virtual sword in the game (see e.g., "Chinese gamer sentenced to life". *BBC NEWS* 8 June 2005.). I think the aforementioned act should not be considered a virtual cybercrime, because it was not computer-simulated or made possible by computer simulation in itself; only the virtual sword that gave rise to a conflict that resulted in the killing satisfied these conditions. This will be further discussed in section 1.2.2.

their own eyes and other senses, see section 1.1.3) have not yet been exploited for criminal activities; at least there have not yet been reported cases of crime instrumented by virtual reality technologies. That is because virtual realities do not yet offer multi-user access or at least not beyond a very limited degree. Except for rare cases of "victimless" crimes such as gambling, crimes generally victimize another person. And thus virtual realities are not likely to provide new opportunities for crime until they become multi-user accessible on a larger scale. Future possibilities for crime involving virtual reality technologies will be discussed in section 1.3.5.

Finally, it is important to note that none of the virtual cybercrimes listed above concern new human activities; they are all different (i.e., virtual) forms of traditional crimes. Virtual cybercrime consists either of a computer-simulated traditional crime (e.g., gambling on a virtual slot machine in a virtual casino) or of a traditional crime that is defined in terms of a computer-simulated person or object (e.g., the production, distribution, and possession of virtual child pornography). Therefore, it only requires legislators to extend existing laws and not to enact new ones.[3]

1.1.5 Definition and scope of virtual cybercrime

Against this background, virtual cybercrime can be defined as a computer-simulated human act or a human act made possible by computer simulation that is prohibited by the extension of an existing law. The scope of virtual cybercrime is unclear, however. Only a handful of human acts made possible by computer simulation, i.e., the production, possession, and distribution of virtual child and animal pornography, and theft of virtual items, have been brought under the scope of criminal law in certain countries. There is also a computer-simulated human act that has been brought under the scope of criminal law: namely, gambling on a virtual slot machine. A much-discussed example of a putative computer-simulated crime is virtual rape. In the next section I will examine what the necessary and sufficient conditions are for a computer-simulated human act or a human act made possible by computer simulation to obtain in order to be prohibited under existing law so that I can ultimately determine the scope of the term "virtual cybercrime".

[3] As will be explained in section 1.2.2, a virtual cybercrime sometimes counts as one crime in the context of its virtual environment and as another crime in the context of the non-virtual world. In chapter 3 I will, for example, argue that a virtual rape like the one Dibbell described counts as rape in its virtual environment but as sexual harassment in the context of the non-virtual world.

1.2 Necessary and sufficient conditions in order to count as a crime

It was established in the last section that only a few virtual cybercrimes have been brought under the scope of criminal law so far. Since it would be a fallacy to make a general statement about virtual cybercrime on the basis of so few examples, the above-mentioned descriptive exploration does not provide a solid basis in order to establish what the necessary and sufficient conditions are in order to bring a computer-simulated human act or a human act made possible by computer simulation under the scope of criminal law. This is, as explained in the introduction, the next step in the legal-ontological study of virtual cybercrime that this chapter aims to provide. Therefore, I will analyze virtual cybercrime from a different point of view in this section. As mentioned at the beginning of this chapter, applied forms of ontology such as legal ontology, often put the tools of general forms of ontology to use in order to categorize things within a specific domain. I will make use of this method and put the tools of the ontology of the American philosopher Searle to use in order to categorize virtual cybercrime within existing law. I choose to draw from Searle's work, because he provides the most influential recent social ontology, which is an ontology that does not focus on matters of biology and physics but on matters of society, and pays special attention to the law. I will first briefly explain Searle's ontology and then apply it to virtual cybercrime. Next, I will argue that ontology alone does not suffice to categorize virtual cybercrime within existing law but that we also need to make use of moral principles.

1.2.1 Searle's ontology

Searle distinguishes between two types of facts: brute facts and social facts (Searle 1995, pp. 2, 5). Brute facts are matters of brute physics and biology. The fact that there is snow and ice on the summit of the Mount Everest is an example of a brute fact. Social facts are matters of culture and society (Ibid., p. 27). The fact that a certain tool is a screwdriver is an example of a social fact. The distinction between brute facts and social facts is of importance, because they have different modes of existence. Brute facts are ontologically objective: they exist independently of any human being. Social facts are ontologically subjective: they exist by human agreement or acceptance (Searle 2010, p. 10).

Ontological objectivity and subjectivity need to be distinguished from *epistemic* objectivity and subjectivity. Unlike ontological objectivity and subjectivity, epistemic objectivity and subjectivity do not refer to the mode of existence of entities but to the truth or falsity of statements that can be made about them. A statement is epistemically objective if its truth or

falsity can be ascertained without reference to the attitudes and feelings of human beings. The statement "Rembrandt was a Dutch painter" is an example of an epistemically objective statement. A statement is epistemically subjective if its truth or falsity cannot be ascertained without reference to the attitudes and feelings of human beings. The statement "Rembrandt was the greatest painter that ever lived in the Netherlands" is an example of an epistemically subjective statement. Its truth cannot be settled independently of the attitudes and feelings of admirers and detractors of Rembrandt's work and the work of other Dutch painters. It is important to note that epistemically objective statements can be made about ontologically subjective facts, for example, if the shopowner tells me that the screwdriver I want to buy costs three Euros (Searle 2001, p. 55).

Social facts come into being because humans have the capacity to impose functions on objects and people (Searle 2010, p. 7). Humans impose functions on objects when they use them for a certain purpose (Ibid., p. 58). For example, a person imposes the function of paperweight on a stone if s/he uses that stone as a paperweight. Some of the objects on which humans impose functions occur naturally such as stones. Others are artifacts, which are specifically designed to serve the function (Searle 1995, p. 14). A screwdriver, for example, is specifically designed to serve the function of driving screws and a car is specifically designed to serve the function of driving. Stones, screwdrivers, and cars are all "material objects" (Ibid.). They can perform the function that is imposed on them in virtue of their physical structure.

Humans can also impose functions on objects if they "cannot perform the functions solely in virtue of their physical structure" (Searle 2010, p. 7). Humans have, for instance, imposed the function of money on pieces of paper and metal (which coins and banknotes essentially are). Contrary to screwdrivers or cars, these pieces of paper and metal cannot perform their function (solely) in virtue of their physical structure. Functions that are imposed on objects that cannot perform the function (solely) in virtue of their physical structure create a special kind of social facts: "institutional facts" (Searle 1995, p. 1). They are special because they do not need to have a physical structure; they only exist because humans believe them to exist (Ibid.).

Institutional facts are typically not generated by individual people but by human institutions (Searle 2010, p. 10). Human institutions are authorities that have been given the power to impose functions on objects according to specific procedures. An example of a human institution is a central bank (e.g., the European Central Bank (ECB) or the Federal Reserve of the USA). Central banks are, among other things, in charge of the issuance of the national currency and one could, therefore, say that, strictly speaking, they impose the function of money on pieces of paper and metal.

The functions that are imposed on objects that cannot perform the function (solely) in virtue of their physical structure and, thereby, create institutional facts are called "status functions" (Searle 2010, p. 7). Status functions cannot only be imposed on objects but also on persons and other entities. Human institutions have, for instance, imposed the status function of President of the USA on Barack Obama and the status function of marriage on a certain ceremony (Ibid.). Status functions "can only be performed in virtue of the fact that the community in which the function is performed assigns a certain status to the object, person, or entity in question, and the function is performed in virtue of the collective acceptance or recognition of the object, person, or entity as having that status" (Searle 2010, p. 94).

Status functions are imposed on entities by means of "constitutive rules." What constitutive rules are can best be explained by contrasting them with regulative rules (Searle 2010, p. 97). Regulative rules characteristically have the form "Do X" (Ibid., p. 10). They regulate antecedently existing forms of behavior (Ibid., p. 9). Regulative rules have an upward or "world-to-word" direction of fit, which can be represented by this symbol: ↑ (Ibid., p. 97). They aim to bring about a certain form of behavior and they are satisfied if the behavior matches the content of the rule. The traffic rule that obliges people to drive on the right-hand side of the road is an example of a regulative rule (Ibid.).

Constitutive rules characteristically have the form "X counts as Y" or "X counts as Y in context C" (Searle 1995, p. 28). They do not only regulate but also create the possibility of the behavior that they regulate (Searle 2010, p. 10). Constitutive rules are a special kind of statements called "Declarations" (Ibid., p. 11). Declarations aim to change reality to match its propositional content but succeed in doing so because they represent the reality as being so changed (Ibid., p. 12). They do not only have a "world-to-word" direction of fit but also a "word-to-world" direction of fit: ↕ (Ibid., p. 97). Declarations declare that a state of affairs exists and, thereby, bring that state of affairs into existence (Ibid., p. 12). An example of a Declaration is the ancient (often codified) constitutive rule that the oldest (surviving) child (X) is the new monarch (Y), which is still applied in modern constitutional monarchies (C) (Ibid., p. 97).

Constitutive rules of the form "X counts as Y in C" can be "*standing Declarations*" (Searle 2010, p. 13). The prefix "standing" means that the constitutive rule "makes something the case but (…) applies to an indefinite number of such somethings" (Ibid., p. 97). Law is a typical example where constitutive rules function as standing Declarations (Ibid., p. 13). The above-mentioned codified constitutive rule that the oldest (surviving) child is the new monarch is, for instance, a standing declaration; it has governed the succession to the throne in many constitutional monarchies since a long time ago.

For the purposes of this dissertation it is important to highlight that penal provisions are also standing Declarations. Penal provisions do not only regulate but also create the possibility of the behavior they regulate, for they prohibit people from performing certain behavior but also declare that it constitutes a crime. Penal provisions consist of constitutive rules which typically indicate that a certain human act (X) counts as a crime (Y) in a particular jurisdiction (C) and apply to an indefinite number of such acts.

Standing Declarations usually specify the conditions under which certain institutional facts will be created (Searle 2010, p. 98). To be more precise, they take the following form: for any x that satisfies a certain set of conditions p, x has status Y in C (Ibid., p. 99). Consider, for example, the US penal prohibition on murder, which makes it the case that any act (x) that satisfies the conditions of unlawful killing of a human being with malice aforethought (p) counts as murder (Y) in the jurisdiction of the USA (C) (18 US Code (USC) § 1111).

(Standing) Declarations do not only assign status to entities but they, thereby, also regulate and create power relationships between people (Searle 2010, p. 106). That is because status functions carry "deontic powers" (Searle 2010, p. 8). Deontic powers consist of rights, duties, obligations, authorizations, and so on (Searle 2010 pp. 8-9). Status functions assign rights, duties, obligations, authorizations, and so on to people, because they relate them to the status function created (Searle 2010, p. 102). If a (standing) Declaration in the form of a legal provision, for example, assigns the status of property to an object it, thereby, also creates property rights for the property owner. And for the purposes of this dissertation, it is important to note that if a penal provision assigns the status of crime to a behavior it, thereby, also creates criminal liability for the perpetrator.

The status of entities and the deontic powers they imply can be unclear (Searle 2010, p. 103). Questions like "Does this act count as a crime under the jurisdiction of a particular country and does it, therefore, give rise to criminal liability?" can arise. Such questions have to be answered by human institutions. As far as the legal status of entities is concerned, these questions are answered by a different human institution than the human institution that assigned the status to the entity in the first place. Under the doctrine of the separation of powers there is one human institution, the legislature, that enacts the law according to a specific procedure[4] (i.e., assigns legal statuses to entities by means of standing Declarations) but another human institution, the judiciary, that interprets the law and applies it to the facts of each case.

In sum, Searle distinguishes a special class of facts: institutional facts. Institutional facts are special, because they are ontologically subjective but epistemically objective: they only exist

[4] Note that this procedure is usually found in the Constitution. Consider, for example, articles 81-87 of the Dutch Constitution (Grondwet voor het Koninkrijk der Nederlanden).

by human agreement or acceptance but the truth or falsity of statements about them can be ascertained without reference to their attitudes or feelings. Institutional facts come into being because human institutions impose status functions on entities that they cannot perform solely in virtue of their physical structure. Status functions are imposed by means of constitutive rules (or: declarations). Many declarations are not applicable to one specific entity but to an indefinite number of entities that all share the same feature(s). They are called "Standing Declarations" and generally take the following form: for any x that satisfies a certain set of conditions p, x has status Y in C. (Standing) Declarations have a double function: they do not only assign status to entities but they also confer rights, duties, and obligations ("deontic powers") upon people. For the purposes of this dissertation it should be highlighted that penal provisions are Standing Declarations. They typically indicate that a human act (X) with certain features (p) counts as a crime (Y) in a particular jurisdiction (C) and can apply to an indefinite number of such acts. Penal provisions do not only assign the status of crime to certain human acts but they also confer the deontic power of criminal liability upon people.

1.2.2 Applications of Searle's ontology

I will now use Searle's framework in order to establish when a computer-simulated human act or a human act made possible by computer simulation can be brought under the scope of criminal law. I repeat that, according to Searle, a human act is considered to be a crime only when a human institution (the legislature or judiciary) has imposed the status function of crime on it by means of a Standing Declaration in the form of a penal provision. Searle claims that penal provisions generally take the following form: for any x that satisfies a certain set of conditions p, x has status Y in C (Searle 2010, p. 99). It follows that a computer-simulated human act or a human act made possible by computer simulation (X) counts as a crime (Y) in the jurisdiction of a particular country (C) when it satisfies a certain set of conditions (p). What this set of conditions entails will be studied below.

In legal terms, the conditions that a human act needs to satisfy in order to count as a crime are called elements. The specific elements required vary depending on the crime but there are two basic elements that are required by each crime: an *actus reus* (an unlawful act or failure to act) and a *mens rea* (a blameworthy mental state; usually such that the actor acts knowingly, purposely or recklessly).[5] In fact, all crimes also require, implicitly or explicitly, that the actus

[5] The terms "actus reus" and "mens rea" derive specifically from Anglo-American jurisprudence. But these elements are, under a different name, also found in other legal systems.

reus must have a certain consequence, e.g., the death or injury of a person or a loss of property. This common element is called *causation*.

In the case of computer-simulated human acts and human acts made possible by computer simulation the basic elements of a crime can be satisfied "intravirtually" (within the virtual environment where the act takes place) or "extravirtually" (outside its virtual environment).[6] The element of actus reus can be satisfied either intravirtually or merely extravirtually. A computer-simulated human act satisfies the element of actus reus intravirtually, because such an act is committed within a virtual environment through an input device. A human act made possible by computer simulation satisfies the element of actus reus merely extravirtually, because such an act, although it is defined in terms of a virtual object, takes place outside the virtual environment. The element of mens rea can only be satisfied extravirtually, even when the element of actus reus is satisfied intravirtually. That is because the element of mens rea concerns the mental state of the human actor, who is necessarily extravirtual.[7] This does not mean that, in the case of an intravirtual actus reus, the mental state of the actor is judged entirely independently from the virtual environment in which the act has taken place, for circumstances in the virtual environment can indicate whether s/he has acted knowingly, willingly or purposely. Like the element of actus reus, the element of causation can be satisfied either intravirtually or extravirtually. The element of causation is satisfied intravirtually when the actus reus has a consequence within the virtual environment and extravirtually when it has a consequence outside the virtual environment. It should be noted that where the element of causation is satisfied, within or outside the virtual environment, is not dependent on where the element of actus reus is satisfied: an intravirtual actus reus can have an extravirtual consequence and vice versa.

Where the element of causation is satisfied, intravirtually or extravirtually, is of crucial importance, because it determines the context (C) in which the crime status (Y) of a computer-simulated human act or human act made possible by computer simulation (X) holds. A computer-simulated human act or human act made possible by computer simulation (X) that satisfies the element of causation (p) *intravirtually* cannot count as a crime (Y) in the context of the non-virtual world (C) but may count as a crime (Y) in the context of its virtual environment (C). A computer-simulated human act or human act made possible by computer simulation (X)

[6] The distinction between "intravirtual" and "extravirtual" derives from Søraker 2012, pp. 504-509.

[7] In the future, the element of mens rea will not necessarily concern the mental state of a human actor anymore, since autonomous, learning machines, based on neural networks, genetic algorithms and agent architectures will be capable of having a mens rea of their own (see Matthias 2004). When such a machine is part of a virtual (reality) environment, the element of mens rea can be satisfied intravirtually as well. Since this paper focuses on computer-simulated *human* acts and *human* acts made possible by computer simulation, the intravirtual mens rea is beyond its scope, however.

that satisfies the element of causation (p) *extravirtually* counts as a crime (Y) in the context of the non-virtual world (C).

The context (C) in which the crime status (Y) of a computer-simulated human act or human act made possible by computer simulation (X) holds, its virtual environment or the non-virtual world, determines whether or not the act can be included in the scope of an existing penal provision. Criminal law does not apply within virtual environments. This is often explained in terms of a "magic circle". In short, the magic circle is a metaphorical line which separates the virtual from the non-virtual realm and excludes criminal law from virtual environments; regulation of conduct within these environments is left to the moderators or users. (For a further analysis of the "magic circle" see section 2.2.) It is important to note that the rules set up by the moderator or users and govern the virtual environment may establish the same crimes as we know in the non-virtual world but they may also prohibit conduct that does not constitute a crime in the non-virtual world or allow for things that are prohibited in the non-virtual world. A computer-simulated human act or a human act made possible by computer simulation that only counts as a crime in its virtual environment thus triggers remedies within that virtual environment but not criminal law. A computer-simulated human act or human act made possible by computer simulation that counts as a crime in the non-virtual world crosses the metaphorical line of the magic circle and is, therefore, within the reach of criminal law. Other authors (i.e., Brenner 2008; Kerr 2008 and Lastowka & Hunter 2004) have reached similar conclusions.

Consider the following example. Most countries prohibit various aspects of the production, trade, and possession of certain drugs, because they can cause severe health problems to the people who use them. Within the virtual world of *Second Life* (2003) users can produce, trade, possess, and use a drug called "Seclimine" through their avatars ("Second Life Seclimine VB Sample". *YouTube* 16 May 2007.). The computer-simulated human act of producing, trading, or possessing Seclimine in *Second Life* (2003) satisfies the element of causation that is implicit in this actus reus intravirtually. After all, Seclimine can only be used through an avatar within the virtual world of *Second Life* (2003) and can, therefore, not cause severe health problems to the person behind the avatar. Since the computer-simulated human act of producing, selling, or possessing Seclimine within *Second Life* (2003) (X) satisfies the element of causation (p) intravirtually, it cannot count as a crime (Y) in the context of the non-virtual world (C). If the rules of *Second Life* (2003) prohibit the producing, selling or possessing of Seclimine, the act does count as a crime in the context of its virtual environment though.

Consider another example. As explained in section 1.1.4, some countries prohibit illegal gambling. The actus reus of illegal gambling can be defined as the unlawful betting or wagering

of money or something else of value. This actus reus implies a certain consequence: financial gain or loss. On the Internet one can gamble illegally in a virtual casino on a virtual slot machine with real, non-virtual money. The computer-simulated human act of illegal gambling on a virtual slot machine with real money satisfies the element of causation that is implicit in this actus reus extravirtually. After all, the money gained or lost is not virtual. Since the computer-simulated human act of illegal gambling on a virtual slot machine with real money (X) satisfies the element of causation (p) extravirtually, it counts as a crime (Y) in the context of the non-virtual world (C) and can thus be brought under the scope of the penal prohibition on illegal gambling that some countries apply.

Sometimes, a computer-simulated human act (X) can satisfy the actus reus element and the attendant element of causation of one crime intravirtually and, thereby, satisfy the actus reus element and the attendant element of causation of another crime extravirtually. Such an act counts, therefore, as crime Y in the context of its virtual environment (C) and as crime Z in the context of the non-virtual world (C).[8] Consider the example below.

Several media reported the case of a 43-year-old Japanese woman who "killed" the avatar to whom her own avatar had been married in the virtual world of the online multiplayer computer game *MapleStory* (2003), because it had suddenly divorced her avatar. The woman hacked into the account of the person behind her virtual husband and deleted his avatar. When the person found out, he called the police. The police investigated the case and arrested the woman at her home but she was never formally charged (see e.g., "Jilted Woman 'Murdered Avatar' ". *SkyNews* 23 October 2008). Provided that the deleting of an avatar is indeed considered manslaughter in the virtual environment of *MapleStory* (2003), the act of the Japanese woman satisfies both the actus reus element (killing) and the element of causation (the death of the avatar) of that crime intravirtually. After all, both the act of killing and the death of the avatar occur within the virtual environment of *MapleStory* (2003).

But the death (deleting) of the avatar in *MapleStory* (2003) also has a consequence in the non-virtual world, for the user who was represented by the avatar has lost his virtual alter ego. As explained in section 1.1.1, countries also commonly prohibit the deterioration of computer data without right (Council of Europe Convention on Cybercrime, article 4). Since an avatar consists of computer data, I would say that the killing of the avatar equals the deterioration of (a set of) computer data. And since the woman illegally accessed the account of the user the avatar represented, it is also without right.[9] By satisfying the elements of the crime of manslaughter

[8] This idea is based on Brey 2014, pp. 49-50.
[9] It should probably be added that this already constitutes a crime in itself and that the woman could, therefore, also be held liable for hacking (in the sense of illegal access) (see article 2 Convention on Cybercrime; section 1.1.1).

intravirtually, the Japanese woman who killed another user's avatar in *MapleStory* (2003) thus satisfies the elements of the crime of deterioration of computer data extravirtually. In sum, the computer-simulated human act of killing an avatar (X), which counts as manslaughter (Y) in the context of its virtual environment (C), counts as deterioration of computer data (Z) in the context of the non-virtual world (C).

With regard to human acts made possible by computer simulation it is important to note that although they merely satisfy the element of actus reus extravirtually, there must always be an aspect of the actus reus that is satisfied intravirtually (i.e., the virtual object in terms of which the act is defined); otherwise it cannot be considered a virtual cybercrime. Consider an example previously mentioned in section 1.1.4: theft of virtual items. The actus reus of theft can, in general terms, be described as the taking of another person's property without his or her consent. If one steals another person's virtual property, all aspects of this actus reus are satisfied extravirtually, except for the property, which resides in a virtual environment.

Consider another example. In 2005 several media reported that a Chinese player of the online multiplayer computer game *Legend of Mir 3* (2004) had murdered a fellow player because they had a fight over a virtual sword in the game. The perpetrator had lent his virtual sword to the victim but instead if giving it back, he had sold it. The perpetrator's attempts to take the dispute to the police failed, because virtual property is not protected under Chinese law (see e.g., "Chinese gamer sentenced to life", *BBC News* 8 June 2005). As mentioned before in section 1.2.1, the actus reus of murder can be described as unlawful killing of a human being with malice aforethought. The reason of killing is not part of the actus reus. In the aforementioned case, none of the aspects of the actus reus of murder were satisfied intravirtually and thus can it not be considered a virtual cybercrime.

In sum, a computer-simulated human act or a human act made possible by computer simulation counts as a crime in the jurisdiction of a particular country when it satisfies a certain set of conditions, which are in legal terms called elements. Each crime consists of the following basic elements: actus reus, mens rea, and causation. A computer-simulated (criminal) human act satisfies the actus reus element intravirtually; a (criminal) human act made possible by computer simulation merely extravirtually. Both satisfy the element of mens rea extravirtually. Where a computer-simulated (criminal) human act or (criminal) human act made possible by computer simulation satisfies the element of causation, intravirtually or extravirtually, determines the context in which it counts as a crime: in the virtual or in the non-virtual world. Criminal law is only applicable in the non-virtual world. So, in order to be brought under the scope of existing criminal law, it is a *necessary* condition for a (criminal) computer-simulated human act or

(criminal) human act made possible by computer simulation that it satisfies the element of causation of the crime extravirtually. But is that also a sufficient condition? Or are there other questions to be met? As will be explained below, the answer to these questions depends on the stand one takes in the legal philosophical debate between legal positivists and natural law theorists.

1.2.3 The debate between legal positivists and natural law theorists

In legal philosophy there are two main rival theories about the content of the law: legal positivism and natural law theory. Legal positivists, like Austin (Austin 1954 [1832]), claim that laws may have any content. They would thus say that legislators and judiciaries are free to bring any computer-simulated human act or human act made possible by computer simulation that has an extravirtual consequence and satisfies the (other) elements of a crime under the scope of criminal law. By contrast, natural law theorists think that the content of laws is determined by their relation to morality. Classical natural law, which was originally developed by ancient philosophers such as Plato and Cicero and further elaborated by Thomas Aquinas, maintains that there is a necessary connection between law and morality and that an immoral law is no law. Typically, there is a particular theory of morality conjoined with that view: that the moral order is part of the natural order and that something is morally right if it is consistent with a natural purpose or end such as survival (Murphy & Coleman 1990, pp. 12, 15). Natural law theorists would say that legislators and judiciaries can only bring a computer-simulated human act or human act made possible by computer simulation that has an extravirtual consequence under the scope of criminal law if the extravirtual consequence consists of a violation of a moral principle.

Searle's framework is neutral with respect to the debate between legal positivists and natural law theorists. Searle neglects morality, for which he is sometimes criticized (see e.g., Zaibert & Smith 2007, p. 164). As Zaibert and Smith point out, Searle has claimed in early work that questions of morality are external to his framework (Ibid., p. 163). I repeat that he claims that a human act is considered to be a crime when a human institution (the legislature or judiciary) has imposed the status function of crime on it by means of a Standing Declaration in the form of a penal provision. But Searle leaves it open *why* human institutions impose the status function of crime on human acts by means of penal provisions, i.e., he leaves it open whether or not they might do so *because of* moral principles. I see it as a strength of Searle's framework that it remains applicable to any variant of legal theory. In this dissertation I do not want to choose

sides in the debate between legal positivists and natural law theorists either. Instead, I will focus on their common ground.

The contemporary debate on the content of the law is dominated by the legal philosophers Hart and Dworkin, and interpretations of their work. Their theories have developed such a level of subtlety and sophistication that the traditional labels of legal positivism and natural law theory hardly apply anymore, however (Murphy & Coleman 1990, p. 36). What has come to be referred to as the Hart-Dworkin debate will be discussed below.

Hart calls himself a soft positivist. In short, he defines law as a system of primary and secondary rules. Primary rules tell human beings how they ought (not) to act. Secondary rules allow human beings to introduce new rules of the primary type, to extinguish or modify old ones, and to apply primary rules in a certain way (Hart 1961, p. 81). The legal validity of primary rules depends on whether they have been created, modified, applied, etc. in accordance with secondary rules (Ibid., p. 107). In legal terms, primary rules are called substantive law and secondary rules procedural law.

Hart explicitly rejects the naturalist claim that there is a necessary connection between law and morality but he does not deny that law and morality overlap (Hart 1961, pp. 185, 193). Hart believes that the law contains a "*minimum content* of Natural Law" (Ibid., p. 193). He thinks that the law incorporates certain "universally recognized principles of conduct" that are also found in morality and which have their basis in central human values such as survival (Ibid.).

Dworkin makes a general attack on legal positivism. He uses Hart's version as a target (Dworkin 1976, p. 34). Dworkin claims that judicial decision involves appeals that are moral in nature, which is a legacy of natural law theory. He does not subscribe to the view that morality is based upon the natural purposes or ends of human beings, however, which is typically conjoined with natural law theory (Murphy & Coleman 1990, p. 40). In short, Dworkin argues that the law does not solely consist of rules, as Hart claims but also of principles. By a principle he means a standard that needs to be observed "because it is a requirement of justice or fairness, or some other dimension of morality" (Dworkin 1976, pp. 34-35). They are most prominently present in difficult lawsuits, for in hard cases judges go beyond the rules and consider principles (Ibid., pp. 41-42).

Hart does not deny the latter, however. He states that "neither in interpreting statutes nor precedents are judges confined to the alternatives of blind, arbitrary choice, or 'mechanical' deduction from rules with predetermined meaning. Very often their choice is guided by the assumption that the purpose of the rules which they are interpreting is a reasonable one, so that

the rules are not intended to work injustice or offend settled moral principles. Judicial decision (...) often involves a choice between moral values" (Hart 1961, p. 204). The core difference between Hart's and Dworkin's theory of law is the following. Hart thinks that, in hard cases, judges appeal to moral principles, which are ultimately grounded in moral values, as a matter of their judicial discretion; he believes that they do not only consider the legal rule at stake but also moral principles, in order to come to the best interpretation of that rule. Dworkin thinks that the moral principles judges appeal to are, although not rules, legally binding (Coleman 1982, p. 144).

For the purposes of this dissertation, however, not the difference but the common ground between Hart's and Dworkin's theory of law is of importance. Hart and Dworkin agree that the law is open to arguments grounded in moral principles. Taking this assumption as a starting point, Van der Burg argues that the law is most strongly open to moral arguments with regard to special fields or issues that are still developing such as biotechnology or Information and Communication Technology (ICT) (Van der Burg 2010, pp. 22, 25). This claim can be explained as follows. As was discussed in section 1.1.1, developing fields or issues such as biotechnology or ICT give rise to new and different forms of human activity that evade the reach of existing criminal law such as virtual cybercrime. It is not always clear how criminal law should deal with them and this uncertainty is exhibited in the case of virtual cybercrime. Moral principles can be used to understand, analyze, and evaluate arguments about how criminal law should deal with these new and different forms of human activity (Van der Burg 2010, p. 7). Yet the question arises which moral principles can help to determine how criminal law should deal with virtual cybercrime. Answering this question will be the aim of the next section.

1.2.4 Feinberg's liberty-limiting (moral) principles

The general question of what moral principles are of importance to determine which human conduct should be criminalized and which not is extensively treated in Feinberg's work *The Moral Limits of Criminal Law*, which consists of four separate books. Feinberg points out that when legislators or judiciaries bring a certain human act under the scope of a penal provision, citizens are no longer "at liberty" to perform that act (Feinberg 1984, p. 7). According to Feinberg such an interference with the liberty of citizens by means of criminal law is usually legitimated on the basis of one of the following liberty-limiting (moral) principles: the harm principle, the offense principle, legal paternalism, or legal moralism (Feinberg 1985, p. ix). I will discuss each of these liberty-limiting principles below.

The first liberty-limiting principle, the harm principle, originally derives from Mill. The harm principle entails "that the only purpose for which power can be rightfully exercised over any member of a civilised community, against his will, is to prevent harm to others'' (Mill 1865, p. 6). For reasons of clarity it needs to be emphasized that Feinberg, contrary to Mill, does not believe that the harm principle is the *only* valid principle for legal coercion: after all he thinks that there are also other liberty-limiting principles (Feinberg 1984, pp. 11-12).

Clearly, the harm principle crucially depends on what is understood by harm (Holtug 2002, p. 357). Mill never explicitly defined harm but Feinberg has done so. He distinguishes between harm in a non-normative sense, which he defines as a setback to interest, and harm in a normative sense, which he defines as a wrong, that is a violation of rights caused by morally indefensible conduct (Feinberg 1984, pp. 33-34). Conduct is morally indefensible if it cannot be justified or excused, e.g., because the victim him- or herself voluntarily consented to a setback of his or her own interests (Ibid., p. 215). Feinberg claims that only setbacks to interests that are wrongs and wrongs that are setbacks to interests can count as harms for the purposes of the harm principle (Ibid., p. 36). He thus defines harm, for the purposes of the harm principle, as a wrongful setback to an interest.

One's interests, or more accurately, the things these interests are in, are components of one's well-being (Feinberg 1984, p. 34). The interests that form the basic requisites of one's well-being are called "welfare interests" and they are protected by law. Welfare interests include: the interest in the continuance of one's life for a foreseeable interval, the interest in bodily integrity, and the interest in the security of property (Ibid., p. 37). Examples of penal provisions that protect the aforementioned welfare interests are, respectively: prohibitions on murder, prohibitions on rape, and prohibitions on theft.

At last it should be added that harms can not only be suffered by an individual person but also by society as a whole. Harms that are suffered by society as a whole consist of wrongful setbacks to "public" interests such as the interest in political or economic stability and the interest in a clean environment. Examples of penal provisions that protect the aforementioned public interests are, respectively: the prohibition on treason, the prohibition on counterfeiting, and antipollution ordinances (Feinberg 1984, pp. 11, 63-64; Goodman & Brenner 2002, p. 178).

The second liberty-limiting principle, the offense principle, is not concerned with (private or public) harm but with offense. Like harm, offense can be defined both in a non-normative and a normative sense. The former includes in its reference all kinds of disliked mental states such as disgust, shame, embarrassment, and fear. The latter refers to those states insofar as they are caused by the wrongful conduct of others. Only offense in this latter sense is intended by the

offense principle (Feinberg 1985, pp. 1-2). Offensive conduct of others is wrongful if it deprives "the unwilling spectators of the power to determine for themselves whether or not to undergo a certain experience", which is a violation of the right to privacy in the sense of autonomy (Ibid., p. 23). The offense principle should not be invoked too easily. Legislators or judiciaries who want to prohibit wrongful offensive conduct have to balance the seriousness of the offense caused (e.g., its intensity and duration) against the independent reasonableness of the offender's conduct (e.g., if wrongful offensive conduct is performed at a location where it is common and known to be common, it is less unreasonable than it would be at a location where it is rare and unexpected) (Ibid., pp. 35, 44, 49). Examples of penal provisions based on the offense principle are: prohibitions on open lewdness, indecent exposure, solicitation, and the distribution or sale of pornography (Feinberg 1984, p. 13).

The third liberty-limiting principle, legal paternalism, is concerned with harm again, like the first liberty-limiting principle: the harm principle. Contrary to the harm principle, legal paternalism is not concerned with harm to *others* but with harm to the *self*. Legal paternalism entails that it is a good and relevant reason in support of a penal prohibition that it prevents harm to the actor him- or herself (Feinberg 1986, p. 4). The interference with a person's liberty is justified by reasons referring exclusively to the welfare interests of the person coerced (Dworkin 1972, p. 65).

According to Feinberg there are two types of paternalism: hard (presumptively blamable) paternalism and soft (presumptively nonblamable) paternalism. Hard paternalism justifies interference with entirely voluntary self-regarding harmful behavior of people for their own good (Feinberg 1986, pp. 5, 12). Soft paternalism "consists of defending relatively helpless or vulnerable people from external dangers, including harm from *other* people when the protected parties have not voluntarily consented to the risk (...)" (Ibid., p. 5). A person's self-regarding harmful behavior is substantially non-voluntary when the choice to perform it stems from coercion, drugs or other voluntariness-vitiating factors and is, therefore, as alien to him or her as the choices of someone else (Ibid., p. 12). Feinberg thinks that the latter type of paternalism is actually no kind of paternalism at all, because it authorizes the restraint of behavior that threatens a person with harm that, although it does not come from another person, is equally "other" from him- or herself (Ibid., pp. 13, 16). He therefore focuses on hard paternalism (Ibid., p. 6).

Examples of penal provisions based on legal paternalism are: prohibitions on the possession use of psychoactive drugs and gambling, as well as requirements, enforced by criminal sanctions such as that motorcyclists wear crash helmets and that motorists use seat belts (Feinberg 1984, p. 8). Most of these penal provisions can, however, not only be defended on the

ground that the actors themselves need to be protected from the harmful consequences of their own acts (legal paternalism) but also on the ground that social harm needs to be prevented generally (the harm principle). That is because there is always a public interest involved; at least to a small extent, when people harm themselves. Think, for instance, of tax money spent on healthcare costs (Feinberg 1986, pp. 21-22).

The last liberty-limiting principle, legal moralism, is not concerned with harm or offense but with evils of other kinds (Feinberg 1988, p. 3). According to Feinberg there are two types of legal moralism: pure and impure moralism. Pure moralism entails that "it can be morally legitimate (...) to prohibit conduct on the ground that it is inherently immoral, even though it causes neither harm nor offense to the actor or to others" (Ibid., p. 4). Impure moralism refers to the approach of some writers in legal philosophy who are called legal moralists, although the basic appeal in their arguments is to the harm or offense principle (Ibid., p. 8). Of them Lord Devlin is the best known. Lord Devlin claims that human conduct is sometimes prohibited solely because society finds it immoral (Devlin 1965, p. 7). He argues that it is legitimate for society to legislate against immorality, because society is kept together by the invisible bonds of a common morality, and would fall apart if these bonds were not protected (Ibid., p. 10). Devlin thus thinks that immoral behaviour harms the social cohesion in society and, thereby, appeals to the harm principle. Examples of penal provisions based on legal moralism are: prohibitions on prostitution and bigamy (Feinberg 1984, p. 13).

To my knowledge, no writer in legal philosophy denies the validity of the harm principle as a good and relevant reason in support of a penal provision. Most writers acknowledge the offense principle as well (see, e.g., Weckert 2000). But legal paternalism and legal moralism are contested (Feinberg 1984, pp. 14-15). Feinberg himself thinks that "harm and offense prevention are far and away the best reasons that can be produced in support of criminal prohibitions, and the only ones that frequently outweigh the case for liberty. (...) The other principles state considerations that are at most sometimes (but rarely) good reasons (...)" (Feinberg 1988, p. 323).

From an empirical point of view, it can be established that the harm principle is the most commonly and frequently used ground for criminalization. Although there are differences across countries and societies in how criminal behaviors are viewed and treated, the core of criminal law, across geography and across time, consists of crimes that produce direct and serious harm to individual persons or groups. Criminal law contains everywhere and at any time penal provisions defining crimes against persons such as murder, assault, rape, and battery. Almost as non-controversial as these crimes against persons are various crimes against property such as theft,

arson, and fraud (Goodman & Brenner 2002, p. 178).[10] Penal provisions based on the offense principle, legal paternalism or legal moralism deviate across geography and across time. Note that, respectively, the distribution and sale of pornography, the possession and use of certain psychoactive drugs, and prostitution are, for example, not prohibited everywhere.

In conclusion, the following moral principles can help determine how criminal law should deal with virtual cybercrime: the harm principle, the offense principle, legal paternalism, and legal moralism. In the last section, it was established that it is a necessary condition for a computer-simulated human act or a human act made possible by computer simulation that satisfies the elements of a crime that it has an extravirtual consequence if it is to be brought under the scope of a penal provision. It can now be established that this is also a sufficient condition if the extravirtual consequence consists of harm (to another or to the self), offense or an evil of another kind. Yet the question arises when computer-simulated human acts or human acts made possible by computer simulation result in harm, offense or evils of other kinds. Answering this question will be the aim of the next section.

1.3 Extravirtual harm to others or the self, offense, and evils of other kinds

In this section I will take a so-called top-down approach[11]: I will apply the harm principle, the offense principle, legal paternalism, and legal moralism to particular examples of computer-simulated human acts or human acts made possible by computer simulation that fall under these principles. In this way I wish to show when computer-simulated human acts or human acts made possible by computer simulation result in extravirtual harm (to others or to the self), offense, or evils of other kinds.

1.3.1 Extravirtual harm to others

As mentioned in the last section, Feinberg defines harm, for the purposes of the harm principle, as a wrongful setback to an interest. He thinks that one's interests, or at least the things these

[10] It should be added that criminal law has started to focus less on harm and more on risk, however. This trend is currently merely visible in the periphery of criminal law. In the Netherlands, for example, local laws have been enacted to ban youths from the places where they hang around in order to prevent vandalism. If this trend continues, it will sooner or later also affect the core of criminal law and make harm a less important ground for criminalization (Koops 2009a, p. 17).

[11] Beauchamp (2003, pp. 7-8) describes the top-down approach as one of the models of moral reasoning in applied ethics.

interests are in, are components of one's well-being. He claims that those interests that are vital for our well-being, our welfare interests, are (to be) protected by criminal law. Yet the question arises when a computer-simulated human act or a human act made possible by computer simulation causes a wrongful setback to a welfare interest. However, before answering this question, it is important to point out two supplementary principles that guide the application of the harm principle in practical contexts.

The first supplementary principle makes sure that criminal law does not concern itself with trivia. It entails that the harm principle can only be invoked if enough well-being is under threat (Feinberg 1984, p. 189). But how great must the infliction upon a welfare interest be in order for the harm principle to warrant criminal law to prevent it? According to Holtug, the harm principle involves a sliding threshold, such that the quantity of well-being that is under threat varies proportionally with the severity of the coercion in question. For example, there must be more well-being under threat to legitimate a prison sentence than a small fine (Holtug 2002, p. 366). If the amount of well-being that is under threat is so minor it cannot even legitimate the imposition of a small fine, the harm principle cannot be invoked at all.

The second supplementary principle is closely connected to the first. It entails that the application of the harm principle requires a conception of normalcy. “It is the person of normal vulnerability whose interests are to be protected by coercive power; the person who, figuratively speaking, can be blown over by a sneeze cannot demand that other people's vigorous but normally harmless activities be suspended by government power” (Feinberg 1984, p. 50). But what is a person of normal vulnerability? Since people and their situations differ, the amount of their well-being that is affected by a certain harmful act can vary. This problem is of crucial importance with regard to interactions in the virtual realm, because one generally does not know who the other person behind the screen is and, therefore, it is even more difficult than in the non-virtual world to estimate to which degree a certain harmful act affects the well-being of the other person.

Criminal law solves the above-mentioned problem by positing a “standard person” who is to be protected from “standard forms of harm” to “standard [welfare] interests” (Feinberg 1984, p. 188). It was established in the last section that the core of criminal law protects interests of personality and interests of property. According to Feinberg, standard interests of personality include absence of harmful bodily contact, freedom from confinement, and absence of emotional distress. Standard interests of property include the exclusive enjoyment and possession of land, chattels and other material resources and their good physical condition. Other legally protectable interests are: interests in privacy and interests in reputation. Not all countries protect the latter

interests by means of criminal law; however, some protect them instead by compelling compensation for harm to them under civil law (Feinberg 1984, pp. 61-62). Finally, as mentioned earlier, criminal law often does not only protect individual interests but also public interests such as the interest in a clean environment and the interest in economic and political stability (Feinberg 1984, pp. 11, 63-64).

Standard inflictions upon interests of personality consist of harm to a person's bodily health through, e.g., murder or assault; harm to a person's mental health through, e.g., harassment; diminutions of a person's security by the creation of threats or dangers, and reductions of a person's liberty of movement through abduction or false imprisonment. Standard inflictions upon interests of property consist of depletion of a person's material resources through, e.g., theft, arson or fraud. Standard inflictions upon interests in privacy consist of intrusions upon solitude such as "stalking" or unpermitted disclosure of intimacies e.g., through unlawful photography or filming (Feinberg 1984, pp. 61-62; Goodman & Brenner 2002, p. 178). It should be added that the precise definition of "stalking" differs from country to country but in general terms it can be described as unwanted, repeated intrusions (e.g., surveillance) and communications (e.g., phone calls, letters, gifts) that are inflicted upon a victim. Standard inflictions upon interests in reputation consist of false statements of fact about a person made in public (defamation). Defamation encompasses both libel and slander: libel refers to written statements or visual depictions; slander refers to verbal statements and gestures. Finally, standard inflictions upon public interests such as the interest in a clean environment and the interest in economic and political stability consist of, respectively, environmental crimes (e.g., pollution); certain economic crimes (e.g., counterfeiting and smuggling), and crimes against the state (e.g., treason, rioting, and obstruction of justice) (Feinberg 1984, p. 11; Goodman & Brenner 2002, p. 178) . Below, it will be examined which of these standard forms of harm to standard welfare interests can be caused by computer-simulated human acts or human acts made possible by computer simulation.

Remember that in section 1.1.4 a computer-simulated human act was described as an act that is performed in a virtual environment through an input device. It consists of three steps. First, a human being performs a bodily action, e.g., the pressing of a button. Second, the computer simulation interprets the bodily action as a particular command. Third, the computer simulation makes the changes to the virtual environment (and possibly to the non-virtual world as well) that are required by the command (Søraker 2010, pp. 137, 147). A human act made possible by computer simulation was described as an act that is defined in terms of a virtual

object. Computer simulation is the condition of possibility for such an act and the nature of that act is partly determined by features of the computer simulation (Ibid., pp. 33-34).

Although it seems improbable at first sight, a computer-simulated human act or a human act made possible by computer simulation may result in harm to a person's bodily health. Consider the following example. In 2008 hackers intruded into the nonprofit Epilepsy Foundation's website and posted a message with a legitimate sounding-title. Users who clicked on the post were redirected to a page with a computer-generated animation that consisted of a pattern of squares rapidly flashing in different colors, which was designed to trigger seizures in both photosensitive and pattern-sensitive epileptics. Several epilepsy patients were affected (Poulsen 2008). This was possibly the first assault made possible by computer simulation and, to my knowledge, the only one. As far as I am aware, the hackers concerned have not been prosecuted.

A computer-simulated human act could do the same type of harm if a user of a virtual environment would, by the press of a button, make such a computer-generated animation designed to trigger seizures appear on the screen of another user who was a photo- and pattern-sensitive epileptic. And if virtual reality technologies became multi-user accessible in the future, the possibilities to do physical harm to persons by means of a computer-simulated human act would increase. As was established in section 1.1.3, virtual reality technology allows a computer to give sensory feedback to a user through a dataglove or datasuit. If virtual reality technology became multi-user accessible in the future, one user could press a button and thereby command the computer to give certain harmful sensory feedback to another user through his or her dataglove or -suit, e.g., an electric shock causing a burn. In section 1.3.5, I will discuss in more detail the possibilities to do harm that virtual reality technologies might allow for in the future.

Much more often than harm to the bodily health of a person, computer-simulated human acts do harm to the "bodily health"[12] of a person's avatar. For example, a person can (use his or her avatar to) assault, rape or torture another person's avatar. This results in (intravirtual) harm to the bodily health of the avatar but does not do (extravirtual) harm to the bodily health of the person him- or herself. Several authors (Huff, Johnson and Miller 2003; Powers 2003; Wolfendale 2007) argue that the computer-simulated human act of harming the bodily health of an avatar may not do harm to the bodily health of the person behind it but can result in harm to that person's mental health. When a person is emotionally engaged in the virtual environment, because s/he is attached to and identifies with his or her avatar, bodily harm done to the avatar is

[12] The term bodily health is used as a metaphor here. The bodily health of an avatar cannot literally be harmed, because an avatar does not have a physical body. But an avatar has a virtual body that can be virtually harmed within the virtual environment.

felt as mental harm to the person (Wolfendale 2007, p. 112, 114-115). As will be further explained in section 3.4, a person whose avatar is raped, for example, can feel sexually harassed. Note that this is one of the special cases as were discussed in section 1.2.2 where a computer-simulated human act (X) satisfies the elements of one crime intravirtually and, thereby, satisfies the elements of another crime extravirtually and, therefore, counts as crime Y in the context of its virtual environment (C) and as crime Z in the context of the non-virtual world (C). With regard to assault and torture of an avatar I doubt whether there is enough well-being under threat to invoke the harm principle.

It should be added that a computer-simulated human act causing harm to a person's mental health is not necessarily aimed at the bodily health of that person's avatar; it can also be of a different nature. Heider provides the following example. "My friend Monica Kanto had land and a nice cabin. An angry neighbor had covered his land with giant purple phalluses, which Monica could clearly see from her house. She was very upset and angry by this turn of events. I had a hard time understanding and relating to how she was feeling. This wasn't her real house; after all (…). But for Monica, who spent four or more hours a day in *Second Life* (2003), it was a serious matter" (Heider 2009, p. 134). In legal terms, Monica felt sexually harassed. As far as I am aware, she did not press charges. But did she suffer harm? The computer-simulated human act of covering land with giant purple phalluses performed by her neighbor clearly had an extravirtual emotional consequence on Monica. However, as Heider indicates, it is highly questionable whether or not the aforementioned act would have the same effect on the standard person. And as explained above, Feinberg claims that is a necessary requirement in order to justify the conclusion that an act is harmful.

A similar event that occurred in *Second Life* (2003) constitutes an example of computer-simulated sexual harassment that would be more likely to meet the above-mentioned requirement. When Ailin Graef, the woman who became a millionaire by investing in virtual real estate in *Second Life* (2003), appeared through her avatar Anshe Chung on a chat show in the virtual world of *Second Life* (2003) to talk about her success, the event was sabotaged by a group of other users. For fifteen minutes, Graef's avatar was swarmed by flying pink phalluses and photographs of Graef herself that were digitally altered to make her look like she was holding a giant phallus. A video of the event was put on *YouTube*. Graef felt sexually harassed (Terdiman 2007). In this case, the sexual harassment within the virtual world of *Second Life* (2003) spilled into the non-virtual world, because the identity of the person behind the avatar was known to the perpetrators. The harassment was not aimed at Graef's avatar (intravirtual) but at Graef herself

(extravirtual). This became especially clear, because a photograph of Graef was used. As far as I am aware, Graef did not press charges.[13]

Harassment cannot only cause harm to the mental health of victims, it can also cause a diminution of the victim's security, if the harassment consists of threats. Recently, a US teen was arrested because he threatened through the chat function of an online multiplayer computer game to shoot up the local high school. A short time later another teen was arrested for making a similar threat. Although both teens said they had just been joking, the police took the threats very seriously (Soave 2013). The aforementioned threats were made possible by computer simulation. One can argue that their nature was also partly determined by computer simulation, for the virtual, game-like environment in which the threats were expressed led to ambiguity with regard to their seriousness.

It seems implausible that a computer-simulated human act or a human act made possible by computer simulation could cause extravirtual reductions of a person's liberty of movement through abduction or false imprisonment; at least I cannot think of an example. In section 1.1.4, I provided two examples of human acts made possible by computer simulation that caused a depletion of the material resources of persons through larceny, which will be further discussed in chapter 2. I will conclude that if virtual property is purchased with funds having extravirtual value (value in the non-virtual world, e.g., pecuniary value), the extortion thereof constitutes extravirtual harm. A computer- simulated human act could lead to the same result.

Computer-simulated human acts or human acts made possible by computer simulation can raise privacy issues as well. One can, for example, make one's avatar stalk another person's avatar in a virtual world. This is a computer-simulated human act. One can also think of the computer-simulated act of unauthorized photography within a virtual world. Vanacker and Heider provide the following example. In 2004 a *Second Life* (2003) user created a building in which he put a screen showing images of so-called "upskirt" pictures he had secretly taken of other user's avatars using a function called "the Alt-cam" (Vanacker & Heider 2011, p. 78). I think it is clear that this "upskirt gallery", as Vanacker and Heider call it, unpermittedly disclosed the intimacies of the avatars concerned.[14] But did it also violate the privacy of the users to whom the avatars belonged? Vanacker and Heider have studied the debate that the upskirt

[13] Graef's (extravirtual) husband filed a complaint with *YouTube*, though not under the prohibition on sexual harassment but under the prohibition on copyright infringement. *YouTube* pulled the video. Later, Graef's husband withdrew his complaint, because he acknowledged that the video, which he still considered a sexual attack on his wife, was not copyright infringement (Duranske 2007b).

[14] This is meant metaphorically. The virtual intimacies of the avatars were unpermittedly disclosed within the virtual environment. *Cf.* footnote 12.

gallery sparked on the *Second Life* (2003) discussion forum. Although many users agreed that no extravirtual harm had occurred, some argued that this was indeed a violation of the privacy of the users to whom the avatars belonged (Vanacker & Heider 2011, pp. 80-82). As far as I am aware, this case has not been brought to court.

Second Life (2003) does not only provide possibilities for unauthorized photography but also for unauthorized filming. Films made in *Second Life* (2003) are often put on *YouTube*. Yet one could film the private moments of an avatar, for example, of the avatar having sex, put the film on *YouTube* without permission and, thereby, violate the privacy of the avatar concerned and possibly also of the user to whom the avatar belongs. This is a human act made possible by computer simulation.

In order to answer the question of whether or not the above-mentioned examples computer-simulated human acts and human acts made possible by computer simulation result in extravirtual harm, I propose to follow the same line of reasoning as was applied to the cases of computer-simulated sexual harassment. Stalking, unauthorized photography or unauthorized filming in the virtual world can spill into the non-virtual world when the perpetrator knows who the person behind the avatar is. I think it is highly questionable, however, whether or not there is enough well-being under threat here, to invoke the harm principle.

Computer simulation also offers new possibilities for defamation. Consider the following example. In 2010 a Dutch man was convicted for libel because he had put a digitally altered image of the then Prime Minister Balkenende online that depicted him, among other things, with a Hitler moustache and swastikas (Gerechtshof 's-Gravenhage, 16 November 2010, ECLI: NL: GHSGR: 2010: BO4035). I would not qualify the aforementioned act as a human act made possible by computer simulation as defined in section 1.1.4. Although computer simulation is the condition of possibility for the act, its nature is not partly determined by the features of the computer simulation. I do not think it makes a difference that the image was digitally altered in order to depict the Dutch Prime Minister with a Hitler moustache and swastika's; the perpetrator could, for instance, also have drawn them on a photograph and that would change nothing about the libelous nature of the act. This would be different if the perpetrator had, for instance, digitally altered or generated an image, indistinguishable from an actual photograph, of the Prime Minister kissing a woman other than his wife. In that case, the features of computer simulation might have made the image look so realistic that it would have made many people to believe the false rumor that the Prime Minister was cheating on his wife.

One can also think of the defamation of avatars here, e.g., by means of a written statement on an Internet forum. Defamation of an avatar cannot only take effect in the non-

virtual world when other users know who the person behind the avatar is. Some people make money through their avatars; think, for example, of the earlier mentioned case of Ailin Graef, who became a millionaire by investing in virtual real estate in *Second Life* (2003) through her avatar. If someone made a false statement of fact about Graef's avatar - for example, that she is involved in virtual real estate fraud - and as a result nobody were willing to do business with her anymore, Graef would suffer a non-virtual financial loss.

In sum, I have established in this section that computer-simulated human acts and human acts made possible by computer simulation can set back interests of personality, interests of property, interests in privacy and interests in reputation. As mentioned at the beginning of this section, criminal law often does not only protect these individual interests but also public interests such as the interest in a clean environment and the interest in economic and political stability. I cannot think of any computer-simulated human acts or human acts made possible by computer simulation that intrude upon public interests, however.

1.3.2 Extravirtual offense

In the last section, it was established that Feinberg defines offense as a disliked mental state such as disgust, shame, embarrassment or fear, caused by the wrongful conduct of others. Offensive conduct of others is wrongful if it deprives "the unwilling spectators of the power to determine for themselves whether or not to undergo a certain experience" (Feinberg 1985, p. 23). According to Feinberg, examples of penal provisions based on the offense principle are: prohibitions on open lewdness, indecent exposure, solicitation, activities and materials offensive to religious or patriotic sensibilities (e.g., blasphemous materials), racial and ethnic slurs, and the distribution or sale of pornography (Feinberg 1984, p. 13).

Weckert, who has done extensive research on offense on the Internet, divides the above-mentioned offensive behaviors into three categories. The first category concerns things that are not necessarily directed at any person or group. This category includes indecent exposure and solicitation. It actually also includes the sale and distribution of pornography but Weckert has excluded pornography from his categorization, because it raises issues of its own (Weckert 2000, p. 108). The second category concerns the ridiculing or criticizing of beliefs and commitments. This category includes activities and materials offensive to religious or patriotic sensibilities. The last category concerns offense taken at language that is racist or sexist, or denigrates people with mental or physical disabilities or the victims of accidents or crimes. This category includes racial and ethnic slurs. It may also include open lewdness insofar as the lewdness denigrates people

with mental or physical disabilities or the victims of accidents or crimes (Weckert 2000, pp. 108-109).

Weckert claims that only the last category of offensive behaviors should be restricted on the Internet. This claim can be explained as follows. As mentioned in the last section, Feinberg thinks that the seriousness of the offense caused (e.g., its intensity and duration) has to be balanced against the independent reasonableness (avoidability) of the offender's conduct when the offense principle is invoked. Weckert points out that most offenses on the Internet can easily be avoided. If one is offended by the content of a certain website, e.g., because it contains materials that one considers blaspheme, one can simply choose not to visit that website. It would be different if one were confronted with the offensive material every time one logged on to the Internet, say by a particular welcoming message or the wording of an image or icon (Weckert 2000, pp. 114-115). And it would definitely be different if one were confronted with the offensive material on the road one had to pass on one's way to work, e.g., on a billboard.

Given the high degree of avoidability of offense on the Internet, only very serious offenses can tip the scales so that the offense principle can be invoked. As Weckert explains, only offenses from the third category are serious enough to do that. They are, contrary to offenses from the first category, aimed directly at (a group of) persons. They also differ from offenses from the second category, since they offend because of characteristics over which people do not have control such as race, gender, and physical appearance, whereas offenses from the second category offend because of characteristics over which people have at least some control such as political and religious beliefs. Offenses from the third category are thus the most serious types of offenses because they single out individuals or groups by characteristics which they have no power to change and; therefore, there is reason to restrict them on the Internet (Weckert 2000, pp. 116-117).[15]

Weckert's argument does not only make sense with regard to human acts involving the use of the Internet in general, it also applies to computer-simulated human acts and human acts made possible by computer-simulation specifically. The degree of avoidability with regard to computer-simulated human acts or human acts made possible by computer simulation is high, because one has the choice not to participate in a certain virtual world known for its offensiveness. Of course, this argument is the strongest with regard to virtual worlds with a pre-designed content. In virtual worlds where users merely shape the virtual world themselves such

[15] If the "unwilling spectator" is a child, there might also be reason to restrict indecent exposure on the Internet, which belongs to the first category of offenses. That is because for children the degree of avoidability of such an offense is lower, especially when an adult persuades them to watch (see Koops 2009b, p. 66). One could argue, however, that indecent exposure of an adult to a child does not constitute offense but mental harm and that thus the harm principle instead of the offense principle should be invoked.

as *Second Life* (2003), it might be problematic for new users to know whether or not they will find (an area of) the virtual world offensive. But ultimately, one can always turn off the computer. So, here, Weckert's conclusion that only offenses from the third category are serious enough to tip the scales and invoke the offense principle applies as well.

Such offenses, i.e., racial or ethnic slurs, and open lewdness insofar as it denigrates people with mental or physical disabilities or the victims of accidents or crimes, are most likely to consist of comments, suggestions, requests, proposals, or other communications in an environment made possible by computer simulation, e.g., a computer game with a chat function. But they can also consist of images (Weckert 2000, p. 106). In the UK, for instance, a man was sentenced to 300 hours of community service because he had posted an offensive digitally altered image of a teenage shooting victim on *Facebook* (Gillett 2012). Computer simulation is the condition of possibility for the aforementioned act. Following the same line of reasoning as was used with regard to libelous images in the last section, the nature of the act is partly determined by the features of the computer simulation if the image looks so realistic that it would make many people to believe it is real. Since I have not been able to find more details on the image at stake, I do not know whether or not that was the case.

Computer-simulated human acts can produce offenses from the third category as well. Think, for instance, of a person who makes his or her avatar do the Nazi salute when it meets a black avatar in a virtual world. No matter whether or not the person behind the avatar is black him- or herself, s/he can take offense.

Offense in the virtual realm differs in one important aspect from harm in the virtual realm: whereas harm can be either intra- or extravirtual, offense can only be extravirtual. In section 1.2.4, harm was defined as a wrongful setback to an interest. As was established in section 1.3.1, a wrongful setback to an interest can be either intra- or extravirtual. Sometimes, an intravirtual wrongful setback to one interest (e.g., bodily harm to an avatar) counts as an extravirtual wrongful setback to another interest (e.g., mental harm to the user to whom the avatar belongs). As mentioned above, offense can be defined as a disliked mental state caused by the wrongful conduct of others. A disliked mental state can only be extravirtual, because it concerns a human being and human beings are necessarily extravirtual. An extravirtual disliked mental state can be caused either by intra- or extravirtual wrongful conduct of others but that does not make a difference for the disliked mental state: one can be as offended by seeing an avatar doing the Nazi salute in the virtual world of a computer game (intravirtual wrongful conduct) as by being shown an offensive (digitally altered) image in the non-virtual world (extravirtual wrongful conduct).

1.3.3 Extravirtual harm to the self

As was established in section 1.2.4, criminal law does not only outlaw behaviors that harm others but also behaviors that harm the *self*. Penal provisions that prohibit behaviors that inflict harm upon the self are called paternalistic. They are justified by reasons referring exclusively to the welfare interests of the person coerced. There are two kinds of paternalistic penal provisions: provisions that *prohibit* certain kinds of behavior such as the use of psychoactive drugs and gambling, and provisions that *require* certain kinds of behavior, enforced by criminal sanctions such as that motorcyclists wear crash helmets and that motorists use seat belts (Feinberg 1984, p. 8). Most of these penal provisions can, however, also be defended on the ground that social harm needs to be prevented generally, because there is always a public interest involved; at least to a small extent, when people harm themselves, e.g., the tax money spent on healthcare costs (Feinberg 1986, pp. 21-22).

In section 1.3.1, I distinguished different types of harm, i.e., harm to a person's bodily or mental health; diminutions of a person's security by the creation of threats or dangers; reductions of a person's liberty of movement through abduction or false imprisonment; depletion of a person's material resources; violations of a person's privacy; defamation, and inflictions upon public interests such as the interest in a clean environment and the interest in economic and political stability. Not all of these types of harm can be inflicted upon the self. Public harms are singled out by definition. It also seems implausible that a person could reduce his or her own liberty of movement through abduction or false imprisonment, or that a person could violate his or her own privacy. Yet the question arises which harms inflicted upon the self can constitute crimes. As will be explained below, Dworkin provides an answer to this question.

In his influential 1972 article on paternalism, Dworkin lists the following eleven examples of paternalistic interferences by law (Dworkin 1972, pp. 65-66):

1. "Laws requiring motorcyclists to wear safety helmets when operating their machines.
2. Laws forbidding persons from swimming at a public beach when lifeguards are not on duty.
3. Laws making suicide a criminal offense.
4. Laws making it illegal for women and children to work at certain types of jobs.
5. Laws regulating certain kinds of sexual conduct, e.g., homosexuality among consenting adults in private.

6. Laws regulating the use of certain drugs which may have harmful consequences to the user but do not lead to anti-social conduct.
7. Laws requiring a license to engage in certain professions with those not receiving a license subject to fine or jail sentence if they do engage in the practice.
8. Laws compelling people to spend a specified fraction of their income on the purchase of retirement annuities. (Social Security)
9. Laws forbidding various forms of gambling (often justified on the grounds that the poor are more likely to throw away their money on such activities than the rich who can afford to).
10. Laws regulating the maximum rates of interest for loans.
11. Laws against dueling."

Not all of these examples concern criminal law. The fourth, eighth, and tenth example concern laws that are generally not part of criminal law. With regard to the fifth example, it should be added that most countries have repealed their laws against homosexuality. Besides, Feinberg thinks that the laws against homosexuality that still exist are not based upon legal paternalism but upon legal moralism, for they are to be found in cultures where homosexuality is considered a "crime against nature" (Feinberg 1986, p. 17). The other examples all concern penal provisions that protect people from harm to their bodily health inflicted by themselves, except for laws forbidding various forms of gambling, which mainly protect people from depletion of material resources inflicted by themselves.

As the seventh example shows, the class of people whose welfare interests are protected does not need to be identical with the class of people being coerced. In the case of professional licensing it is the practitioner's freedom which is directly interfered with and it is the would-be patient or client whose welfare interests are presumably being served (Dworkin 1972, p. 67). This can be called "impure paternalism" (Ibid., p. 68). It might be thought that it is superfluous to distinguish impure paternalism, because any such case could be brought under the scope of the harm principle. The difference between instances of impure paternalism and instances of harm to others is, however, that in the former but not in the latter cases the harm is of such a nature that it could be avoided by the individuals affected if they so chose. The incurring of the harm requires the active co-operation of the victim (Ibid.). In the case of professional licensing the practitioner is coerced so that the would-be patient or client cannot choose to be treated by an unlicensed practitioner, which might cause (bodily) harm.

I will now establish which of the paternalistic laws that Dworkin mentions are

applicable to computer-simulated human acts or human acts made possible by computer simulation. One can think of a computer-simulated equivalent of most of the (potentially) self-harming prohibited human activities mentioned above. One can, for example, make an avatar drive a motorcycle without a safety helmet, swim at an unguarded beach, or commit suicide. And as mentioned in section 1.2.2, people can use a drug called "Seclimine" through their avatars within the virtual world of *Second Life* (2003). Also, many multiplayer computer games, e.g., *World of Warcraft* (2004), allow players to duel against each other through their avatars. But the aforementioned activities only endanger the (intravirtual) bodily health of the avatar; they do not endanger the (extravirtual) bodily health of the person behind it and can, therefore, not be brought under the scope of the paternalistic laws prohibiting there non-virtual equivalents. The only computer-simulated human act that can actually cause extravirtual harm to the self and falls under the scope of one of Dworkin's paternalistic laws is the act of gambling on a virtual slot machine. As was discussed in section 1.1.4, the computer-simulated human act of gambling on a virtual slot machine can be brought under the scope of the (paternalistic) prohibition on (illegal) gambling because it involves real, non-virtual money and can thus cause a depletion of a person's material resources in the non-virtual world.

I can also think of an example of a human act made possible by computer simulation that can cause extravirtual bodily harm to the self and can be brought under the scope of one of the paternalistic laws as distinguished by Dworkin. Unlicensed practice of medicine can be made possible by the Internet and, as will be explained later, also by computer simulation. People make use of the Internet as a source of health information and sometimes engage in what has been called "do-it-yourself-healthcare" (Collste 2000, pp. 119-120). Medical research shows that this can have harmful consequences (Crocco, Villasis-Keever & Jadad 2002). That is because it is difficult to control the reliability of health information on the Internet, since there is no system of licensing or another form of authorization available online (Collste 2000, p. 128-129). Crocco, Villasis-Keever and Jadad describe the following fatal case of do-it-yourself-healthcare by the use of health information on the Internet. A 55-year-old man with cancer found information on the Internet that promoted the use of a certain medicine for cancer treatment. After self-medicating for four months with the medicine, which he had obtained from an alternative medicine website, he died. Autopsy findings suggested an adverse reaction from the use of the medicine (Crocco, Villasis-Keever & Jadad 2002, p. 2870).

In the metaverse of *Second Life* (2003) one can find several virtual hospitals. In some of them users can also consult a virtual doctor through their avatars. Here, the reliability problem arises as well and it might be more pressing than in the previous case. After all, it is difficult to

establish whether or not the person behind the virtual doctor is a licensed doctor. Thus, if a user of *Second Life* (2003) takes medical advice from a virtual doctor, this can be as dangerous for his or her health as relying on health information on the Internet. Therefore, the paternalistic law prohibiting unlicensed practice of medicine is in principle applicable.

The above-mentioned example of extravirtual harm to the self made possible by computer-simulation might be a little far-fetched. After all, it is about a *non*-virtual human being in the *non*-virtual world who takes *non*-virtual medical advice. A much clearer example of extravirtual harm to the self made possible by computer simulation would be computer and video game addiction, which seems to be a growing problem and is associated with a range of mental and bodily health problems such as sleep deprivation, social isolation, neglect of personal hygiene, and failure to eat regularly (http://www.video-game-addiction.org). However, people are not protected against the harmful consequences of excessive gaming by a paternalistic penal law; although Korea, for example, developed a (soft) law which stimulates game-related business operators to take appropriate measures to prevent excessive game immersion or addiction, e.g., by means of display of warnings (article 12-3 Game Industry Promotion Act).

As mentioned above, there is always a public interest involved; at least to a small extent, when people harm themselves as intended by legal paternalism. Paternalistic laws can be defended, therefore, not only on the ground that harm to the self needs to be prevented but also on the ground that harm needs to be prevented in general. This proves true for both the prohibition on (illegal) gambling and the prohibition on unlicensed practice of medicine. The New Zealand prohibition on (illegal) gambling discussed before in section 1.1.4, for example, aims to "prevent and minimize the harm caused by gambling", including harm "suffered by society at large" (Gambling Act 2003 sections 3 (b) and 4 (1) (b) (iv)). The long-term effects of problem gambling include (mental) health problems and criminal convictions (New Zealand Government, Department of Internal Affairs 2007, *supra* 26). These effects are not only harmful for the individual problem gambler but also for society at large, for they lead to increased use of public services such as mental healthcare, primary healthcare, and criminal justice, which are funded with tax money (Australian Psychological Society 2012, § 2). Unlicensed practice of medicine can also lead to increased use of (mainly) the health service system, for it may, as explained earlier, result in serious bodily harm. The same could apply to game addiction, since it is associated with a range of mental and bodily health problems; but, as mentioned before, no paternalistic prohibition on excessive gaming needs to be defended.

1.3.4 Extravirtual evils of other kinds

As was established in section 1.2.4, (pure) legal moralism entails that it is legitimate to prohibit conduct on the ground that it is inherently immoral, although it causes neither harm (to the actor or to others) nor offense. Examples of penal provisions based on legal moralism are: prohibitions on deviant sexual activities such as prostitution and bigamy, provided that they are "harmless (because voluntary or consented to) and unoffending (because not forced on the attention of unwilling observers)" (Feinberg 1988, p. 8). Note that there is much inconsistency as to prohibitions based upon legal moralism, because they are the product of a society's values and religious principles and are, therefore, more idiosyncratic in nature (Goodman & Brenner 2002, p. 179). In the Netherlands, for example, prostitution is legal. And in Morocco, for instance, bigamy is not prohibited.

One can find a computer-simulated variant of prostitution in virtual worlds, for example, in the metaverse of *Second Life* (2003). Some people sell sex through their avatars there. They usually work for a virtual escort service or a virtual brothel. As in the non-virtual world, they charge their clients for their services and give the owner of the escort service or brothel a percentage of their earnings (Brenner 2008, pp. 67-68). Some years ago there was a lot of fuss about a minor who claimed to have worked as a virtual prostitute and then to have been a madam for various virtual brothels through his avatar called "Evangeline" in *The Sims* (2000) ("Evangeline: Interview with a Child cyber-Prostitute in TSO". *The Alphaville Herald* 8 December 2003.).Virtual prostitution differs essentially from non-virtual prostitution, however, since no sexual activity actually occurs; it is a computer-generated animation of sex. Therefore, virtual prostitution can better be described as pornography than as prostitution (Brenner 2008, pp. 67-68). Virtual prostitution is thus one of the special cases discussed in section 1.2.2 where a computer-simulated human act (X) satisfies the elements of one crime intravirtually and, thereby, satisfies the elements of another crime extravirtually and, therefore, counts as crime Y in the context of its virtual environment (C) and as crime Z in the context of the non-virtual world (C).[16]

Because virtual prostitution counts as pornography in the non-virtual world the traditional concerns about morality that historically gave rise to the criminalization of prostitution do not apply (Brenner 2008, p. 68). The offense principle, which generally offers grounds to prohibit pornography, cannot be invoked either, however. As was established in section 1.3.2 the

[16] This holds, insofar as prostitution and pornography are considered crimes. As explained above and before in section 1.2.4, it differs from country to country whether or not prostitution and pornography are considered crimes.

seriousness of the offense caused has to be balanced against the independent reasonableness (avoidability) of the offender's conduct when the offense principle is invoked. In the virtual realm, the degree of avoidability is generally high. Therefore, only the most serious offenses can tip the scales so that the offense principle can be invoked. In section 1.3.2 it was explained that pornography is not a serious enough offense to do that.

Bigamy can also occur in *Second Life* (2003). Although the ceremonies are not legally binding, people can marry each other through their avatars there. People who are already married in the non-virtual world can, through their avatars, marry the avatar of a person who is not their spouse. They find themselves engaged in "cross-world bigamy" (Brenner 2008, p. 68). People can also marry more than one avatar, which constitutes intravirtual bigamy. Neither cross-world bigamy, nor intravirtual bigamy can be brought under the scope of the prohibition on bigamy, however, since the law does not recognize *Second Life* (2003) unions (Ibid., p. 69). Therefore, the underlying traditional concerns about morality that historically gave rise to the criminalization of bigamy do not apply either.

Neither prostitution nor bigamy can be made possible by computer simulation; at least I cannot think of examples. Thus, neither of Feinberg's examples of penal provisions based upon legal moralism is applicable to the virtual realm. Nevertheless, I think that there is a prohibition on a human act made possible by computer simulation that is based on legal moralism; namely, the prohibition on the production, distribution, and possession of virtual animal pornography that a few countries apply (see section 1.1.4).

Consider, for example, the process that led to the criminalization of virtual animal pornography in the Netherlands. Until recently, neither bestiality (i.e., sex with animals), nor the production, distribution, or possession of (virtual) animal pornography were prohibited here. When the press reported that a man who had frequently raped a pony could not be prosecuted because there was no penal provision applicable, a public debate raged. Reports that the Netherlands would be the world's largest producer of animal pornography stirred up the debate (Van Beek 2011, p. 89). People had not been aware that such things existed and when they found out, they were shocked. The shock that went through Dutch society ultimately led to consensus in the Dutch Parliament that bestiality and the production, distribution, and possession of animal pornography, including virtual animal pornography, should be prohibited (Ibid., p. 91).

Prohibitions on bestiality and the production, distribution, and possession of *non*-virtual animal pornography can be legitimated on the basis of the harm principle, as they are believed to involve (the profiting from) animal cruelty. But the production, distribution, and possession of virtual animal pornography do not involve animals of flesh and blood and thus no (profiting

from) animal cruelty. Moreover, there is no evidence that virtual animal pornographic images would encourage or seduce those who watch them to engage in animal cruelty, as some have argued (Van Beek 2011, p. 90). The only reason to prohibit the production, distribution, and possession of these images seems to be that their existence shocks society in a way as described above. Feinberg calls this offense at bare thought. Offense at bare thought can legitimate criminalization, though not on the basis of the offense principle, because the offense at stake is not caused by an unwanted confrontation with the conduct but on the basis of legal moralism. People are offended at the bare thought that certain conduct occurs because they find it immoral (Feinberg 1988, p. 15).

The prohibition on the production, distribution, and possession of virtual animal pornography is modeled on the prohibition on the production, distribution, and possession of virtual child pornography. The latter raises issues of its own to be discussed in chapter 4. I will ultimately come to the conclusion that it is also grounded in legal moralism.

1.3.5 Some short comments on what the future holds

In the sections 1.1.4 and 1.3.1, it was noted that virtual reality technologies will probably allow for new possibilities to do harm to others when they become multi-user accessible in the future. In this subsection I will first describe what kind of new possibilities for human action virtual reality technologies might allow for in the future. Then, I will establish how they can be harmful to others. Next, I will examine whether or not virtual reality technologies could also increase the possibilities for giving offense, doing harm to the self, or acting in an inherently immoral way.

Zhai has written a "philosophical adventure" in which he explores, from a theoretical point of view, what kind of human experiences virtual reality technologies might allow for in the future (Zhai 1998). He explains that state-of-the-art virtual reality technologies entail the following. One wears a helmet or goggles and earphones so that one is not able to see anything except 3-D animated video images on two small screens in front of one's eyes; nor does one hear anything except sounds from the earphones. One also wears a bodysuit, including gloves, that gives different amounts of pressure against different parts of one's body in accordance with one's changing video and audio sensations. One is situated in a motion-tracker that detects one's movements and feeds the signals into the computer that also processes all the visual and audio information so that the computer can coordinate one's movements with the images one sees and the sounds one hears. In this way one is fully immersed in a virtual reality environment, where

the goggles are equivalent to one's eyes and the body suit is equivalent to one's skin (Zhai 1998, pp. 2-4).

In the virtual reality environment one can encounter all kinds of virtual things that are the result of digital programming. One can perceive rocks, trees, animals, etc., with which one can interact. One can, for example, pet an animal, and the glove one wears will give sensory feedback so that it feels like one is really petting an animal. The virtual rocks, trees, and animals one perceives may be equal to the rocks, trees, and animals one has seen before in the non-virtual world but they may also be different. It may be, for instance, that if one lifts one of the rocks it feels like it weighs as much as a rock would weigh in the non-virtual world but it may also be that it feels like the rock is weightless. In the virtual reality environment one can also meet other human beings. They may be virtual human beings whose behavior is totally programmed by the computer, but they may also be the virtual representations of persons who are wired to the same computer system as one is oneself (Zhai 1998, p. 49). When a person interacts with the virtual representation of another person wired to the same computer system, both persons get the sensory feedback belonging to the act from the bodysuit and gloves they are wearing (Ibid., p. 3). One can, for example, shake hands with the virtual representation of another person wired to the same computer system and this information is transformed and transmitted to (the glove worn by) the other person so that s/he feels like his or her hand is shaken. And much more complicated interactions are possible. Zhai describes, for example, how two persons wired to the same computer system could have sex through "a seamless combination of digital simulation, sensory immersion, and functional teleoperation" (Ibid., p. 169).

Zhai does not think that human interactions mediated by virtual reality technologies can be harmful. He states: "(...) in the [virtual reality environment], nobody can physically affect us in a way our self-managed program does not allow. We set the limit in the infrastructure to prevent any serious injury" (Zhai 1998, p. 61). But this idea seems to be too positive. Europol has just launched a project that aims to explore "scenarios for the future of cybercrime" (European Cybercrime Center (EC3) and International Cyber Security Protection Alliance (ICSPA) 2013). These scenarios include crime which involves the use of virtual reality technologies. One of the scenarios is that a user would be able to hack the program of another user's bodysuit and change the settings, which would enable him or her to commit criminal violence against the other user (Ibid., p. 7).

Taking Europol's scenario as a starting point, I imagine that one could hit, kick or otherwise physically hurt the virtual representation of another person wired to the same computer system as oneself and the other person would get painful sensory feedback through his or her

bodysuit. One would even be able to kill the other person when one would, for example, be able to impose an electric shock on him or her through the bodysuit. Bodily harm to the other person could also be done without being wired to the same computer system oneself: one could hack into the program of a user of a virtual reality technology and bodily harm him or her. One could even add a virtual human being to the virtual reality environment that hits, kicks or does another kind of bodily harm. In chapter 3, I will discuss a very specific case of bodily harm to other persons made possible by virtual reality technologies: namely, rape in a virtual reality environment involving a haptic device or robotics. This would entail that one user takes control over another user's haptic device or robot so that s/he can give that user sexually laden sensory feedback to which s/he did not consent (see section 3.1.2). To sum up, virtual reality technologies could allow for increased possibilities to do bodily harm to others through computer-simulated human acts or human acts made possible by computer simulation in the future. Yet the question arises whether or not virtual reality technologies could also allow for new possibilities to give offense, to inflict harm upon the self or to act in inherently immoral ways.

It seems implausible that virtual reality technologies would allow for possibilities to give offense in the future that differ essentially from the possibilities that computer simulation offers already. It was established in section 1.3.2 that offense in the virtual realm differs in one important aspect from harm in the virtual realm: where harm can be either intra- or extravirtual, offense can only be extravirtual. It was explained that offense is a disliked mental state, caused by the wrongful conduct of others, and that a disliked mental state can only be extravirtual, because it concerns a human being and human beings are necessarily extravirtual. An extravirtual disliked mental state can be caused either by intra- or extravirtual wrongful conduct of others but that does not make a difference for the disliked mental state. In general, virtual reality technologies increase the possibilities for intravirtual human acts to have extravirtual consequences. But since offense results in a disliked mental state, which is necessarily extravirtual, virtual reality technologies do not increase the possibilities for giving offense.

Virtual reality technologies could allow for new possibilities to do harm to the self. As was established above, they could offer their users possibilities for hitting, kicking or otherwise physically hurting each other. Virtual reality technologies might, therefore, be used for dueling. They could also provide new ways to commit suicide, e.g., by imposing a fatal electric shock on oneself through one's body suit. Virtual reality technologies might be used for unlicensed practice of medicine as well. But I do not think that they will offer possibilities that differ essentially from the possibilities that computer simulation offers already. The same goes for

gambling. It seems implausible that virtual reality technologies could increase the possibilities for any of the other types of harm to the self that have been discussed in section 1.3.3. They may give one the impression that one, for example, drives on a motorcycle without a safety helmet, swims at an unguarded beach or is under the influence of drugs. But such impressions do not pose real risks to one's bodily health and there is thus no reason to bring them under the scope of criminal law.

Virtual reality technologies could also allow for new possibilities for inherently immoral behavior. In section 1.3.4, it was stated that neither prostitution nor bigamy, Feinberg's examples of inherently immoral behavior, can currently be made possible by computer simulation. Virtual reality technology could make both possible in the future. As mentioned above, Zhai claims that people might be able to have sex in the virtual reality environment in the future. If so, they can also sell sex and thus prostitute themselves in the virtual reality environment. And bigamy could also be made possible by virtual reality technologies in the future. In several countries, including the Netherlands, it is allowed to marry by proxy. One can marry someone who has consented to the marriage but is not able to attend the ceremony, for instance because s/he is far abroad and not able to come over for the marriage. In other words, one marries at a distance. Virtual reality technologies could be used for marriage by proxy. Wearing the goggles, earphones, bodysuit, and glove two persons wired to the same computer could say yes to, exchange a ring with and kiss a virtual representation of each other and the devices would make them hear “yes”, make them feel like they have a ring put around their finger and make them have the sensation of being kissed. Once virtual reality technologies are used for marriage by proxy, bigamy through virtual reality technology will also be possible.

Finally, it might be worth pointing out that virtual reality technologies could lead to confusing situations. Zhai, for example, comes up with an interesting thought. What if the body suits of person A and person B get mixed up? Then, person A gets, through her body suit, the sensory feedback that belongs to the actions that person B performs and vice versa. So if person B hits his leg, person A feels the pain (Zhai 1998, p. 12). In that way (un)intended harm to the self could cause harm to others. One could also confuse a virtual human being with the virtual representation of another person wired to the same computer system. One could then physically hurt the other person believing that it is just a virtual human being that will feel no pain. These confusing situations will not challenge criminal law, however. As was established in section 1.2.2 one of the basic elements that is required by each crime is a *mens rea* (a blameworthy mental state; usually such that the actor acts knowingly, purposely or recklessly). So it depends on whether or not one knew, or could have known, that one could physically hurt another person

by one's act. If not, one cannot have a *mens rea*. And if this basic requirement of each crime cannot be satisfied, an act cannot be brought under the scope of criminal law.

1.4 Conclusion

In this chapter I studied the question when virtual cybercrime should be brought under the scope of criminal law. In order to answer that question I conducted a legal-ontological study of virtual cybercrime, which consists of three steps: a descriptive exploration, a philosophical analysis and a moral evaluation. This chapter consists of three sections; each of them will be discussed below.

The first section of this chapter was concerned with the first step of the legal-ontological study of virtual cybercrime: the descriptive exploration. In this section, I examined what virtual cybercrime is and how, if at all, it is treated within existing legal systems. I defined cybercrime as any new or different human act that is carried out through the use of computers or computer networks and is prohibited by the enactment of a new or the extension of an existing law. I pointed out that it differs from country to country which behaviors involving the use of computers or computer networks are outlawed but that the Convention on Cybercrime, its Additional Protocol, and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse provide a list of new and different human acts involving the use of computers or computer networks that are commonly prohibited. This list includes: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, crimes related to child pornography, crimes related to infringements of copyright and related rights, acts of a racist and xenophobic nature that are committed through computer systems, and "grooming." The first five crime categories concern new forms of human activity that did not exist before the advent of computers and computer networks. That is because they can only be carried out through the use of computers or computer networks. The next crime categories concern traditional crimes where computers or computer networks are used as a tool to commit the crime in a different way.

Subsequently, I described virtual cybercrime as cybercrime that is carried out through the use of a specific feature of computers and computer networks: namely, computer simulation. It consists of a computer-simulated human act or a human act made possible by computer simulation, i.e., a human act that is defined in terms of a virtual object. In contrast with ordinary cybercrime, virtual cybercrime does not concern new human activities, only different human activities. Therefore, it requires legislators to extend existing laws, not to enact new ones. In sum, virtual cybercrime can be defined as a computer-simulated human act or a human act made

possible by computer simulation that is prohibited by the extension of an existing law. It was established that the scope of virtual cybercrime is unclear, however. Only a handful of human acts made possible by computer simulation, i.e., the production, possession, and distribution of virtual child and animal pornography, and theft of virtual items, have been brought under the scope of criminal law in certain countries. There is also a computer-simulated human act that has been brought under the scope of criminal law; namely, gambling on a virtual slot machine. A much-discussed example of a putative computer-simulated crime is virtual rape.

The second section of this chapter was concerned with the second step of the legal-ontological study of virtual cybercrime: the philosophical analysis. In this section I established what the necessary and sufficient conditions are for virtual cybercrime in order to count as crime under existing law. I explained that the descriptive exploration of the law from the first section does not suffice to answer the question what the necessary and sufficient conditions are for a computer-simulated human act or a human act made possible by computer simulation in order to be prohibited under existing law, since the production, distribution, and possession of virtual child pornography are the only virtual cybercrimes that are commonly prohibited and it would be a fallacy to make a general statement about virtual cybercrime on the basis of one specific instance of virtual cybercrime. Therefore, I studied virtual cybercrime from a different point of view. As stated in the introduction, the study of virtual cybercrime belongs to the field of legal ontology. Applied forms of ontology often put the tools of philosophical ontology to use in order to categorize things within a specific domain. I made use of this method and put the tools of the philosophical ontology of the American philosopher Searle to use in order to categorize virtual cybercrime within existing law.

Searle claims that penal provisions generally take the following form: for any x that satisfies a certain set of conditions p, x has status Y in C (Searle 2010, p. 99). So, following Searle, legislators or judiciaries decide that a particular human act (X) counts as a crime (Y) in the jurisdiction of a particular country (C) when they find that the set of conditions (p) for that crime has been satisfied. I explained that, in legal terms, the conditions that a human act needs to satisfy in order to count as a crime are called elements. The specific elements required vary depending on the crime but there are two basic elements that are required by each crime: an *actus reus* (an unlawful act or failure to act) and a *mens rea* (a blameworthy mental state, usually such that the actor acts knowingly, purposely or recklessly). In fact, all crimes also require, implicitly or explicitly, that the actus reus must have a certain consequence, e.g., the death or injury of a person or a loss of property. This common element is called *causation*.

I argued that, in the case of virtual cybercrime, the basic elements of a crime can be satisfied intravirtually (within the virtual environment where the act takes place) or extravirtually (outside its virtual environment), except for the element of *mens rea*, which can only be satisfied extravirtually, since it concerns the human actor, who is necessarily extravirtual. I established that it is of crucial importance where the element of causation is satisfied, intravirtually or extravirtually, because it determines the context (C) in which the crime status (Y) of a computer-simulated human act or human act made possible by computer simulation (X) holds. A computer-simulated human act or human act made possible by computer simulation (X) that satisfies the element of causation (p) *intravirtually* counts as a crime (Y) only in the context of its virtual environment (C); a computer-simulated human act or human act made possible by computer simulation (X) that satisfies the element of causation (p) *extravirtually* counts as a crime (Y) in the context of the non-virtual world (C). In special cases, a computer-simulated human act or human act made possible by computer simulation (X) can satisfy the elements of one crime intravirtually and, thereby, satisfy the elements of another crime extravirtually. Such an act counts, therefore, as crime Y in the context of its virtual environment (C) and as crime Z in the context of the non-virtual world (C).

Subsequently, I claimed that the context (C) in which the crime status (Y) of a computer-simulated human act or human act made possible by computer simulation (X) holds – the virtual environment or the non-virtual world - determines whether or not the act can be included in the scope of an existing penal provision. I explained that lawyers commonly agree that criminal law belongs to the non-virtual realm and that it, therefore, cannot be applied *within* virtual environments. An existing penal provision may thus not be stretched so far as to include in its scope a computer-simulated human act or human act made possible by computer simulation that only counts as a crime in its virtual environment but it may include in its scope a computer-simulated human act or human act made possible by computer simulation that counts as a crime in the context of the non-virtual world.

To sum up, I think that it is a *necessary* condition for a computer-simulated human act or a human act made possible by computer simulation in order to be brought under the scope of criminal law that it has an extravirtual consequence, so that it can count as a crime in the non-virtual world, provided that it also satisfies the (other) elements of a crime. I explained that it depends on the stand one takes in the legal philosophical debate between legal positivists and natural law theorists, whether or not that is a sufficient condition as well. Legal positivists claim that laws may have any content. They would thus say that legislators and judiciaries are free to bring any computer-simulated human act or human act made possible by computer simulation

that has an extravirtual consequence and also satisfies the (other) elements of a crime under the scope of criminal law. Natural law theorists would say that legislators and judiciaries can only bring a computer-simulated human act or human act made possible by computer simulation that has an extravirtual consequence under the scope of criminal law if the extravirtual consequence consists of a violation of a moral principle.

The contemporary debate on the content of the law is dominated by the legal philosophers Hart and Dworkin, and interpretations of their work. Their theories have developed such a level of subtlety and sophistication that the traditional labels of legal positivism and natural law theory hardly apply any more (Murphy & Coleman 1990, p. 36). Most legal philosophers would nowadays agree that the law is open to arguments that are grounded in moral principles, especially with regard to special fields or issues that are still developing such as ICT. Taking this assumption as a starting point, I argued that Feinberg's liberty-limiting (moral) principles, i.e., the harm principle, the offense principle, legal paternalism, and legal moralism, can help to determine how criminal law should deal with virtual cybercrime (Feinberg 1984, 1985, 1986, 1988).

The third section of this chapter was concerned with the third step of the legal-ontological study of virtual cybercrime: the moral evaluation. In this section, I studied when virtual cybercrime meets the above-mentioned necessary and sufficient conditions. I first established that computer-simulated human acts or human acts made possible by computer simulation can result in several types of extravirtual harm to others and that they can, therefore, be brought under the scope of the harm principle. Then, I argued that computer-simulated human acts or human acts made possible by computer simulation can result in extravirtual offense and that they can, therefore, be brought under the scope of the offense principle. Next, I claimed that computer-simulated human acts or human acts made possible by computer simulation can result in extravirtual harm to the self and that they can, therefore, be brought under the scope of legal paternalism. Subsequently, I established that computer-simulated human acts or human acts made possible by computer simulation can result in extravirtual evils of other kinds and that they can, therefore, be brought under the scope of legal moralism.

Finally, I argued that, in the future, virtual reality technologies might allow for new possibilities to do harm (to others or to the self) or to act in an inherently immoral way but that it seems implausible that virtual reality technologies would allow for possibilities to give offense that differ essentially from the possibilities that computer simulation offers already. That is because virtual reality technologies increase the possibilities for intravirtual human acts to have extravirtual consequences. But since in the case of offense the consequence, a disliked mental

state, is necessarily extravirtual, virtual reality technologies do not increase the possibilities to give offense.

PART II: CASE STUDIES

CHAPTER 2 THEFT OF VIRTUAL ITEMS

An earlier version of this chapter was published as a paper titled "Theft of virtual items in online multiplayer computer games: an ontological and moral analysis." *Ethics and Information Technology*, *Volume 14*, *Issue 2*, 89-97 (2012).

Introduction

This second chapter consists of a case study of theft of virtual items in online multiplayer computer games. It takes the Dutch convictions for theft of virtual items in the virtual worlds of the online multiplayer computer games *Habbo* (2001) and *RuneScape* (2001) mentioned before in chapter 1 as a starting point. The facts of these cases will briefly be described below. The issue of theft of virtual items in online multiplayer computer games is not limited to these two cases, however. Research suggests that in the (near) future there might be "a mature illicit market for virtual items, both stolen and counterfeit" (European Cybercrime Center (EC3) and International Cyber Security Protection Alliance (ICSPA) 2013, p. 7).

In 2009 Dutch judges convicted three minors of theft for stealing virtual furniture in the virtual world of the online multiplayer computer game *Habbo* (2001) (Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791). *Habbo* (2001) consists of a virtual hotel where players have their own room, which they can furnish. The perpetrators had used phishing techniques to create a false website and to trick other players of *Habbo* (2001) into providing their usernames and passwords, so that they could access their accounts and transfer their virtual furniture to their own *Habbo* (2001) accounts.

In a similar case, two minors were convicted of theft for stealing a virtual amulet and a virtual mask in the virtual world of the online multiplayer computer game *RuneScape* (2001) (Gerechtshof Leeuwarden, 10 November 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764). This judgement was confirmed by the Dutch Supreme Court (Hoge Raad, 31 January 2012, ECLI: NL: HR: 2012: BQ9251). *RuneScape* (2001) is a virtual medieval fantasy realm in which players earn points and items such as the aforementioned amulet and mask, through their activities in the realm. The perpetrators had violently forced another player of *RuneScape* (2001) to give them access to his account, so that they could transfer his virtual amulet and virtual mask to their own *RuneScape* (2001) accounts. They had hit and kicked him and threatened him with a knife.

As was established in section 1.1.4, the acts of stealing in the above-mentioned cases are human acts made possible by computer simulation. They are not virtual in themselves, because

they involve infractions outside the game (deceit, violence), but they are defined in terms of virtual objects (the virtual items stolen). The legal status of these virtual objects is subject of dispute. Lawyers in- as well as outside the Netherlands have extensively debated on the question of whether or not virtual items such as a virtual mask, a virtual amulet, and virtual furniture, should count as "objects" that can be "stolen" under criminal law (e.g., Hoekman & Dirkzwager 2009; Moszkowicz 2009; Rijna 2010; Brenner 2008; Kerr 2008). Some of them are convinced that virtual items are "mere illusions" to which "real world law" does not apply; others see them as a new form of property deserving legal protection (Ibid.). In this chapter I aim to answer the aforementioned question from a legal-ontological point of view. I will apply the general findings from the first chapter to this particular instance of virtual cybercrime and study the specific issues that arise.

The structure of this chapter will be as follows. In the first section, I will analyze the ontology of the virtual worlds of (online multiplayer) computer games and the virtual entities that can be found in there. I will make use of the findings of Brey who, in turn, draws from the social ontology of Searle discussed before in section 1.2. On the basis of my ontological analysis I will argue that the answer to the question of whether or not virtual items can count as objects that can be stolen depends on whether or not the act of stealing them can count as theft in the non-virtual world. In the second section, I will examine whether or not it makes sense to see the act of stealing virtual items in an online multiplayer computer game as theft. I will establish that this only makes sense if the virtual items count as property worthy of value in the non-virtual world. The third section takes up the question whether or not virtual items in the virtual world of an online multiplayer computer game can count as such. I will come to the conclusion that virtual items can, under certain circumstances, be considered property worthy of pecuniary or hedonistic value in the non-virtual world.

2.1 Ontology in the virtual worlds of computer games

The virtual items encountered in the virtual worlds of online multiplayer computer games such as *Habbo* (2001) or *RuneScape* (2001) can be divided into two main categories. On the one hand, virtual items can be representations of real entities; in the virtual world of a computer game one can, for instance, encounter a virtual chair or a virtual car. On the other hand, one might encounter virtual items that do not have a real, non-virtual counterpart such as a virtual dragon or a virtual gnome. These items are not only virtual; they are also fictitious. According to Brey the first category of virtual items, the representations of real entities, can be further categorized as

follows. He thinks that they are either "mere simulations of real-world entities" or "genuine ontological reproductions, recognized as part of reality" (Brey 2003, p. 282).

The virtual representations of real entities that have certain essential physical properties such as mass, are mere simulations. The virtual counterparts of such real entities are not recognized as part of reality, because computers are evidently "not able to reproduce their essential physical properties" (Brey 2003, pp. 277-278). Consider the following example. Although the producer claims that its new computer game *Gran Turismo 5* (2010) provides a real driving experience, driving a car through the mountains in the virtual world of *Gran Turismo 5* (2010) is not normally interpreted as a real experience but as a mere simulation, because computers are not able to reproduce the essential physical properties of a car (e.g., the mass) and mountains (e.g., the height). The virtual representations of real "institutional" entities can be genuine ontological reproductions, recognized as part of reality. Below, it will be explained what institutional entities are and why they can be adequately ontologically reproduced in virtual environments.

By institutional entities Brey means entities on which a status function has been imposed by means of Searle's constitutive rule "X counts as Y in context C" (see section 1.2). As Brey points out, institutional entities can be adequately ontologically reproduced in virtual worlds, because they usually do not need to have physical properties of the kind that cannot be reproduced by computers. "In principle, any status function can be assigned to anything, if only there is the collective will to do it" (Brey 2003, p. 278). However, in practice, people will only assign status functions to entities that have the features that make it sensible to do that (Ibid.).

According to Brey many real institutional entities are ontologically reproduced in virtual environments nowadays, because there are "many virtual entities that lend themselves well to the meaningful assignment of status functions" (Brey 2003, pp. 278-279). He divides the virtual counterparts of real institutional entities into two categories: "real institutional activities" and "requisite objects" (Ibid.). Online gambling is an example of a real institutional activity; a virtual slot machine is the requisite object. Another example of a real institutional activity is online banking; virtual (or: electronic) money is the requisite object.

Yet the question arises as to which category the virtual mask, virtual amulet, and virtual furniture that were at stake in the *RuneScape* and *Habbo* cases belong. These virtual items are not fictitious; they are representations of real entities. At first glance one would say that they belong to the subcategory of virtual items that are mere simulations of real entities, because computers are evidently not able to ontologically reproduce the essential physical properties of furniture, a mask or an amulet such as their mass. If one looks at them from a legal perspective,

however, one can argue that the virtual mask, virtual amulet, and virtual furniture that were at stake in the *RuneScape* and *Habbo* cases are genuine ontological reproductions, recognized as part of (institutional) reality. The judges in these cases seem to have assumed that the act of stealing in the virtual world of *RuneScape* (2001) or *Habbo* (2001) is a real institutional activity. In line with Searle's "constitutive rule" they have recognized that the act of stealing in the virtual world of these online multiplayer computer games (X) counts as theft (Y) in the non-virtual world (C). They have, thereby, also recognized that the requisite objects, a virtual mask, virtual amulet, and virtual furniture (X), count as objects that can be stolen (Y) in the non-virtual world (C).

As mentioned earlier, Brey claims that status functions are usually only assigned to entities in virtual worlds that have the features that make it sensible to do that (Brey 2003, p. 278). The *Habbo* and *RuneScape* cases raise the question whether it makes sense to see the act of stealing in the virtual world of an online multiplayer computer game as the real (ontologically reproduced) institutional activity of theft and virtual items as requisite objects (objects that can be stolen). Answering these questions will be the aim of the following sections.

2.2 Stealing in the virtual world of an online multiplayer computer game, real theft?

I will start with the question whether it makes sense to see the act of stealing in the virtual world of an online multiplayer computer game as the real institutional activity of theft. In order to gain as broad a picture as possible, I will make use of different models of (moral) reasoning. These models are: the top-down model, the bottom-up model, and the coherence method. What these models of moral reasoning entail, will be explained below.

2.2.1 Reasoning top-down: taking the prohibition of theft as a starting point

At first glance, the "top-down model" seems the best way to find the answer to the question at stake. In a top-down model of reasoning, it is established whether a new, particular situation falls under a general rule. A general rule can for instance consist of a principle, a norm or an ideal (Beauchamp 2003, p. 7). In this case, it needs to be established whether the act of stealing in the virtual world of an online multiplayer computer game falls under the prohibition of theft, which is a (penal) norm.

As was briefly mentioned before in section 1.2.2, many lawyers argue that (criminal) law should not be applied within the virtual worlds of computer games (e.g., Brenner 2008; Kerr 2008; Moszkowicz 2009; Rijna 2010). They think that there is a kind of metaphorical line, a "magic circle", between the fantasy realms of the virtual worlds of computer games and the non-virtual world (Fairfield 2009, p. 824; Salen & Zimmerman 2004, pp. 93-100). The concept of the magic circle originally derives from the Dutch philosopher Huizinga (Huizinga 1950 [1938]). The thrust of the magic circle is that conduct that is performed in a (computer) game setting is not real and can, therefore, not be sanctioned by real law (Fairfield 2009, p. 825).

There does indeed seem to be a magic circle. In the virtual worlds of computer games players often act out scenarios that would fall under a penal norm if performed in the non-virtual world (Fairfield 2009, p. 826). In the virtual world of the computer game *Grand Theft Auto V* (2013) for instance, players can kill policemen. An actual murder charge has never been brought against a player who killed a policeman in *Grand Theft Auto V* (2013), however.

The magic circle can be explained as follows. The virtual worlds of computer games are, usually, governed by the rules of the game. Some of them, e.g., *Habbo* (2001) and *RuneScape* (2001), are governed by "formally generated rules", which are set by the company that owns and operates the computer game and to which players have to agree before they can play the game. The virtual worlds of other computer games, e.g., *Second Life* (2003), are governed by "informally generated rules", which are agreed upon by players themselves (Fairfield 2009, pp. 831-832). As long as players act out scenarios that fall under the scope of these rules, there is no room for legal regulation (Ibid., p. 826). An undesirable act can then be sanctioned by a punishment set by the company that owns and operates the computer game or a punishment on which the players have collectively agreed. On the other hand, if a player acts out a scenario that does not fall under the scope of the (formally or informally generated) rules of the game, the metaphorical line of the magic circle is crossed and the act might, therefore, be subjected to (criminal) law instead (Ibid., pp. 831-832).

Computer games can be compared to sports such as soccer, with regard to this matter. During a soccer game players often perform acts, such as kicking an opponent player, that would fall under a penal norm (e.g., battery) if performed in a different context. In the context of a soccer game, however, the aforementioned behaviour will usually be governed by the rules of the game and the player will, for instance, be shown a yellow or a red card. But, as the following example shows, an act performed during a soccer game can exceed the rules of the game and, therefore, be subjected to criminal law instead. In 2004 a Dutch soccer player committed a foul on an opponent player and thereby caused his leg to break in several places. He was convicted of

battery under criminal law (Hoge Raad, 22 April 2008, ECLI: NL: HR: 2008: BB7087). The judges in this case established that there are two types of situation in which an act performed in a game context does not fall under the scope of the rules of the game. First of all, an act can constitute such a grave violation of the rules of the game that they do not provide an adequate punishment. Secondly, an act can be (partly) performed outside the game setting (Ibid., § 4.5).

The first type of situation was at stake in the case at hand: even the most severe punishments of the soccer rules, penalty and expulsion, are not proportional to a compound leg fracture. This type of situation could also occur in the context of an online multiplayer computer game. Consider the following example. Some online multiplayer computer games, e.g., *Habbo* (2001) and *RuneScape* (2001), provide a chat interface. Generally, the rules of these computer games prohibit the use of racist language. Players who break this rule face a penalty, usually in the form of a (temporary) ban or mute. But if a player uses racist language that is found to be so offensive that a (temporary) ban or mute is not considered to be a proportional punishment, a penal norm, i.e., the prohibition on hate speech, might be applied instead.

As the judges in these cases explain, the second type of situation was at stake in the *Habbo* and *RuneScape* cases (Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791; Gerechtshof Leeuwarden, 10 November 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764). The acts of stealing in *Habbo* (2001) and *RuneScape* (2001) were partly performed outside the setting of these games, because they involved infractions outside the game. In the *Habbo* case, the act of stealing was accomplished through out of the game deceit. The perpetrators had used phishing techniques to create a false website and to trick other players of *Habbo* (2001) into providing their usernames and passwords, so that they could access the other players' accounts and transfer their virtual furniture to their own *Habbo* (2001) accounts (Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791). In the *RuneScape* case, the act of stealing was accomplished through a physical confrontation in the non-virtual world. The perpetrators had violently forced their victim to give them access to his account so that they could transfer the virtual amulet and virtual mask to their own accounts. They had hit and kicked him, and threatened him with a knife (Gerechtshof Leeuwarden, 10 November 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764).

The acts of stealing in the *Habbo* and *RuneScape* cases thus crossed the metaphorical line of the magic circle and do, therefore, not fall under the scope of the rules of the game but if we want to bring them under the scope of criminal law instead, we first have to examine whether or not they satisfy the necessary and sufficient conditions for criminalization as were established in section 1.2. It was established in section 1.2 that a virtual cybercrime must necessarily have an

extravirtual consequence (a consequence outside the virtual environment) in order to count as a crime under existing law. It was added that not any extravirtual consequence suffices; it needs to be of such a nature that it can legitimate an interference with the liberty of citizens by means of criminal law on the basis of one of Feinberg's liberty-limiting principles, which means that it has to result in (extravirtual) harm, offense, harm to the self or an evil of another kind.

Online multiplayer computer games such as *Habbo* (2001) and *RuneScape* (2001), involve "networked computers and multiple users" (Allen 2010, p. 232). Therefore, it is possible that the act of one player has an extravirtual impact on another player or other players, albeit through the computer-mediated world of the game (Fairfield 2009, p. 825). Yet the question arises whether or not this extravirtual impact can be of such a nature that it can legitimate an interference with the liberty of citizens by means of criminal law on the basis of one of Feinberg's liberty-limiting principles.

2.2.2 Reasoning bottom-up: taking Feinberg's liberty-limiting principles as a starting point

In order to answer the above-mentioned question it helps to stop reasoning top-down but to reason the other way around; to take the case as a starting point instead of the general norm or principle. This way of moral reasoning is called bottom-up reasoning, which works as follows. Bottom-up models of moral reasoning include several distinct methodologies, of which casuistry (case-based reasoning) is the most used (Beauchamp 2003, p. 8). In case-based reasoning, the new, particular situation is compared to one or more cases to which the general rule does or does not apply (Søraker 2007, p. 342). If the new, particular situation is relevantly similar to the paradigmatic case(s), it should be treated in a similar manner; if it is relevantly different, it should be treated differently (Ibid.). This method of moral reasoning has much in common with legal case-based reasoning (case-law): the decision of a court can be authoritative for other courts hearing cases with similar facts (Beauchamp 2003, p. 9).

Real-life cases in which theft is widely acknowledged as such result in harm. As mentioned before in section 1.3.1, Feinberg defines harm, for the purposes of the harm principle, as a wrongful setback to a welfare interest (i.e., an interest which is vital for our well-being). Real-life cases of theft constitute a violation of the property rights of the property owner (Stewart 2010, p. 20). Property rights can be seen as interests which are vital for our well-being (Feinberg 1984, p. 62). This can be explained as follows. According to the prevalent common-sense conception of well-being, wealth is conducive to well-being (Søraker 2010, p. 263). And

property, or at least valuable property, is conducive to wealth. A deprivation of valuable property thus causes a deprivation of wealth and, therefore, of well-being. The key harm that is caused by theft is pecuniary loss (Steel 2008, p. 736).

The act of stealing virtual items in the virtual world of an online multiplayer computer game will thus be relevantly similar to real-life cases in which theft is widely acknowledged as such if these virtual items are valuable property, and it will be relevantly different if they are not. Apparently, the act of stealing virtual items in the virtual world of an online multiplayer computer game satisfies the necessary and sufficient conditions in order to count as the crime of theft under existing law if the virtual items stolen are valuable property. It is here, that top-down and bottom-up reasoning reconcile. If the focus is on the requirement that the case has to meet in order to fall under the scope of the general rule, neither the case nor the general rule is taken as a starting point for moral reasoning. This way of reasoning is called the "coherence method" (Beauchamp 2003, p. 10). The coherence method enables us to shift back and forth between the general rule and the case via the necessary requirement until they fit each other (Søraker 2007, p. 345).

Yet it can (preliminarily) be concluded that it makes sense to bring the act of stealing virtual items in the virtual world of an online multiplayer computer game under the prohibition on theft if these virtual items count as valuable property in the non-virtual world. In the next section it will be established whether virtual items can meet this requirement. It should be noted that, thereby, I do not only reach a final conclusion on the question whether it makes sense to see the act of stealing in the virtual world of an online multiplayer computer game as theft, but I will also establish whether it makes sense to see virtual items as requisite objects of theft (objects that can be stolen).

2.3 Virtual items: real property, real value?

In this section it will first be established whether or not virtual items can count as real property in the non-virtual world. Then, it will be established whether or not they represent real value in the non-virtual world.

2.3.1 Virtual items as real property

At first glance, one would say that virtual items in the virtual world of an online multiplayer computer game are the property of the company that owns and operates the game. The terms of service (ToS) of most online multiplayer computer games, e.g., those of *Habbo* (2001) and *RuneScape* (2001), state that all items in the game are the (intellectual) property of the company that owns and operates the game. This determination does not enable us to bring the act of stealing virtual items in the virtual world of the online multiplayer computer game under the scope of the prohibition of theft, however. After all, when one player steals virtual items from another player within the virtual world of an online multiplayer computer game, the property rights of the company that owns and operates the game remain unviolated.

The requirement that the act of stealing virtual items in the virtual world of an online multiplayer computer game has to meet in order to fall under the scope of the prohibition on theft thus needs to be refined. If it can be established that virtual items in the virtual world of an online multiplayer computer game also count as a particular player's (valuable) property in the non-virtual world, the act of stealing them in the virtual world of the computer game constitutes a violation of this player's property rights and it thus makes sense to bring this act under the prohibition on theft. Can virtual items count as a particular player's property in the non-virtual world? Before answering this question it should be noted that the fact that virtual items in the virtual world of an online multiplayer computer game are formally owned by the company that owns and operates the computer game, is not an obstacle to consider them also (valuable) property of a player in the non-virtual world, for the purpose of applying criminal law (Gerechtshof Leeuwarden, 10 November 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764).

(Private) property can be defined as a system that allocates particular objects to particular persons, to the exclusion of others (Waldron 2004, introduction). An object is allocated to a person if some past event of appropriation has established that person as the owner. The past event of appropriation can, for instance, consist of the effort that has been put into acquiring the property. In his famous *Two Treatises of Government* Locke stated: "whatsoever then he removes out of the state that nature hath provided, and left it in, he hath mixed his labour with, and joined to it something that is his own, and thereby makes it his property" (Locke 2007 [1689], p. 30, § 27). But, as Hume has pointed out, one may, for instance, also acquire property by a payment ("fortune") (Hume 1978 [1739], p. 489).

Virtual items in the virtual world of an online multiplayer computer game can be brought under the above-mentioned definition of property. They are allocated to a particular player of the

game, to the exclusion of other players, when they are accessible only through the owner's account with a password and username. The past event of appropriation that established a particular player of an online multiplayer computer game as the owner of a virtual item can consist of the effort that was put into acquiring it. In the virtual world of *RuneScape* (2001), for instance, players can purchase items such as a virtual mask and a virtual amulet, by the performance of certain tasks. The past event of appropriation can also consist of a payment. In the virtual world of *Habbo* (2001), for instance, players can purchase virtual furniture with "credits", which they can buy with real, non-virtual money.

In sum, virtual items in the virtual world of an online multiplayer computer game can count as a particular player's property in the non-virtual world. Can they also represent value in the non-virtual world? In order to determine the real, non-virtual value of a virtual item one has to go back to what defined it as property. That is because the value that virtual property represents in the non-virtual world is related to the nature of the event of appropriation by which a person has established him- or herself as the owner.

2.3.2 The real, non-virtual value of virtual items

If a player really needs to pay in order to purchase a virtual item in the virtual world of an online multiplayer computer game, this virtual item represents pecuniary value in the non-virtual world (Rijna 2010, pp. 792-793). As a matter of fact, most things that count as property in the non-virtual world are of pecuniary value. As was established in the last section, the key harm that is caused by theft is pecuniary loss.

Virtual items that cannot be purchased by a payment but only by effort, such as the virtual mask and the virtual amulet that were at stake in the *RuneScape* case, do not represent pecuniary value in the non-virtual world; at least not officially.[17] But they do (also) represent another type of value, which is not conducive to wealth but to another aspect of well-being. According to Mooradian, hedonism is the philosophical theory of well-being that best explains (non-pecuniary) value attributions to virtual entities (Mooradian 2006, p. 688). Hedonism claims that all and only pleasure has value and all and only pain has disvalue for well-being. Both pleasure and pain are understood broadly. Pleasure is taken to include all pleasant experience;

[17] Some players trade virtual items in the virtual worlds of online multiplayer computer games such as *RuneScape (2001)*, for real money on eBay or other trading websites. The rules of most online multiplayer computer games, including those of *RuneScape (2001)*, do not allow the selling of virtual items for real money, however. Since 2007 ebay has also prohibited the sale of virtual items, except for *Second Life* virtual items (http://www.ebay.com/gds/Buying-and-Selling-Virtual-Items-on-eBay-/10000000004609906/g.html).

pain is taken to include all unpleasant experience (Moore 2004, introduction). Thus, hedonism argues that the constituents of (dis)value are (un)pleasant sensations, feelings, and emotions (Mooradian 2006, p. 688).

There are several hedonist accounts of the level or amount of pleasure's value. Bentham claimed, for instance, that the amount of value varies with pleasure's quantitative features: its duration, intensity or strength (Bentham 1789 as summarized by Moore 2004, § 2). Mill thought that the amount of value varies with pleasure's quality; he thought that there are 'higher' and 'lower' pleasures (Mill 1863 as summarized by Moore 2004, § 2). In sum, hedonism reduces value judgments to judgments about "the qualities of sensations and feelings as well as the probability and frequency of their occurence, among other things" (Mooradian 2008, p. 688).

The virtual entities that are encountered in the virtual worlds of online multiplayer computer games cannot provide for sensory pleasures or pains, however. Therefore, their value cannot be explained in ordinary hedonistic terms. As Søraker points out, it is a special kind of hedonism that can explain the value of virtual entities: "Confidence Adjusted Intrinsic Attitudinal Hedonism (CAIAH)" (Søraker 2010, p. 191). CAIAH assumes that well-being is not enhanced or reduced by sensory pleasures or pains but by attitudinal pleasures or pains. It is not about physical pleasure or pain but about the pleasure or pain one takes in something (e.g., if one enjoys playing a computer game). The more confident one is about the pleasure or pain one takes in something, the more conducive or detrimental it is to well-being (Ibid., p. 191-192).

Media effects studies show that (online multiplayer) computer games elicit real emotions in the non-virtual world (e.g., Järvinen 2009, p. 86). Players take pleasure or pain in gameplay. According to Järvinen the pleasures or pains that are triggered by gameplay are mainly "prospect-based emotions": they are fundamentally related to the goals the game imposes on the players and with which they identify (Ibid., p. 90). A player can, for instance, become frustrated if s/he does not reach the next level of the game (hedonistic disvalue) and happy if s/he does (hedonistic value). The intensity of these emotions depends on the degree to which the player is "immersed" or "engaged" in the game world (Ibid., p. 92).

Not only events but also items in the virtual world of an (online multiplayer) computer game can embody prospect-based emotions. Järvinen states: "a tool that the player can use to her advantage in order to reach the goal (...), represents an object that embodies the solution to the challenge that the goal represents. The object communicates a prospect for the player, and thus, such an instrumental object, and its use, is bound to elicit emotions" (Järvinen 2009, pp. 99-100).

This can be illustrated as follows. In the virtual world of *RuneScape* (2001) players can develop their abilities in a number of skills such as fishing, woodcutting or crafting, at different levels. Some of their talents they can use to create items which they can sell to other players. Other talents they can use to perform tasks. By the performance of tasks players can obtain items and points. The richer a player becomes and the more points and items s/he possesses, the more powerful s/he becomes in the game. So virtual items in the virtual world of *RuneScape* (2001) communicate a prospect for the player: the more of these items s/he possessess, the closer s/he comes to the goal that *RuneScape* (2001) imposes on its players: to become the most powerful player of the game.

Thus, virtual items in the virtual world of an online multiplayer computer game that are purchased by effort can represent hedonistic value in the non-virtual world if they are tools that the player can use to his or her advantage in order to reach the goal of the game. The (amount of) hedonistic value that a virtual item represents in the non-virtual world, differs from player to player and item to item however. As was established earlier, it depends on the degree to which the player is "immersed" or "engaged" in the game world, how intense the emotions are that the gameplay elicits. The more confident a player is about the pleasure s/he takes in the gameplay, the more pleased s/he is if s/he reaches the goal that the computer game imposes on its players and the more hedonistic value a virtual item that can be used for this represents. Of course, the amount of hedonistic value that a virtual item represents also depends on how conducive that particular item is to reaching the goal of the computer game.

In conclusion, virtual items in the virtual world of an online multiplayer computer game can count as a particular player's property in the non-virtual world. They can also represent (pecuniary or hedonistic) value in the non-virtual world. If they do, it makes sense to bring the act of stealing them under the prohibition on theft and to count these virtual items, thereby, as requisite objects of theft (objects that can be stolen).[18]

[18] An anonymous reviewer suggested the following case as a challenge to the view I present here. In the virtual worlds of certain online multiplayer computer games players can own tools that could be considered illegal in the non-virtual world, e.g., weapons or other tools for violence. Should they count as objects that can be stolen? I do not think that the (legal) status of the real, non-virtual equivalent of a virtual item is of importance for the question of whether or not it should count as an object that can be stolen. The real, non-virtual equivalent of a virtual item might be illegal; there also might not be a real, non-virtual equivalent of the virtual item (if it is fictitious, e.g., a magic potion). As long as a virtual item can be considered property worthy of (pecuniary or hedonistic) value in the non-virtual world, it should count as an object that can be stolen.

2.4 Conclusion

In this chapter, I studied the question of whether or not virtual items should count as "objects" that can be "stolen" under criminal law. I took the Dutch convictions for theft of virtual items in the virtual worlds of the online multiplayer computer games *Habbo* (2001) and *RuneScape* (2001) as a starting point (Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791; Gerechtshof Leeuwarden, 10 November 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764; Hoge Raad, 31 January 2012, ECLI: NL: HR: 2012: BQ9251). From an ontological point of view, it can be said that the judges in the *Habbo* and *RuneScape* cases have counted the act of stealing virtual items in the virtual world of an online multiplayer computer game (X) as theft (Y) in the non-virtual world (C) and, thereby, they have admitted that virtual items (X) count as "objects that can be stolen (Y) in the non-virtual world (C). I argued that it also makes sense to count them as such under the following conditions.

An act of stealing in the virtual world of an online multiplayer computer game is to be governed by the rules of the game, unless the magic circle (a metaphorical line between the fantasy realms of computer games and the non-virtual world) is crossed. The metaphorical line of the magic circle is crossed if the act of stealing constitutes such a grave violation of the rules of the online multiplayer computer game that they do not provide an adequate punishment or if the act of stealing is performed outside the setting of the game. In the *Habbo* and *RuneScape* cases the metaphorical line of the magic circle was crossed, because they involved infractions outside the game (i.e., deceit and violence) and were, therefore, (partly) performed outside the setting of the game.

According to the general findings of the first chapter, an act of stealing in the virtual world of an online multiplayer computer game can be brought under the scope of criminal law instead of the rules of the game, if it has an extravirtual consequence (a consequence outside the virtual environment) which is of such a nature that it can legitimate an interference with the liberty of citizens by means of criminal law on the basis of one of Feinberg's liberty-limiting principles. I established that an act of stealing in the virtual world of an online multiplayer computer game has an extravirtual consequence if the object(s) stolen can count as another player's valuable property in the non-virtual world. If so, the act of stealing them can also be brought under Feinberg's first liberty-limiting principle (the harm principle), for it then results in harm, in the sense of a deprivation of wealth and, therefore, of well-being.

Virtual items can be considered a particular player's property in the non-virtual world if they are allocated to this particular player, to the exclusion of others. A virtual item is allocated

to a particular player if some past event of appropriation has established that player as the owner. In the virtual world of *Habbo* (2001) players can, for example, acquire virtual items by means of a payment; in the virtual world of *RuneScape* (2001) players can acquire virtual items by means of effort.

The value that virtual items represent in the non-virtual world is related to the nature of the event of appropriation by which a player has established him- or herself as the owner. If a player really needs to pay in order to purchase a virtual item in the virtual world of an online multiplayer computer game, this virtual item represents pecuniary value in the non-virtual world. If the virtual item is acquired by effort, it can represent hedonistic value in the non-virtual world. The constituents of hedonistic value are pleasant emotions (Mooradian 2006, p. 688). Virtual items can elicit pleasant emotions if they are tools that the player can use to his or her advantage in order to reach the goal of the game. The intensity of the pleasant emotions a virtual item elicits and thus the amount of hedonistic value it represents, depend on the degree to which the player is "immersed" or "engaged" in the virtual world of the online multiplayer computer game. The amount of hedonistic value that a virtual item represents also depends on how conducive the particular item is to reach the goal that the game imposes (Järvinen 2009, pp. 86-100).

In conclusion, it makes sense to count the act of stealing virtual items in the virtual world of an online multiplayer computer game as theft and, thereby, virtual items as "objects" that can be "stolen" if these virtual items can be considered property with (pecuniary or hedonistic) value in the non-virtual world. I am aware that this conclusion raises other questions. For example, how to "measure" the amount of hedonistic value that a particular virtual item represents for a particular player? Answering these questions is beyond the scope of this chapter, however. The issue of theft of virtual items in the virtual worlds of online multiplayer computer games is in need of further discussion and analysis from academics not only in the field of computer ethics, but also in the respective fields of law and psychology.

CHAPTER 3 VIRTUAL RAPE

A slightly different version of this chapter was published as a paper titled "Present and future instances of virtual rape in light of three categories of legal philosophical theories on rape." *Philosophy & Technology*. doi: 10.1007/s13347-014-0167-6.

Introduction

As early as 1993, Julian Dibbell caused a stir by describing what he called a "virtual rape" (Dibbell 1993). In the New York newspaper The Village Voice he reported how a user of a virtual world called *LambdaMOO* (1990) took control over two other users' avatars (their virtual representations) and forced them to have sex with his avatar, and with each other, and to do horrible, brutal things to themselves (Ibid.). Dibbell's story gave rise to a heated debate on the question of whether or not events like the one he described should count as crimes under criminal law. In 2007, fourteen years after Dibbell's story was published, new life was put into this debate when Belgian newspapers announced that the Belgian Federal Police would investigate a "virtual rape" that had occurred in the virtual world of *Second Life* (2003) (Duranske 2007a). The precise facts that led to the police investigation are unknown.

In this chapter, I will study the above-mentioned question whether or not virtual rape should count as a crime under criminal law. Many other authors, merely in the field of computer ethics, have also studied this question. I will provide a broader perspective than they have provided, for I will discuss virtual rape in light of three categories of legal philosophical theories on rape, each defining the crime of rape differently. Moreover, I will, contrary to other authors, not only pay attention to what is possible now but also to what might be possible in the near future with regard to virtual reality technologies.

The structure of this chapter will be as follows. First, I will establish what a virtual rape precisely is. As stated before, I will pay attention to both present and future instances of virtual rape. Then, I will study what conditions (in legal terms: "elements") an act of virtual rape would need to satisfy in order to count as the crime of rape. I will explain that one can take different perspectives resulting in different outcomes here, because there are several legal philosophical theories on the nature of rape, and each theory defines the elements of the crime of rape in accordance with that theory. Subsequently, I will thoroughly discuss the three categories of legal philosophical theories of rape mentioned before and apply them to the case of virtual rape. I will argue that a virtual rape in a future virtual reality environment involving a haptic device or robotics satisfies the elements of the crime of rape as it is viewed under the liberal theories

dominant under current law. It will turn out that this does not mean that virtual rape in a virtual reality environment involving a haptic device or robotics can count as the crime of rape under the current law of each and every country. In some countries, e.g., the UK, it would count as an equivalent of the crime of rape, e.g., assault by penetration (section 2 (1) (a) of the Sexual Offences Act 2003). A surprising finding will be that a virtual rape in a virtual world like the one Dibbell described, re-actualizes the conservative view of rape that used to dominate the law in the Middle Ages and satisfies the elements of the crime of rape as it is viewed under the feminist theories that criticize current law. However, virtual rape in a virtual world does not satisfy the elements of the crime of rape as it is viewed under current law, and at the end of this chapter, I will suggest qualifying it as the crime of sexual harassment instead.

3.1 What is a virtual rape?

In order to answer the question what a virtual rape is, I will first explain what it means for an act of rape to be virtual in nature, then I will define the term "rape". As was briefly mentioned before in section 1.1.4, a virtual rape is a computer-simulated human act, which is an act that is virtual in itself. I argued that when someone performs a computer-simulated act, s/he acts in a virtual environment through an input device (Søraker 2010, p. 147). Such an act generally consists of three steps. First, a human being performs a bodily action on an input device, e.g., s/he presses a button or clicks the mouse. Second, the computer simulation interprets the action as a particular command; in this case, the command is in effect "rape". Third, the computer simulation makes the changes to the virtual environment (and possibly to the non-virtual world as well) that are required by the command; in this case, there will be a victim that is raped (Ibid., p. 137).

What is to be defined as "rape" will be discussed thoroughly in section 3.2, for now, it suffices to describe rape in general terms. In general terms, rape can be described as the act of forcing sex upon an unwilling person (<http://dictionary.findlaw.com/ definition/rape>; <http://legal-dictionary.thefreedictionary.com/rape>). What the computer-simulated human act of forcing sex upon an unwilling person entails precisely depends merely on the virtual environment in which it takes place. As explained in section 1.1.3, it is important to distinguish between virtual worlds, in which users represent themselves by means of a virtual alter ego called an "avatar" and virtual reality environments, in which, as will be explained later, users are immersed themselves. Below, I will first discuss the two examples of virtual rape that were already mentioned briefly in the introduction. They took place in virtual worlds. Then, I will

abstract from these particular cases and establish what features a virtual rape in a virtual world has in general. Last, I will discuss the (future) possibilities for virtual rape that arise in virtual reality environments. No cases of virtual rape in virtual reality environments have been reported yet so the examples will be hypothetical.

3.1.1 Virtual rape in a virtual world

The infamous case of virtual rape that has been described by Dibbell took place in the virtual world of *LambdaMOO* (1990). *LambdaMOO* (1990) is a MUD (Multi-User Dungeon), which is a fantasy world that consists entirely of text. To be more precise, it is a MOO, which stands for MUD, Object-Oriented. Users represent themselves by means of an avatar that consists of a nickname. When a user is logged into *LambdaMOO* (1990), s/he is presented with a textual description of the rooms of which this virtual world consists, the avatars and objects there present, and the things happening.

The night that the virtual rape occurred a user represented by an avatar named "Mr. Bungle" took control over two other users' avatars by means of a "voodoo doll": a subprogram that served the purpose of attributing actions to avatars that their users did not consent to (Dibbell 1993). The first avatar, called "legba", was then made to sexually service Mr. Bungle in a variety of more or less conventional ways and to eat his or her (the gender of this avatar was indeterminate) own pubic hair. The second avatar, called "Starsinger", was made to engage into unwanted liaisons with other users' avatars and to violate herself with a piece of kitchen cutlery. The users who logged into *LambdaMOO* (1990) on the night the virtual rape occurred were presented with a textual description of rape; they were confronted with the unasked-for

LAMBDAMOO

Connected
The Living Room
The Living Room has a warm and inviting decor. It is packed with people. They are chatting.

Starsinger asks you, "How are you?"
say I am fine, how are you?
You say "I am fine, how are you?"
Mr. Bungle takes control over Starsinger by means of a voodoo doll.
As if against her will, Starsinger stabs a steak knife up her ass, causing immense joy.

Figure 3 Impression of the virtual rape Dibbell (1993) describes © Litska Strikwerda 2014

opportunity to read the words "as if against her will, Starsinger stabs a steak knife up her ass, causing immense joy" and similarly constructed sentences (Ibid.).

The precise facts of the virtual rape that led to the Belgian police investigation are unknown but it is known that it took place in *Second Life* (2003), which is a virtual world that offers an augmented version of reality, through which users can navigate and where they can connect, socialize, and create things. Contrary to *LambdaMOO* (1990), *Second Life* (2003) is not a text-based virtual world but an image-based virtual world, consisting of 3D visuals. Users' avatars consist of graphical objects, which usually have a human-like form. Voodoo doll-type subprograms, like the one that was used to accomplish the virtual rape described by Dibbell, exist in *Second Life* (2003) too. They are called "scripts" and allow one user to take control of another user's avatar. Although software controls in *Second Life* (2003) are supposed to require that a user gives permission before another user can take control over his or her avatar, it is possible that one user takes control of another user's avatar against his or her will, particularly if the victim is new to and unfamiliar with *Second Life* (2003). That is because the code that makes scripts work could be built into anything, from a virtual teacup to a virtual tennis bracelet, and, in theory at least, objects with a built-in script could be given to an unsuspecting avatar in order to make a virtual rape possible (Duranske 2007a). But a user could also take control over another user's avatar by means of hacking in order to make a virtual rape possible.[19] In case of a virtual rape in *Second Life* (2003), the user to which the avatar belongs (and other users) would see a graphical depiction of a rape; they would be confronted with images of sexual activities involving the user's avatar against his or her will.

Figure 4 Avatar in Second Life © S@R (Snow Rabbit) 2013 CC by 2.0 (Retrieved from <http://www.flickr.com/photos/snumaw/8581217273>).

When I abstract from these particular cases, I establish that a virtual rape in a virtual world generally has the following features. First of all, a user of a virtual world takes control over another user's avatar by means of a controlling feature such as the "voodoo doll" that was discussed above or hacking. Then, the user makes the other user's avatar appear to engage in sexual activities by giving certain commands through an input device, e.g., by pressing buttons or clicking the mouse. The other user has not consented to make his or her avatar appear in sexual activities and is thus, depending on the virtual world where the avatar resides, unwillingly

[19] It should probably be added that hacking (in the sense of illegal access) already constitutes a crime in itself for which the user could be held liable (see article 2 Convention on Cybercrime; section 1.1.1).

confronted with a textual description or a graphical depiction (virtual worlds are either text- or image-based) of a sexual act involving his or her own avatar. Other users can see the description or depiction as well. A virtual rape in a virtual world thus entails that a user of a virtual world takes control over another user's avatar and, depending on the nature of the virtual world, confronts this user and other users with a textual description or a graphical depiction of a sexual act involving the user's avatar without his or her consent.[20]

3.1.2 Virtual rape in a (future) virtual reality environment

Let us now turn to virtual reality environments. As explained before in section 1.1.3, users do not need to represent themselves by means of avatars in virtual reality environments but they can become immersed in these virtual environments themselves. Virtual reality environments are designed to exploit the sensory systems of human beings so as to produce a sense of presence in those environments (Allen 2010, p. 220). They consist of three-dimensional, interactive, computer-simulated environments with 3-D visuals, and are experienced by users through their own eyes and other senses. This is possible because the users wear goggles or a head-mounted display and a dataglove or datasuit, attached to a computer. As the user navigates through and interacts with the computer-simulated environment, the computer gives large-scale sensory feedback through the dataglove or datasuit (Brey 2008, p. 362). Since virtual reality environments do not offer multi-user access yet; at least not beyond a very limited degree, users mainly interact with objects instead of other users (Søraker 2010, pp. 52, 55). Highly advanced datagloves can, for instance, make the user feel resistance when s/he grabs a computer-simulated object in the computer-simulated environment (Søraker 2010, p. 54).

In 1998, Philip Zhai wrote "a philosophical adventure in virtual reality", a book which was discussed before in section 1.3.5. In this book Zhai claims that virtual reality technology aided by haptic devices will allow people to have sex in a virtual reality environment. He provides the following scenario. Users will wear a standard VR outfit (goggles or head-mounted display and dataglove or datasuit) which is attached to a computer. They will also be provided with an artificial mouth (lips, teeth, tongue, saliva, etc.) and artificial (male or female) genitalia, "both imitating human flesh as closely as possible but planted with microsensors all over the surface, and moved by motors connected to the computer" (Zhai 1998, p. 44). While users actually have sex with these devices, their goggles or head-mounted display will make them see

[20] It is important to emphasize that this definition of virtual rape is only applicable to virtual worlds, which are accessed by multiple users at the same time, and not to single-player computer games like the infamous RapeLay (2006) in which users can rape virtual characters that do not represent other users.

a human being, and because the device closely imitates human flesh, it will feel like they have sex with that human being instead of with a device. To make it feel even more real, the dataglove or datasuit will give users the impression that they can touch the human being they see as well. Users could also have sex with each other in a virtual reality environment. Imagining two people of the opposite sex, Zhai explains that a female user could receive sensory feedback through her device that corresponds with the interactions of a male user with his device and vice versa, provided that their computers, to which their devices are attached, are connected (Ibid., p. 45).

Zhai's scenario is not a remote possibility anymore. Haptic devices like the ones he described already exist. They are commonly called “teledildonics” and consist of sex toys that users can connect to their computers so that other people can control them over the Internet (Lynn 2004, see e.g., <http://www.fleshlight.com>). They generally work as follows. The user has to connect a transmitter to the USB port of his or her computer. This transmitter communicates with a wireless receiver, which is to be connected to a sex toy that consists of a vibrator (for women) or a sleeve-style vibrator (for men). Then, the user has to subscribe to a website so that other users can operate the sex toy via a control panel on that website. One user’s sex toy can also be used as a transmitter for another user’s sex toy so that it can give sensory feedback which corresponds with that other user’s interactions with his or her own sex toy (Lynn 2004).

In the near future, robotics might provide for experiences that are even more sophisticated than Zhai imagined when they could replace the haptic devices in his scenario. A US company has developed a female sex robot called “Roxxxy.” A male version of Roxxxy, called “Rocky”, is in the works. Roxxxy has a flesh-like synthetic skin that covers her anatomically correct skeleton. She has the same temperature as a human being, for she has a mechanical heart that pumps warm liquid through her body. Roxxxy is able to make certain movements, and sensors enable her to “sense” when she is touched and “listen” when someone talks to her. She can also respond to both touch and speech. Roxxxy has cables running out of her back so that users can attach her to a computer. Users can download one of Roxxxy's five pre-existing personalities from the Internet and program it into her. They can also add particular likes and dislikes (Dillow 2010). The same will be true for Rocky when he is fully developed. Probably, it will soon also be possible for a person other than the user to control Roxxxy or Rocky over the Internet like it is possible for a person to control another person's haptic device over the Internet, as explained above. If Roxxxy could, just like the haptic device for men described above, function as a transmitter, a female user interacting with Rocky could receive the sensory feedback that corresponds with the interactions of a male user with Roxxxy,

provided that both robots are connected to a computer and the Internet. This would also work vice versa.[21]

A user could commit a virtual rape in a virtual reality environment involving a haptic device or robotics. Where in the case of a virtual rape in a virtual world, one user takes control over another user's avatar in order to make his or her avatar appear to engage in sexual activities the user did not consent to, in this case, one user would have to take control over another user's haptic device or robot so that s/he can give that user sexually laden sensory feedback to which s/he did not consent. There are several possibilities here. First of all, a user can have sexual intercourse with a device/robot which is attached to a computer and communicates over the Internet with the device/robot of another user who does not consent to have sex with that user but was forced, e.g., by means of (the threat of) violence, to attach the device/robot to his or her computer and to have sexual intercourse with it. It might also be that the user initially attached the device/robot to the computer voluntarily and consented to have sex with the other user, then changes his or her mind and wants to quit but is forced to continue by the other user. Secondly, it can be that two users have consensual sex with each other through their devices/robots but that a third person takes control over the computer of one of the users and makes one or both of their devices/robots give different sensory feedback than it receives from the other user so that the user(s) get sensory feedback they did not consent to. Last, it can be that a user has sex with a device/robot which is attached to the computer and that another person starts operating the device/robot over the Internet without that user consenting to that.

3.2 Can virtual rape count as a crime?

In section 1.2.2 I argued that penal provisions formulate the conditions that an act needs to satisfy in order to count as a crime. In legal terms, these conditions are called elements. The specific elements required vary depending on the crime but there are two basic elements that are required by each crime: an *actus reus* (an unlawful act or failure to act) and a *mens rea* (a blameworthy mental state; usually such that the actor acts knowingly, purposely or recklessly). In fact, all crimes also require, implicitly or explicitly, that the actus reus must have a certain consequence, e.g., the death or injury of a person or a loss of property. This common element is called *causation*.

[21] Roxxxy and Rocky would make the wearing of the goggles and dataglove or datasuit from Zhai's scenario superfluous, for they are not needed to give users the impression that they can see and touch the person they have sex with, users can touch their robots and they will look and feel the same as a real human being.

I further argued that a computer-simulated human act, like a virtual rape, can satisfy the elements of a crime *intravirtually* (i.e., within the virtual environment where it is performed) or *extravirtually* (i.e., outside that virtual environment, in the non-virtual world). The element of actus reus is necessarily satisfied intravirtually, because a virtual rape is performed within a virtual environment through an input device (see section 3.1). The element of mens rea can only be satisfied extravirtually. That is because the element of mens rea concerns the mental state of the human actor, who is necessarily extravirtual. This does not mean that the mental state of the actor is to be judged entirely independently from the virtual environment within which the act has taken place, for circumstances in the virtual environment can indicate whether s/he has acted knowingly, willingly or purposely. The element of causation can be satisfied either intravirtually or extravirtually. The element of causation is satisfied intravirtually when the actus reus has the effect required by the penal provision within the virtual environment and extravirtually when it has that effect outside the virtual environment. A virtual rape can only count as a crime if it satisfies the element of causation of that crime extravirtually.

Yet the question arises whether or not virtual rape satisfies the elements of the crime of rape and, in particular, the element of causation extravirtually. Here, one can take different perspectives resulting in different outcomes, because there are several legal philosophical theories on the nature of rape and each theory defines the elements of the crime of rape in accordance with that theory (Burgess-Jackson 1996, pp. 30-34). The aforementioned theories on the nature of rape will be discussed in the next section. In the subsequent section, they will be applied to the case of virtual rape.

3.2.1 Three categories of legal philosophical theories on rape

Legal philosophical theories on the nature of rape can roughly be divided into three categories: namely, conservative, liberal, and feminist theories (Burgess-Jackson 1996, p. 43). In a nutshell, they all agree that rape should be prohibited, because it causes harm. This means that they assume that the prohibition of rape is grounded in the harm principle, as was discussed in the sections 1.2.4 and 1.3.1. As stated in the first-mentioned section, harm has been defined by Feinberg as a wrongful setback to a welfare interest (Feinberg 1984, pp. 33-34). The aforementioned three legal philosophical theories on the nature of rape disagree about which welfare interest is set back by rape and why rape is wrong, however (Burgess-Jackson 1996, p. 36). It is for this reason that their interpretations of the elements of the crime of rape differ, and therefore, they have different opinions on what counts as a rape. Below, I will discuss how the

aforementioned categories of theories on the nature of rape view rape, which interest they claim to be set back by rape and what makes rape wrong according to them. Later I will explain how their interpretation of the elements of the crime of rape is influenced by these views.

The first category, conservative theories, views rape as a kind of trespass to property. In this view, women belong to and acquire social status in virtue of their relationships to men, e.g., their husband, father or brother (Burgess-Jackson 1996, p. 44; McGlynn & Munro 2010, p. 1). These men, individually or collectively, have an interest in women's reproductive capacities and hence in their sexuality. Rape is a setback to this interest. It constitutes a "contamination" of a man's property as well as a possible ruination of the bloodline (Burgess-Jackson 1996, pp. 44-49). In case the woman is not yet married, rape also causes an economic loss, for it decreases the woman's value on the marriage market (Ibid., p. 68). But rape does not only set back the interest of one or more particular men, it also sets back the interest of society as a whole in having strong patriarchal marriages and families. What makes rape wrong in the conservative view is not that the woman did not consent to the intercourse but that the man to whom the woman belongs did not consent to the intercourse. According to Burgess-Jackson, this explains why, in this view, a man cannot rape his own wife (Ibid., pp. 44-49). Conservative theories constituted the dominant view under law in the Middle Ages. Remains of these conservative theories can still be discovered in current law, however. In South Africa, for example, perceptions of ownership of female sexuality by men continue to be pervasive (Mills 2010, p. 252). Moreover, most Western countries did not abolish the aforementioned marital-rape exemption until the 1980s and 1990s, and it is still applicable in many non-Western countries (see e.g., Gotell 2010, p. 210; Radačić & Turković 2010, pp. 170-171). It should be added, however, that (early) modern marital-rape exemptions, although they might originate from the idea of women as property, are or were based on the idea that a man's wife has given a general consent to intercourse at the time of marriage (see the historical work of Sir Matthew Hale 1847 [1736]).

The second category, liberal theories, currently constitutes the dominant view under law. Liberal theories developed; at least in part, in opposition to conservative theories. They view rape as a form of battery, which is understood as the unlawful touching of another *person* without his or her consent (Burgess-Jackson 1996, p. 49). Unlike conservative theories liberal theories do thus not focus specifically on women (see e.g., Radačić & Turković 2010, p. 171; Rush 2010, p. 239). In the liberal view, every person has an interest in, and a corresponding right to, bodily integrity, which is based upon the moral value of autonomy or self-determination. Rape constitutes a setback to the interest of bodily integrity and the corresponding value of (sexual) autonomy (Burgess-Jackson 1996, pp. 49-50; Cowan 2010, p. 160; McGlynn & Munro

2010, p. 4). What makes rape wrong in the liberal view is that the person him- or herself has not consented to the intercourse (Burgess-Jackson 1996, p. 50).

The third category, feminist theories, criticizes the liberal theories dominant under current law. Supporters of feminist theories claim that almost all rapists are men and almost all rape victims are women and, therefore, they believe that liberals are wrong in defining rape in gender-neutral terms (Burgess-Jackson 1996, p. 53). Although there is a greater feminist consensus with regard to rape than with regard to other areas of concern to feminists such as prostitution or pornography, there have always been distinctive feminist approaches to conceptualizing rape and its wrong, however (McGlynn & Munro 2010, p. 3). There are two main perspectives: liberal feminism and radical feminism (Whisnant 2009). They will be discussed below.

Liberal feminists focus on the harm that rape does to individual women. They do not only take into account the physical aspects of rape but also pay attention to the emotional and psychological consequences (Whisnant 2009). Liberal feminists view rape as degradation (Burgess-Jackson 1996, p. 53). They believe that rape does not (only) constitute a setback to bodily integrity and sexual autonomy but (also) to the broader interest of personal dignity. According to Munro, the decision of the International Criminal Tribunal for Rwanda in the *Akayesu* case (ICTR-96-4-T, 2 September 1998) reflects this view (Munro 2010, p. 17). What makes rape wrong in the liberal feminist view is not only that the woman has not consented to the intercourse but also that the perpetrator dehumanizes, devalues, and disrespects her (Herring & Dempsey 2010, p. 37).

Radical feminists focus on the harm that rape does to women as a group (Whisnant 2009). They believe that rape does not only degrade individual women but that it also, and more importantly, degrades women as a class. Rape harms because it is an instance of class-based subordination especially aimed at women and, therefore, sets back their interest in social equality. What makes rape wrong in this view is that it subjugates a class of persons solely on the basis of their class membership, which is not chosen by them. In other words, what makes rape wrong is that the rapist harms a woman, because she is a woman (Burgess-Jackson 1996, pp. 53-58).

3.2.2 The elements of the crime of rape as interpreted by these theories

As was indicated in section 3.1, the actus reus of rape can in general terms be described as the forcing of sex upon an unwilling person. None of the theories on the nature of rape discussed above would deny this general meaning of rape but they apply different interpretations of the

terms "sex", "unwilling", and "force". Conservative theories assume that sex, as part of the definition of rape, involves penile penetration of a vagina (Burgess-Jackson 1996, p. 46; Cowan 2010, p. 155; Burman 2010, p. 197). That is because they view rape as trespass, which is *entry* onto another's property, and penile penetration of the vagina of a woman who belongs to another man satisfies that requirement (Burgess-Jackson 1996, p. 46). In New Zealand, for example, the current prohibition on rape still requires penile penetration of (female) genitalia (section 128 (2) of the Crimes Act 1961 No 43).

Under the influence of liberal theories on the nature of rape, most other countries have broadened their notion of sex as part of their legal definition of rape. In the UK, for instance, the current prohibition on rape includes penile penetration of other body parts than (female) genitalia in the definition of rape (section 1 (a) of the Sexual Offences Act 2003). In many other countries, current prohibitions on rape also include other forms of penetration than penile penetration such as penetration by an object, in the definition of rape. Consider, for example, the prohibitions on rape of the following countries: the Netherlands (section 242 Wetboek van Strafrecht), Belgium (section 375 Strafwetboek), Germany (section 177 (2) (1) Strafgesetzbuch), Norway (section 192 General Civil Penal Code); South Africa (Chapter 2, part 1, section 3 Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007), and Israel (section 345 (c) Penal Law 5737-1977).

Feminist theories of rape broaden the notion of sex, as part of the definition of rape, even further, for they do not necessitate any physical contact (MacKinnon 1997, p. 3). That is because they view rape as degradation, which does not necessarily do physical harm: the focus is more on emotional and psychological or societal harm. Feminist theories of rape have not resulted in a reinterpretation of the crime of rape under current law but as will be explained in section 3.4, they have led to the recognition of another crime: namely, sexual harassment, in addition to rape.

There is a fundamental difference between the interpretation of unwillingness by conservative theories on the one hand and by liberal and feminist theories on the other hand. In the conservative view, it is the man who "owns" the woman who is unwilling; whether or not the woman is also unwilling is redundant, because she is presumed to have all and only the interests of her father, brother or sovereign (Burgess-Jackson 1996, p. 45). In the liberal and feminist view, it is the person / woman who is raped him- or herself who is unwilling.[22]

The same dichotomy is seen with regard to the interpretation of force. In conservative theories on the nature of rape, force is limited to physical force or threats of death or bodily injury (Burgess-Jackson 1996, pp. 92-93; see also Radačić & Turković 2010, p. 170). Liberal

[22] It should be added that sexual intercourse with a person who is, under law, incapable of consenting to sex, i.e., minors and physically and/or mentally incapacitated persons, is usually considered rape in itself (statutory rape).

and feminist theories on the nature of rape apply a broader concept of force, for they do not limit threats to threats of death or bodily injury but for instance also include threats of economic harm, and some of them add that force cannot only consist of threats but also of coercive offers. In order to explain what a coercive offer is, it is first of all important to point out that force, as part of rape, is closely related to the unwillingness of the victim. Force undermines the willingness of the victim: it is what makes him or her participate in sexual intercourse with the perpetrator while s/he is actually unwilling to do so. A coercive offer does precisely the same. It has the following features: the coercer imposes a choice on the coerced that s/he may and must choose one out of two options, the least unattractive of the two options being what the coercer wants the coerced to choose (Burgess-Jackson 1996, pp. 95-98). Think, for example, of a man who tells a woman who is starving to death in a war situation that if she has sexual intercourse with him, he will give her food but if she does not submit to his advances, she will not get anything.

It should be added that theories on the nature of rape do not only interpret aspects of the actus reus of rape differently, they also differ in which aspects they emphasize. Conservative theories expect that a female rape victim resists the unwanted sexual intercourse with utmost vigor. The emphasis is thus on the forceful actions of the perpetrator rather than on the unwillingness of the victim. Under liberal theories, the emphasis has shifted from the aspect of force to the aspect of unwillingness. While some jurisdictions, e.g., Scotland and certain US states, retreated from narrow force-based accounts relatively recently, in many other jurisdictions, e.g., England and Wales, the law has since long converted to a response to rape that is grounded mainly in the unwillingness of the victim (Munro 2010, p. 19). Some feminists shift the emphasis back to the aspect of force. Others continue to emphasize the aspect of unwillingness (Whisnant 2009; Munro 2010, pp. 19-22).

Now that I have established how the different theories on the nature of rape define the actus reus of rape, I will turn to the element of mens rea. As explained in the last section, the element of mens rea requires that the alleged perpetrator had a blameworthy mental state at the time the crime occurred. Usually, it is required that s/he acted knowingly, purposely or recklessly. The requirement of a mens rea comes from liberalism; at the time of conservative theories, it did not yet exist. Liberal theories have designed the element of mens rea to insure that only individuals who are both deterrable and deserving of punishment are subject to criminal law (Burgess-Jackson 1996, p. 51). In the case of rape, the element of mens rea requires that the alleged perpetrator knowingly, purposely, or recklessly forced sex upon an unwilling person. If s/he reasonably believed that the person consented to the sexual intercourse, then s/he is excused (Ibid. p. 146; McGlynn 2010, p. 141; Cowan 2010, p. 156; Rush 2010, pp. 245-246). The

reasonable-belief defense plays a key role in many rape cases being closed without prosecution (Burman 2010, p. 201; Radačić & Turković 2010, p. 174). Feminist theories criticize the reasonable-belief defense. They claim that rape should be deemed to have occurred not when the perpetrator understands the act as a rape but when the victim or women in general would understand it as rape (Burgess-Jackson 1996, p. 146; McGlynn 2010, p. 141).

Finally, I will discuss the element of causation. In the last section, it was explained that the element of causation requires that the actus reus has a certain consequence. Which consequences are required by the three categories of theories on the nature of rape was already indicated above, when I discussed which interest is set back by rape according to these theories but I will briefly repeat them here. The conservative theories claim that rape causes a "contamination" of a man's property as well as a possible ruination of his bloodline. In case the woman who is raped is not yet married, the rape causes an economic loss as well, for it decreases the woman's value on the marriage market. And from a societal point of view, rape also weakens the strong patriarchal marriages and families that society is built upon (Burgess-Jackson 1996, pp. 44-49, 68). For liberal theorists, rape causes an injury to a person's bodily integrity (Ibid., pp. 49-50; Cowan 2010, p. 160; McGlynn & Munro 2010, p. 4). And according to feminist theorists, rape causes either degradation of the individual woman who is raped, resulting in an injury to personal dignity, or degradation of women as a class, which results in social inequality of women in general (Burgess-Jackson 1996, p. 53-58; Munro 2010, p. 17; Herring & Dempsey 2010, p. 37; Whisnant 2009).

3.3 Virtual rape in light of the three categories of legal philosophical theories on rape

In this section, I will examine whether or not virtual rape can be considered rape under the three categories of theories on the nature of rape that were discussed in the last section. I will establish whether or not a virtual rape can satisfy the specific elements of the crime of rape (actus reus, mens rea, and causation) as they interpret them. Remember that in section 3.1, I made a distinction between virtual rape in a virtual world and virtual rape in a virtual reality environment. I will start this discussion with virtual rape in a virtual world and later discuss virtual rape in a virtual reality environment.

Virtual rape in a virtual world re-actualizes the conservative, medieval view of rape as a kind of trespass to property. After all, a virtual rape is committed by one user against another user but it is not the user him- or herself who is raped but his or her avatar. The way conservative

theories interpret the term, sex (as part of the actus reus of rape) necessarily involves penetration, though not of the male victim of the rape but of the woman he owns (Burgess-Jackson 1996, p. 46; Cowan 2010, p. 155; Burman 2010, p. 197). Virtual rape in a virtual world may involve (intravirtual) penetration of the user's avatar (i.e., penetration of the avatar within the virtual environment where the avatar resides). In the conservative interpretation of the term "unwilling", as part of the actus reus of rape, it is the male victim of rape who is unwilling, and because he is unwilling, the woman he owns is presumed to be unwilling too (Burgess-Jackson 1996, p. 45). This interpretation of unwillingness is applicable to virtual rape in a virtual world as well, for here, it is the user who is unwilling and because s/he is unwilling the avatar, which is his or her virtual representation, is presumed to be unwilling too. The conservative interpretation of the term "force", as part of the actus reus of rape, is limited to physical force or threats of death or bodily injury (Ibid., pp. 92-93; see also Radačić & Turković 2010, p. 170). Virtual rape in a virtual world may involve (intravirtual) violence or the threat thereof but that is not how sex is forced upon the user's avatar. As explained in the first section, a user is able to force sex upon another user's avatar when s/he has taken control over that avatar by means of a controlling feature or hacking. It is self-evident that the use of a controlling feature does not normally involve physical violence or the threat thereof.

The element of mens rea is not part of conservative theories, so I will continue with the element of causation. I repeat that conservative theories claim that rape causes a "contamination" of a man's property, a possible ruination of his bloodline and, in case the woman who is raped is not yet married, also an economic loss, for it decreases her value on the marriage market. From a societal point of view, rape weakens the strong patriarchal marriages and families that society is built upon as well. A virtual rape in a virtual world cannot have any of the aforementioned consequences; at least not extravirtually. That is because the relation of ownership between a man and his woman / women and a user and his or her avatar differs. An avatar does not relate to the user who owns it as a relative or a spouse: it is a representation of the user him- or herself. Nevertheless, a virtual rape in a virtual world can have (extravirtual) consequences that resemble a contamination of a man's property or a decrease of value on the marriage market. The user him- or herself or other users might continue to associate the avatar with the rape, which may ultimately lead to the user not wanting to represent him- or herself by that avatar anymore. It might also be that the user uses his or her avatar to trade in the virtual world and, thereby, earns real money. When the avatar is raped and hence other users are confronted with a description or depiction of the avatar having (some sort of controversial) sex, other users might not want to trade with the avatar anymore, which results in an economic loss for the user.

Because liberal theories view rape as battery, i.e., the unlawful touching of another person, they assume that sex, as part of the actus reus of rape, involves some form of harmful or offensive bodily contact (Burgess-Jackson 1996, p. 49). In the case of virtual rape in a virtual world there may be (intravirtual) harmful or offensive contact between two persons' avatars. The liberal interpretation of unwillingness, as part of the actus reus of rape, gives rise to a problem. Liberal theories claim that it is the person who is raped who must be unwilling (Ibid.). In the case of virtual rape in a virtual world, it is the user who is unwilling but his or her avatar who is raped. This problem can easily be solved, however, if we accept that the user and the avatar speak with the same voice, because the avatar is the user's virtual representation. Liberal theories assume that force is what makes the victim participate in sexual intercourse with the perpetrator while s/he is actually unwilling to do so (Ibid., pp. 95-98). As was described above, a user of a virtual world is able to "force" sex upon another user's avatar when s/he has taken control over that avatar by means of a controlling feature or hacking. This would fall under the definition of force in the broad, liberal interpretation. As mentioned in the first section, a user of the virtual world of *Second Life* (2003) can take control over another, unsuspecting user's avatar by giving that avatar a present with a built-in controlling feature. This bears resemblance to a coercive offer, because the receiver of the present has the choice to either accept or decline the gift but in this case, the "coercer" does not exploit the vulnerability of the "coerced" in a certain situation but his or her ignorance.

The element of mens rea, as interpreted by liberal theories, poses particular challenges in virtual worlds. It requires that a person accused of rape be excused if s/he reasonably believed that the victim consented to the sexual intercourse (Burgess-Jackson 1996, p. 146; McGlynn 2010, p. 141; Cowan 2010, p. 156; Rush 2010, pp. 245-246). This reasonable-belief defense might, for example, be applicable to the above-mentioned example where a user of *Second Life* (2003) gives the avatar of another user a present with a built-in script, provided that s/he thought the other user knew about the script and its applications. It is very difficult to verify, however, whether or not the one user reasonably thought that the other user knew about the script and its implications, since the users only have contact with each other through their avatars and, therefore, lack things like body language signs. The element of causation, as liberal theories interpret it, is problematic in the context of virtual rape in a virtual world as well. I repeat that liberal theories claim that rape causes an injury to a person's bodily integrity (Burgess-Jackson 1996, pp. 49-50; Cowan 2010, p. 160; McGlynn & Munro 2010, p. 4). Since virtual rape in a virtual world does not involve physical contact between persons, it cannot cause an (extravirtual) injury to a person's bodily integrity.

Feminist theories apply a very broad notion of sex as part of the actus reus of rape, for it does not even necessitate physical contact (MacKinnon 1997, p. 3). Virtual rape in a virtual world involves (intravirtual) sex, which can be included in this broad notion of sex. The feminist interpretation of both unwillingness and force, as part of the actus reus of rape, is similar to the liberal interpretation and, therefore, the same arguments apply. The element of mens rea, as interpreted by feminist theories, entails that rape is deemed to have occurred not when the perpetrator understands the act as a rape but when the victim or women in general would understand it as a rape (Burgess-Jackson 1996, p. 146; McGlynn 2010, p. 141). A virtual rape in a virtual world can thus be considered a rape when the user of the avatar that is raped understands what happened as rape or when women in general would do so.

Virtual rape in a virtual world can also satisfy the element of causation as interpreted by feminist theories. They affirm that rape causes degradation of the individual woman who is raped, which results in an injury to personal dignity, or of women as a class, which results in social inequality of women (Burgess-Jackson 1996, p. 53-58; Munro 2010, p. 17; Herring & Dempsey 2010, p. 37; Whisnant 2009). In the case of a virtual rape in a virtual world, the individual user whose avatar is raped might feel degraded and violated in her personal dignity. Moreover, research suggests that degrading portrayals of women in computer games negatively influence people's attitudes and behaviors towards and their feelings about women in real life (Burgess, Stermer & Burgess 2007, p. 428). Based on these findings, one can also argue that a virtual rape of a user's female avatar in a virtual world, which is also visible for other users, might lead to degradation of women as a class resulting in social inequality of women, provided that the rape is depicted or described in a degrading way.

In sum, virtual rape in a virtual world can be considered rape under feminist theories. Virtual rape in a virtual world also satisfies many but not all of the elements of the crime of rape as interpreted by conservative theories. Virtual rape in a virtual world cannot be considered rape under liberal theories, because it does not constitute an (extravirtual) injury to a person's bodily integrity.

It is precisely here, where the main difference lies between virtual rape in a virtual world and virtual rape in a virtual reality environment involving a haptic device or robot. Although it is mediated by a device/robot, virtual rape in a virtual reality environment does involve physical contact with another person. Therefore, virtual rape in a virtual reality environment can, contrary to virtual rape in a virtual world, cause (extravirtual) injury to a person's bodily integrity. The dichotomy between the unwillingness of the avatar and the unwillingness of the user does not hold for virtual rape in a virtual reality environment either, for we only have to take into account

the unwillingness of the user who, although mediated by a device/robot, directly interacts with another user. Therefore, virtual rape in a virtual reality environment can, contrary to virtual rape in a virtual world, satisfy all the elements of the crime of rape as interpreted by liberal theories.

This does not mean that virtual rape in a virtual reality environment involving a haptic device or robotics can count as the crime of rape under the current law of each and every country. As explained in section 3.2.2, New Zealand, for instance, still applies a conservative definition of rape, for the current New Zealand prohibition on rape requires penile penetration of (female) genitalia (section 128 (2) of the Crimes Act 1961 No 43). And in the UK, for example, the current prohibition on rape does include penetration of other body parts than (female) genitalia in the definition of rape but still requires penetration by a penis (section 1 (a) of the Sexual Offences Act 2003). Penetration by means of a haptic device or sex robot would thus not count as rape in these countries. It would count as a similar crime, however. In New Zealand virtual rape in a virtual reality environment involving a haptic device or robotics can be considered an "unlawful sexual connection" (section 128 (3) of the Crimes Act 1961 No 43) and in the UK it can be brought under the scope of the prohibition on assault by penetration (section 2 (1) (a) of the Sexual Offences Act 2003).

In many other countries, virtual rape in a virtual reality environment involving a haptic device or robotics can count as the crime of rape. That is because their prohibitions on rape include other forms of penetration than penile penetration such as penetration by an object, in the definition of rape. Consider, for example, the prohibitions on rape of the following countries: the Netherlands (section 242 Wetboek van Strafrecht), Belgium (section 375 Strafwetboek), Germany (section 177 (2) (1) Strafgesetzbuch), Norway (section 192 General Civil Penal Code); South Africa (Chapter 2, part 1, section 3 Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007), and Israel (section 345 (c) Penal Law 5737-1977).

I will not apply the other theories on the nature of rape to virtual rape in a virtual reality environment involving a haptic device or robotics, for it suffices for the purposes of this chapter to establish that it can be considered rape under liberal theories which currently dominate the law and can in fact count as the crime of rape in many countries. Virtual rape in a virtual world cannot count as the crime of rape under the liberal theories but, as will be explained in the next section, that does not mean that virtual rape in a virtual world cannot count as a crime under current criminal law at all.

3.4 Virtual rape in a virtual world as sexual harassment

As was discussed before in section 1.2.2, a computer-simulated act can sometimes satisfy the actus reus element and the attendant element of causation of one crime intravirtually and, thereby, satisfy the actus reus element and the attendant element of causation of another crime extravirtually. Such an act thus counts as crime Y within its virtual environment and as crime Z in the non-virtual world. In this section, I wish to argue that virtual rape in a virtual world counts as the crime of rape (Y) within its virtual environment but as the crime of sexual harassment (Z) in the non-virtual world.

Both Dibbell and Brenner suggest including the conduct that constitutes virtual rape in a virtual world into the definition of sexual harassment (Dibbell 1993; Brenner 2008, p. 79). I agree with this argumentation, because sexual harassment bears resemblance to how feminist theorists view rape and, therefore, many of the arguments that were used to advocate that virtual rape in a virtual world constitutes a rape in the feminist view on the nature of rape, can also be used to advocate that it constitutes sexual harassment. This is not a coincidence. The feminist critique on the liberal theories on the nature of rape that are most influential current law has not resulted in a reinterpretation of the crime of rape but it has led to the recognition of sexual harassment as a crime in addition to rape in the late 1970s (Franke 1996-1997, p. 698; Davidson 1991, p. 39).

How the actus reus of sexual harassment is defined precisely differs from country to country but a general definition can be found in UN General Recommendation No. 19 to the Convention on the Elimination of all Forms of Discrimination Against Women, which has been ratified by 187 countries worldwide. According to the aforementioned recommendation sexual harassment consists of "such unwelcome sexually determined behavior as physical contact and advances, sexually colored remarks, showing pornography, and sexual demands, whether by words or actions" (UN General Recommendation No. 19 to the Convention on the Elimination of all Forms of Discrimination Against Women, § 18). Virtual rape in a virtual world can be brought under the scope of the actus reus of sexual harassment, for it entails, among other things, that a user is unwillingly confronted with a textual description or a graphical depiction of a sexual act involving his or her own avatar without his or her consent, which can be seen as the unwelcome sexually determined behavior of showing pornography, provided that one includes virtual pornography in the definition of pornography.[23]

[23] It should be added that virtual rape involving avatars that appear to be minors can be seen as virtual child pornography. Virtual child pornography raises issues of its own, which will be discussed in chapter 4.

Virtual rape in a virtual world can also satisfy the mens rea element of sexual harassment. It was explained in the third section that feminist theorists claim with regard to the mens rea element of rape that rape should be deemed to have occurred not when the perpetrator understands the act as a rape but when the victim or women in general would understand it as rape. The same line of reasoning applies to sexual harassment (Franke 1996-1997, p. 745-746). A virtual rape in a virtual world can thus be considered sexual harassment when the user of the avatar that is raped understands what happened as sexual harassment or when users in general would do so.

The element of causation of sexual harassment is also similar to the element of causation of rape as interpreted by feminist theories. Both sexual harassment and rape as interpreted by feminist theorists focus on emotional and societal rather than physical harm. According to the above-mentioned recommendation sexual harassment "can be humiliating and may constitute a health and safety problem: it is discriminatory when the woman has reasonable grounds to believe that her objection would disadvantage her in connection with her employment, including recruitment or promotion, or when it creates a hostile working environment" (UN General Recommendation No. 19 to the Convention on the Elimination of all Forms of Discrimination Against Women, § 18). Contrary to rape as interpreted by feminist theorists, sexual harassment is thus only considered to be discriminatory when it occurs in the workplace; at least according to the aforementioned definition.

Virtual rape in a virtual world does not typically take place in a working environment and can, therefore, not be considered discriminatory under this definition of sexual harassment but, as explained in the last section, virtual rape in a virtual world can be humiliating (which feminist theorists call degrading with regard to rape) for the individual user represented by the avatar that is raped; it is probably even more humiliating than when one is confronted with pornography involving anonymous figures. Therefore, virtual rape in a virtual world can satisfy the element of causation as well. In conclusion, virtual rape in a virtual world counts as rape within its virtual environment and as sexual harassment in the non-virtual world.

3.5 Conclusion

In this chapter, I studied the question of whether or not a virtual rape should count as a crime under criminal law. First, I established what a virtual rape is. I explained that a virtual rape is a computer-simulated human act, which is an act that is performed in a virtual environment through an input device. I distinguished between two types of virtual rape: virtual rape in a

virtual world and virtual rape in a (future) virtual reality environment which involves a haptic device or robotics.

A virtual rape in a virtual world entails that a user of a virtual world takes control over another user's avatar and, depending on the nature of the virtual world, confronts this user and other users with a textual description or a graphical depiction of a sexual act involving the user's avatar without his or her consent. There are several possibilities for virtual rape in a (future) virtually reality environment which involves a haptic device or robotics. First of all, a user can have sexual intercourse with a device/robot which is attached to a computer and communicates over the Internet with the device/robot of another user who does not consent to have sex with that user but was forced, e.g., by means of (the threat of) violence, to attach the device/robot to his or her computer and to have sexual intercourse with it. It might also be that the user initially attached the device/robot to the computer voluntarily and consented to have sex with the other user, then changes his or her mind and wants to quit but is forced to continue by the other user. Secondly, it can be that two users have consensual sex with each other through their devices/robots but that a third person takes control over the computer of one of the users and makes one or both of their devices/robots give different sensory feedback than it receives from the other user so that the user(s) get sensory feedback they did not consent to. Last, it can be that a user has sex with a device/robot which is attached to the computer and that another person starts operating the device/robot over the Internet without that user consenting to that.

Next, I argued that a computer-simulated human act can count as a crime if it satisfies the conditions (in legal terms: elements) of a crime and, in particular, the element of causation extravirtually. The element of causation is satisfied extravirtually when the computer-simulated human act has an effect as required by the applicable penal provision outside the virtual environment, in the non-virtual world. When we want to answer the question of whether or not a virtual rape can count as the crime of rape we can take different perspectives resulting in different outcomes, because there are several legal philosophical theories on the nature of rape. These theories agree that rape should be prohibited on the (moral) ground that it causes harm, which can be defined as a wrongful setback to interest but they disagree about which interest is set back by rape and why rape is wrong. It is for this reason that their interpretations of the elements of the crime of rape differ and, therefore, they have different opinions on what counts as a rape.

I discussed three categories of legal philosophical theories on the nature of rape: conservative, liberal, and feminist theories. Subsequently, I studied virtual rape in light of these theories. I came to the conclusion that virtual rape in a virtual reality environment involving a

haptic device or robotics satisfies the elements of the crime of rape as they are interpreted by liberal theories on the nature of rape which currently dominate the law and, in particular, the element of causation extravirtually. This does not mean that virtual rape in a virtual reality environment involving a haptic device or robotics can count as the crime of rape under the current law of each and every country, as the prohibitions on rape of some countries (e.g., New Zealand and the UK) still apply a conservative definition of rape, which requires penile penetration. In many other countries (e.g., the Netherlands, Belgium, Germany, Norway, South Africa, and Israel) virtual rape in a virtual reality environment involving a haptic device or robotics can count as the crime of rape, for their prohibitions on rape include in the definition of rape other forms of penetration than penile penetration such as penetration by an object. In New Zealand and in the UK virtual rape in a virtual reality environment involving a haptic device or robotics can count as a similar crime (respectively: unlawful sexual connection and assault by penetration).

Virtual rape in a virtual world does not satisfy (all of) the elements of the crime of rape as they are interpreted by liberal theories but it does satisfy the elements of the crime of rape as they are interpreted by feminist theories on the nature of rape which criticize liberal theories and, in particular, the element of causation extravirtually. Virtual rape in a virtual world also re-actualizes the conservative view on the nature of rape, which used to dominate the law in the Middle Ages. In conclusion, virtual rape in a virtual world cannot count as the crime of rape under current law, unless the law is changed according to feminist theories.

I argued, however, that such a radical change of the law is not necessary to make virtual rape in a virtual world count as a crime in contemporary society. Sometimes, a computer-simulated human act can satisfy the actus reus element and the attendant element of causation of one crime intravirtually and, thereby, satisfy the actus reus element and the attendant element of causation of another crime extravirtually. Such an act thus counts as crime Y within its virtual environment and as crime Z in the non-virtual world. This seems to be the case with regard to virtual rape in a virtual world. The way feminist theories interpret rape and the harm it causes within society has much in common with the crime of sexual harassment and its harm. Virtual rape in a virtual world can satisfy the elements of the crime of sexual harassment and, in particular, the element of causation extravirtually. Thus, although virtual rape in a virtual world cannot count as rape (Y) in the non-virtual world under current law, it should nevertheless be considered a crime: namely, sexual harassment (Z).

CHAPTER 4 VIRTUAL CHILD PORNOGRAPHY

An earlier version of this chapter was published under the title "Virtual Child Pornography Why Images Do Harm from a Moral Perspective" in Charles Ess & May Thorseth (Eds.), *Trust and Virtual Worlds Contemporary Perspectives* (pp. 139-161). New York: Peter Lang Publishing (2011).

Introduction

There seems to be an international trend that seeks to ban virtual child pornography. This is evidenced by the adoption of an Optional Protocol to the UN Convention on the rights of the child (UN Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography), the EU initiative on combating sexual exploitation of children and child pornography (Directive 2011/92/EU), and the adoption of the Convention on Cybercrime (Council of Europe Convention on Cybercrime). All tend to criminalize the (electronic) possession, distribution, and production of child pornography, including virtual child pornography.

The legitimacy of the prohibition on virtual child pornography is contested, however. It is often claimed that virtual child pornography does, contrary to *non*-virtual child pornography, not result in (extravirtual) harm and can, therefore, not be brought under the scope of the harm principle. This chapter aims to investigate whether or not the aforementioned claim is true. I will conclude it is true for a particular type of virtual child pornographic images: namely, entirely computer-generated child pornographic images, and with regard to those images I will study whether or not one of Feinberg's other liberty-limiting principles can legitimate their prohibition.

The structure of this chapter will be as follows. In the first section, I will define the term "child pornography" and explain that there are actually three categories of child pornography: namely, (a) images (i.e., photos, videotapes, films) showing a child engaged in sexually explicit conduct, (b) images showing an adult appearing to be a child engaged in sexually explicit conduct, and (c) images which, although realistic, do in fact not involve a real child engaged in sexually explicit conduct. The latter category includes images which are altered or even generated entirely by the computer: i.e., virtual child pornography (Council of Europe Convention on Cybercrime, Expl. Report §101). In the second section, I will discuss whether or not the aforementioned categories of child pornography result in harm; I will highlight the question of whether or not entirely computer-generated child pornography results in harm as intended by the harm principle. I will conclude that this is a "victimless crime" (as described by

Bedau 1974) to which the harm principle does not apply. According to Bedau, the criminalization of victimless crimes is based on either legal paternalism or legal moralism. Therefore, the subsequent sections will continue by exploring whether or not the prohibition on entirely computer-generated child pornography can be brought under the scope of legal paternalism or legal moralism. Ultimately drawing from the positions of virtue ethics and feminism, I will argue that these provide a basis through legal moralism to legitimate the prohibition on entirely computer-generated child pornography.

4.1 Child pornography: definitions

The question of what constitutes child pornography is a complex one. Legal definitions of both child and pornography differ globally (Quayle & Taylor 2002, p. 865). In this chapter, I will stick to the definition of child pornography as provided by article 9 (2) of the Convention on Cybercrime. I have chosen to do so, because this definition is widespread, for, as mentioned before in section 1.1.1, the Convention on Cybercrime has been ratified by almost all members of the Council of Europe as well as the USA, Australia and Japan. Although some states have reserved the right not to apply certain aspects of article 9 (2) of the Convention on Cybercrime, the definition of child pornography under their national law will merely correspond to the one that is proposed by the Convention on Cybercrime (for differences see: Council of Europe Convention on Cybercrime, List of declarations, reservations and other communications).

Article 9 (2) of the Convention on Cybercrime defines the term child pornography as pornographic material which visually depicts:

a a minor engaged in sexually explicit conduct;
b a person appearing to be a minor engaged in sexually explicit conduct;
c realistic images representing a minor engaged in sexually explicit conduct.

For the sake of clarification it should be added that article 9 (3) of the Convention on Cybercrime defines the term minor as “all persons under 18 years of age”. The term sexually explicit conduct covers: “a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse in a sexual context; or e) lascivious exhibition of the genitals or the pubic area of a minor. It is not relevant whether the conduct depicted is real or simulated” (Council of Europe Convention on Cybercrime, Expl. Report §100).

In conclusion, article 9 (2) of the Convention on Cybercrime distinguishes three categories of child pornography. The Explanatory Report to the Convention on Cybercrime discusses these categories of child pornography in more detail. It explains that the first category of child pornography (a) consists of images (i.e., photos, videotapes, films) showing a minor engaged in sexually explicit conduct. The second category of child pornography (b) consists of images showing an adult appearing to be a minor engaged in sexually explicit conduct. The third category of child pornography (c) consists either of 'pseudo' images, i.e., images of a minor which are manipulated or morphed to make it appear like the minor is engaged in sexual activities, or of images which are entirely computer-generated (Council of Europe Convention on Cybercrime, Expl. Report §101). Entirely computer-generated child pornographic can be considered virtual child pornography, because the production of such material involves the use of computer simulation and, therefore, they can be brought under the definition of virtual as "made possible by computer simulation" (see section 1.1.3). The same goes for pseudo child pornographic images insofar as they are manipulated or morphed by means of computer technology (e.g., Photoshop).

4.2 Criminalization of child pornography and its moral grounds

Various aspects of the electronic possession, distribution, and production of child pornography as defined in article 9 (2) of the Convention on Cybercrime have been criminalized by article 9 (1) of the Convention. Most of the signatory states to the Convention on Cybercrime had already established the possession, distribution, and production of child pornography as crimes under their domestic law before but when they ratified the Convention they shaped their definition of child pornography after the above-mentioned definition, although, as mentioned before, some states have reserved the right not to apply certain aspects of article 9 (2) of the Convention. The possession, distribution, and production of child pornography, including virtual child pornography, are thus currently seen as crimes in many countries worldwide.

The Convention on Cybercrime's prohibition on the production, distribution, and possession of (all three categories of) child pornography "seeks to strengthen protective measures for children, including their protection against sexual exploitation" (Council of Europe Convention on Cybercrime, Expl. Report §91). This aim can be explained as follows. The criminalization of the first category of child pornography "focuses more directly on the protection against child abuse", while the criminalization of the second and third category aims at "providing protection against behavior that, while not necessarily creating harm to the 'child'

depicted in the material, as there might not be a real child, might be used to encourage or seduce children into participating in such acts, and hence form part of a subculture favoring child abuse" (Ibid., §102). The aforementioned arguments both seem to appeal to the harm principle; although the first more directly than the second. The Convention on Cybercrime thus seems to claim that the criminalization of the possession, distribution, and production of (all three categories of) child pornography is legitimate, because this conduct harms children, either directly or indirectly. The question arises whether or not this claim is correct.

4.2.1 Do all categories of child pornography result in (direct or indirect) harm?

With regard to the first category of child pornography there is consensus that it indeed directly causes harm, which can be defined as a wrongful setback to a (welfare) interest (see section 1.2.4). It is important to note here, that in sex contacts between adults and children mutual consent is in general assumed to be absent and, therefore, they are always considered sexual abuse (Moerings 1999, p. 190). Sexual abuse results in harm, because it constitutes a setback to an interest of personality (i.e., bodily integrity but also mental health). Since the production of images showing a minor engaged in sexually explicit conduct typically involves a sex contact[24] between adults and children, they can be considered recordings of harmful sexual abuse (Boutellier 2000, p. 455). Following this argument, not only the production but also the possession and distribution of child pornographic images can be considered harmful to children. After all, the possession and distribution (i.e., consumption) of child pornography supports the market for it and, therefore, it causes the harmful sexual abuse of children that comes with the production (Moerings 1999, p. 191). Moreover, the child pornographic images themselves are a permanent record of the sexual abuse occurred in the production that could haunt the children concerned when they grow up if discovered by others (Pember & Calvert 2012, p. 498).

As stated in the last section, the Explanatory Report to the Convention on Cybercrime claims that the second category of child pornography harms children indirectly, because it might be used to encourage or seduce children into participating in sex contacts with adults and hence forms part of a subculture favoring child abuse (Council of Europe Convention on Cybercrime, Expl. Report § 102). But I would say that there is (also) another reason to be thought of here. The prohibition on the second category of child pornography can be legitimated on the ground of

[24] The term "sex contact" has to be interpreted broadly here. It can consist of sexual intercourse but also of, for example, the instruction to take a sexually explicit pose.

a pragmatic-oriented interpretation of harm, for it enables authorities to combat online child pornography and the harm it causes to children effectively. If the prohibition on child pornography would not include images showing an adult appearing to be a minor engaged in sexually explicit conduct in its scope, many child pornography cases would be closed without prosecution, because defendants could then raise the contention that the child depicted could in reality be over eighteen years in age, thereby requiring the prosecution to proof that the child depicted is a minor. This would be a strong defense, especially when the child depicted is a (pre-)adolescent. The age of the child depicted in a child pornographic image can only be established with 100% certainty when the identity of that child is known. Given the worldwide range of the Internet, which is the primary instrument for trading child pornography, it is impracticable for authorities to establish the identity of each child depicted in every single child pornographic image found, however.

With regard to the third category of child pornography it is important to draw a distinction between 'pseudo' images (i.e., images of a minor which are manipulated or morphed to make it appear like the minor is engaged in sexual activities) and entirely computer-generated images. As mentioned in the last section, the Explanatory Report to the Convention on Cybercrime claims that pseudo child pornographic images harm children indirectly, because they might be used to encourage or seduce children into participating in such acts and form part of a subculture favoring child abuse (Council of Europe Convention on Cybercrime, Expl. Report § 102). However, I would say they (also) harm children directly, for if one manipulates or morphs an innocent picture of an actual child into child pornography, the child depicted can, although s/he has not been sexually abused, still be haunted by the image when growing up if s/he learns (through others) s/he was exposed that way (Levy 2002, p. 319). Contrary to the harm of sexual abuse, the harm at stake here, does not consist of a wrongful setback to an interest of personality but of a wrongful setback to another welfare interest: namely, the interest in reputation or the interest in privacy of the child whose picture is used (see e.g., the US case *Doe v. Boland* 698 F. 3d 877 6th Cir. 2012).

The question of whether or not entirely computer-generated child pornography results in harm is the most complicated. It cannot be answered briefly. This question will, therefore, be discussed in a separate subsection below.

4.2.2 The specific case of entirely computer-generated child pornography

First of all, it is important to take a look at the legal origin of the prohibition on entirely computer-generated child pornography as contained in article 9 of the Convention on Cybercrime. This prohibition and the arguments that are used to legitimate it largely resemble the prohibition on entirely computer-generated child pornography and its legitimation as they were provided by the 1996 US Child Pornography Prevention Act (CCPA). However, the CCPA was found unconstitutional by the US Supreme Court, partly on the ground that entirely computer-generated child pornography does not harm actual children (*Ashcroft v. Free Speech Coalition*, 535 U.S. 234 2002).[25] The Supreme Court argued that entirely computer-generated child pornography "is not 'intrinsically related' to the sexual abuse of children. While the Government asserts that the images can lead to actual instances of child abuse, the causal link is contingent and indirect. The harm does not necessarily follow from (…) [it] but depends upon some unquantified potential for subsequent criminal acts" (Ibid.).

The argumentation of the Supreme Court here is two-fold. To begin with, the Supreme Court confirms an assumption which was also made in the Explanatory Report to the Convention on Cybercrime as quoted earlier: namely, that the production and related distribution and possession of entirely computer-generated child pornography does not constitute any victims of sexual abuse and, therefore, does not harm any children *directly*. Secondly, the Supreme Court doubts the correctness of the other assumption also made in the Explanatory Report: namely, that entirely computer-generated child pornographic images could lead to actual instances of child abuse, for they might be used to encourage or seduce children into participating in such acts and form part of a subculture favouring child abuse. The Supreme Court, therefore, holds the opinion that entirely computer-generated child pornography does not harm children *indirectly* either.

[25] As a side note it should be added that a year after the Supreme Court struck down the CCPA, the PROTECT (short for Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today) Act 2003 was passed. The PROTECT Act shaped the current US definition of and prohibition on child pornography (respectively: 18 USC § 2256 (8) and 18 USC § 2252A). The aforementioned penal provisions prohibit the production, distribution, and possession of entirely computer-generated child pornography if it is indistinguishable from real and the pandering of entirely computer-generated child pornography if it is offered as if it were real child pornography. It is important to note that the current US prohibition on entirely computer-generated child pornography thus has another scope than the previous one (i.e., it prohibits entirely computer-generated child pornography that is indistinguishable from real instead of realistic, which implies it is still distinguishable from real). The PROTECT Act legitimates this prohibition on the basis of a pragmatic-oriented interpretation of harm, which is similar to the one used in section 4.2.1 to legitimate the prohibition of the second category of child pornography. Since the Supreme Court's decision in the *Ashcroft v. Free Speech Coalition* case, defendants in child pornography cases commonly raised the contention that the images in question could be virtual, thereby requiring the prosecution to proof that the child depicted is real. The aforementioned prohibition means to avoid this grave threat to the enforcement of child pornography laws that protect real children (PROTECT Act, 108th Congress of the USA, 7 January 2003, Sec. 501 (10) and (14)). The PROTECT Act was upheld by the Supreme Court in the case *USA v. Williams*, 553 U.S. 285 (2008).

Since the prohibition on entirely computer-generated child pornography which is at stake in this chapter (i.e., the one contained in article 9 of the Convention on Cybercrime) continues to resemble the US prohibition the *Ashcroft v. Free Speech Coalition* case was about, the argumentation of the US Supreme Court in the aforementioned case still applies. On the basis of this argumentation I would have to conclude that entirely computer-generated child pornography does not result in (direct or indirect) harm. But does the argumentation of the US Supreme Court in the *Ashcroft v. Free Speech Coalition* case, according to the current state of research, still make sense? Below, I aim to answer that question. I will first discuss the first argument, the question whether or not the second argument still makes sense will feature in section 4.3.

The first argument of the Supreme Court in the *Ashcroft v. Free Speech Coalition* case, which confirms the assumption made in the Explanatory Report to the Convention on Cybercrime that the production, distribution, and possession of entirely computer-generated child pornography does not constitute any victims of sexual abuse and, therefore, does not harm any children *directly*, still makes sense, for they can be seen as "victimless crimes" (Moerings 1999, p. 192). Bedau has defined the concept of a victimless crime as follows: "an activity is a victimless crime if and only if it is prohibited by the criminal code and made subject to penalty or punishment, and involves the exchange or transaction of goods and services among consenting adults who regard themselves as unharmed by the activity and, accordingly, do not willingly inform the authorities of their participation in it" (Bedau 1974, p. 73). As will be explained below the prohibition on the production, distribution, and possession of entirely computer-generated child pornography meets the requirements set by the aforementioned definition.

The distribution of entirely computer-generated child pornographic images can be seen as an exchange of goods. The exchange of entirely computer-generated child pornographic images leads to possession. And their production is also inevitably related to this exchange: on the one hand, no distribution and possession would be possible without production and on the other hand, distribution and (the demand for) possession create the market for production. If I limit myself to adults who intentionally exchange these images, the production, distribution, and possession of entirely computer-generated child pornography can be considered consensual as well. Finally, adults consenting to the exchange do not seem to regard themselves as harmed by this activity either. Many offenders would even argue the opposite and claim that looking at entirely computer-generated child pornographic images provides a safe outlet for feelings that otherwise would lead to the crime of sexual abuse of children (O'Brien & Webster 2007, p. 238).

Dutch researchers have claimed the same with regard to certain groups of pedophiles[26] (Kreulen 2012).

The conclusion that the production, distribution, and possession of entirely computer-generated child pornography can be seen as victimless crimes does not mean that "society has no right to interfere by prohibiting the activity and subjecting it to penal sanctions" (Bedau 1974, p. 75). Because there is no victim a victimless crime cannot result in harm to another person and, therefore, the harm principle does not apply. But according to Bedau, the criminalization of victimless crimes can be legitimated on the basis of two of Feinberg's other liberty-limiting principles: namely, legal paternalism or legal moralism (Ibid.). In the next two sections I will examine whether legal paternalism or legal moralism can legitimate the prohibition on the production, distribution, and possession of entirely computer-generated child pornography.

4.3 Legal paternalism as a ground for criminalization

In this section, I will study whether or not legal paternalism could legitimate the criminalization of entirely computer-generated child pornography. At first sight this seems implausible. As mentioned before in section 1.2.4, legal paternalism entails that it is a good and relevant reason in support of a penal prohibition that it prevents harm to the actor him- or herself (Feinberg 1986, p. 4). As was established in the last section, the production, distribution, and possession of entirely computer-generated child pornography are victimless crimes and one of the features of victimless crimes is that the participants regard themselves as unharmed by them. However, the self-judgement of the participants might, objectively seen, be incorrect (Bedau 1974, p. 76). Although they think otherwise, entirely computer-generated child pornographic images might in fact harm the people who produce, distribute or possess them themselves and if so, legal paternalism would offer a solid ground for criminalization.

As I discussed before in section 1.2.4, Feinberg distinguishes between two types of legal paternalism: soft (presumptively nonblamable) paternalism and hard (presumptively blamable) paternalism. Soft paternalism "consists of defending relatively helpless or vulnerable people from external dangers, including harm from *other* people when the protected parties have not voluntarily consented to the risk" (Feinberg 1986, p. 5). Hard paternalism justifies interferences

[26] I am aware that the term pedophile is disputatious. Pedophilia is a clinical diagnosis that can only be made by a psychiatrist or psychologist; it is not an official legal term (see e.g., Hall&Hall 2009). Throughout this chapter I will use the term pedophile to refer to people with a sexual interest in children.

with entirely voluntary self-regarding harmful behavior of people for their own good (Ibid., pp. 5, 12).

Soft paternalism could legitimate the criminalization of the production, distribution, and possession of entirely computer-generated child pornography if it can be proven that it could encourage or seduce children into participating in sexual contacts with adults, as the Explanatory Report to the Convention on Cybercrime claims (Council of Europe Convention on Cybercrime, Expl. Report § 102; see section 4.2). The basis for prohibition would then be situated in the protection of children against the aforementioned seduction or encouragement, thereby defending them from harm from pedophiles. This would fit well into the framework of traditional protections which criminal law has provided for children "against exploitation, manipulation and injury at the hands of adults" (Bedau 1974, p. 86). Think, for example, of the earlier mentioned legal doctrine that in sex contacts between adults and children mutual consent is assumed to be absent and that they are, therefore, always considered sexual abuse (Moerings 1999, p. 190).

Hard paternalism could legitimate the criminalization of entirely computer-generated child pornography if it can be proven that it encourages or seduces pedophiles to commit child abuse. The basis for prohibition would then be situated in the protection of pedophiles against the aforementioned seduction or encouragement, thereby defending children from harm from them. This can be interpreted as pure paternalism, for one can argue that the prohibition on entirely computer-generated child pornography saves pedophiles from themselves (i.e., their own urge to commit child abuse). That it also prevents harm to children does not stand in the way of that conclusion, since, as was argued before in section 1.2.4, paternalistic penal provisions always involve a public interest and the prevention of harm to children can be seen as such. The prohibition on entirely computer-generated child pornography can also be interpreted as impure paternalism, for one can argue that the class of people whose well-being is protected (children) is not identical with the class of people being coerced (pedophiles).[27] As was discussed before in section 1.3.3, the incurring of the harm requires the active co-operation of the victim in cases of impure paternalism (Dworkin 1972, p. 68). The term child abuse seems to imply that this requirement cannot be met. However, as was argued before in section 4.2.1, sex contacts between adults and children are, regardless their nature, always considered sexual abuse, so it is not impossible that the child actively co-operates.

In this section, I will respectively examine whether or not entirely computer-generated child pornographic images can encourage or seduce children into participating in sexual contacts

[27] *Cf.* the prohibition on unlicensed practice of a certain profession (e.g., medicine), where the unlicensed practitioner is coerced in order to protect the would-be patient or client, as was discussed in section 1.3.3.

with adults or pedophiles to commit child abuse. If (one of) these possibilities turn(s) out to be the case, this means that the second argument of the Supreme Court in the *Ashcroft v. Free Speech Coalition* case does not make sense, for the doubt there expressed as to whether entirely computer-generated child pornography could lead to actual instances of child abuse (a doubt that, as noted in section 4.2.2, rejects the second assumption at work in the Explanatory Report to the Convention on Cybercrime) then lacks justification.

4.3.1 Does entirely computer-generated child pornography encourage or seduce children into participating in sexual contacts with adults?

Investigators have found links between young people who watch pornographic images and their attitudes toward sex (DeAngelis 2007; Rutgers Nisso Groep/ Nederlands Jeugdinstituut/ Movisie, 2008; Movisie 2009; Office of the Children's Commissioner 2013). It has been suggested that the younger the child is, the more influence these images have on them (Movisie 2009, p. 70). Given their pornographic nature, it can thus be assumed that (entirely computer-generated) child pornographic images can influence children's attitudes toward sex, especially at a young age. It does not seem likely that children would deliberately search the Internet themselves for such images. But they might well be used by offenders to groom children into taking part in sexual activities (Johnson & Rogers 2009, p. 77). They could show them to a child in order to encourage participation, stimulate arousal or as an example of what they want the child to do (Quayle & Taylor 2002, p. 866). Another effect of child pornographic images on children could be that they come to think the activity must be acceptable, since others have engaged in it (Levy 2002, p. 320).

Research suggests that the possession of child pornography by pedophiles might, under certain circumstances, be indicative of future child abuse (O'Brien & Webster 2007; Bourke & Hernandez 2009; Fisher, Kohut, Di Gioacchino & Fedoroff 2013, see section 4.3.2). There is no evidence however, that pedophiles frequently make use of (entirely computer-generated) child pornographic images in the way as described above. And more important, they can and do make use of other means to groom children into taking part in sexual activities such as drugs, alcohol, toys, money or force (Levy 2002, p. 320).

As a Dutch court has pointed out, it makes a difference if the entirely computer-generated child pornographic images are specifically aimed at children. In 2008 a Dutch national was convicted for the possession of an entirely computer-generated child pornographic film. It was titled "Sex Lessons for young girls" and showed a virtual girl about 8 years of age engaged in

sexual explicit conduct with a man. The girl depicted is smiling, the man applauds for her and colorful balloons appear. The court argued that, although the persons appearing in the film do not look realistic to adults, they do seem realistic to the average child. Due to the instructional nature of the film and the colorful framing, the film seems to be aimed at children. Therefore, it could be used to encourage or seduce children into participating in sexual activities with adults (Rb.'s-Hertogenbosch, 4 February 2008, ECLI: NL: RBSHE: 2008: BC3225).

The verdict can further be explained as follows. Since the entirely computer-generated child pornographic images at stake are specifically aimed at children, they reflect the intent to use them to groom children into participating in sexual activities with adults. In this case but only in this case, soft paternalism provides for a solid ground for prohibition. The production, distribution, and possession of entirely computer-generated child pornographic images of this nature need to be prohibited in order to protect children against exposure to them and the risk of seduction or encouragement to participate into harmful sexual contacts with adults that comes with that. With reference to all other kinds of entirely computer-generated child pornographic images such a causal link between them and actual instances of child abuse has not been proven. Therefore, soft paternalism cannot provide a solid ground for the criminalization of entirely computer-generated child pornography in general.

4.3.2 Does entirely computer-generated child pornography encourage or seduce pedophiles to commit child abuse?

As stated earlier many offenders argue that entirely computer-generated child pornography has a positive rather than a negative effect on them, because looking at such images provides a safe outlet for feelings that otherwise could lead to sexual abuse of a child. Recently, the Dutch sexologists Van Beek and Van Lunsen have claimed the same with regard to certain groups of pedophiles (Kreulen 2012). They refer to a study by Diamond (Diamond 2010), who found that the number of reported cases of child sex abuse dropped markedly when the production, distribution, and possession of child pornography was decriminalized in the Czech Republic for a while. However, others argue that the reverse is true; they believe that there might be a causal link between watching (entirely computer-generated) child pornographic images and actual instances of child abuse. Consider the following recent examples.

First, a US study of 155 child pornography users suggests that "many Internet child pornography offenders may be undetected child molesters, and that their use of child pornography is indicative of their paraphilic orientation" (Bourke & Hernandez 2009, pp. 185,

190). Second, an international research review concludes that evidence indicates that child pornography use in the context of certain predisposing factors, including psychopathy and previous hands-on crimes, "may warrant increased concern regarding the possibility of future sexual aggression being directed toward (…) children" (Fisher, Kohut, Di Gioacchino & Fedoroff 2013, p. 8). Earlier research presents similar findings (see for an overview: O'Brien & Webster 2007, pp. 238-239). However, there is too little evidence yet to prove that an imminent causal link between entirely computer-generated child pornographic images and child abuse exists; future, larger-scaled research is needed (Bourke & Hernandez 2009, p. 190; Fisher, Kohut, Di Gioacchino & Fedoroff 2013, pp. 6-8).

There might (also) be a causal link between the process of exchanging entirely computer-generated child pornographic images and child abuse though. Prior to the Internet era pedophiles remained a relatively isolated group but this new technology has enabled them to form social networks online, which are called virtual communities or subcultures. The Internet provides them with a medium of exchange, not only of (entirely computer-generated) child pornographic images but also of ideas. Due to its anonymity, the Internet provides a relatively safe environment for the exchange of this illegal or at least generally disapproved content (Quayle & Taylor 2002, p. 867). According to the Explanatory Report to the Convention on Cybercrime the subculture thus formed, favors child abuse, because "it is widely believed that such material and on-line practices such as the exchange of ideas, fantasies and advice among pedophiles, play a role in supporting, encouraging or facilitating sexual offences against children" (Council of Europe Convention on Cybercrime, Expl. Report § 93).

The Explanatory Report to the Convention on Cybercrime seems to appeal to the process of "group polarization" as described by Sunstein here (Sunstein 2001). According to Sunstein, "the Internet gives you the opportunity to meet other people who are interested in the same things you are, no matter how specialized, how weird, no matter how big or how small" in a way that was never possible before (Ibid., p. 54). Sunstein further observes that like-minded people are more likely to convince each other with their arguments online, because "if identity is shared, persuasive arguments are likely to be still more persuasive; the identity of those who are making them gives them a kind of credential or boost" (Ibid., pp. 70-71). This can lead to the process of group polarization, which can be described as follows. "After deliberation, people are likely to move toward a more extreme point in the direction to which the group's members were originally inclined. With respect to the Internet (…) the implication is that groups of like-minded people, engaged in discussion with one another, will end up thinking the same thing that they thought before- but in a more extreme form" (Ibid., p. 65).

Sunstein claims there are two main explanations for the process of group polarization. The first emphasizes the role of the above-mentioned persuasive arguments. On this account, the central factor behind group polarization is the existence of a *limited argument pool*, which is skewed in a particular direction. The tendency of online discussion groups is to entrench and reinforce preexisting positions, often resulting in extremism (Sunstein 2001, pp. 67-68). The second explanation appeals to the idea of *the spiral of silence*. In groups people want to be perceived favorably by other group members and they also want to perceive themselves favorably. Once they hear what others think, they often adjust to the most dominant position in the group. Critical minorities silence themselves (Ibid., pp. 68-69).

According to Quayle & Taylor and O'Brien and Webster, a process of group polarization can indeed be recognized in the virtual communities formed by pedophiles. The following four characteristics of cognitive distortions are common in those who download child pornography. The first characteristic is the *justification* of the behavior, because child pornographic images are just images and watching them does not (directly) involve contact with an actual child. The second characteristic is the *normalization* of the behavior: child pornographic images could validate and justify the behaviour of those with a sexual interest in children, providing proof to them that the existence of such material shows that their behaviour is not abnormal but is shared by thousands of others. Also, most images portray compliant, often smiling children, which could further contribute to the sense of appropriateness and validation. The third characteristic is the *objectification* of the images: through a process of collecting the downloader distances himself from the illegal content. The images are used as a medium of exchange in which the images in themselves act as a form of currency, thereby legitimizing activity and creating social cohesion. The fourth and final characteristic is the *justification of other forms of engagement* with the images or, on occasion, real children, through colluding in a social network (Quayle & Taylor 2002, pp. 866-869; O'Brien & Webster 2007, p. 241).

In sum, due to the process of group polarization as described above pedophiles engaged in the exchange of (entirely computer-generated) child pornographic images will end up thinking of children in the same way as they thought of them before: as sex objects but likely in a more extreme form: that it is justified, normal and not harmful to think of children this way. And they might even come to think that actual child abuse is justified. However, the process of group polarization described does not only consist of the exchange of images: it is typically accompanied by an exchange of speech (Levy 2002, p. 321). Without the exchange of speech, the fourth cognitive distortion distinguished does not seem possible at all. It can thus not be concluded that the sole exchange of (entirely computer-generated) child pornographic images

can lead to a process of group polarization, which can ultimately encourage or seduce pedophiles to commit child abuse. Moreover, even if that could be proven, the causal link between entirely computer-generated child pornographic images and actual instances of child abuse would be indirect and according to the US Supreme Court that is, as mentioned before in section 4.2.2, an insufficient ground to conclude that they are harmful (*Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002)).

4.3.3 Concluding remarks

In conclusion, legal paternalism cannot provide a solid moral basis for the prohibition on the production, distribution, and possession of entirely computer-generated child pornography. There is no evidence that (entirely computer-generated) child pornographic images can encourage or seduce children into participating in sexual contacts with adults, except for images which are specially aimed at them. There is not enough evidence yet that (entirely computer-generated) child pornographic images can encourage or seduce pedophiles to commit child abuse. If (more) research could provide (more) evidence in the future that exposure to (entirely computer-generated) child pornographic images can have the aforementioned effects on children or pedophiles, the moral ground for prohibition of these images could be based in the protection of children against the seduction or encouragement to engage into (harmful) sexual contacts with adults or the protection of pedophiles against the seduction or encouragement to commit child abuse, thereby defending children from harm from them. However, research has not come that far yet.[28] The second argument of the Supreme Court in the *Ashcroft v. Free Speech Coalition* case, i.e., the doubt as to whether entirely computer-generated child pornography could lead to actual instances of child abuse, still makes sense.

[28] As mentioned before in section 1.2.4, criminal law starts to focus more on risk and less on harm (*supra* 8). Taking this shift into account, it could be argued that the prohibition on the production, distribution, and possession of entirely computer-generated child pornography can be legitimated on the basis of legal paternalism, because there is a risk of harm (i.e., possible encouragement or seduction to commit child abuse). This would be in line with the precautionary principle as applied in other fields of law, especially in environmental law (see e.g., article 191 of the EU Treaty on the functioning of the European Union). The precautionary principle entails that authorities may adopt legislative measures when scientific and objective research indicates that a phenomenon may have a dangerous effect (e.g., on human health or the environment) but cannot determine the risk with sufficient certainty (Commission of the European Communities Communication from the Commission of 2 February 2000 on the precautionary principle). However, with regard to the production, distribution, and possession of entirely computer-generated child pornography the research indicating the above-mentioned dangerous effect does not only lack sufficient certainty, it is also disputed by other research. Therefore, I persist in the conclusion that more research is needed.

4.4 Legal moralism as a ground for criminalization

There are two types of legal moralism: pure and impure legal moralism (see section 1.2.4). Supporters of pure legal moralism claim that "it can be morally legitimate (...) to prohibit conduct on the ground that it is inherently immoral, even though it causes neither harm nor offense to the actor or to others" (Feinberg 1988, p. 4). Impure legal moralism refers to the approach of some writers in legal philosophy who are called legal moralists, although the basic appeal in their arguments is to the harm or offense principle, e.g., because they claim that immoral conduct harms the social cohesion in society (Ibid., p. 8). The prohibition on the production, distribution, and possession of entirely computer-generated child pornography can be defended on the basis of arguments that fall under the latter category.

Entirely computer-generated child pornography is generally condemned, because many people feel revulsion and outrage at the thought of it (Sandin 2004). Feinberg would call this offense at "bare thought" (Feinberg 1988, p. 15). Conduct that results in offense at bare thought can sometimes legitimately be criminalized, though not on the basis of the offense principle, since the offense at stake is not caused by an unwanted confrontation with the conduct but by the thought of it. Offense at bare thought falls under the scope of legal moralism instead, for people are offended by the thought of conduct like the production, distribution, and possession of entirely computer-generated child pornography, because they find it morally objectionable (Feinberg 1988, p. 15; Sandin 2004).

As mentioned before in section 1.2.4, the validity of legal moralism as a ground for criminalization is contested. According to Feinberg it is at most sometimes but rarely a good reason to prohibit behaviors (Feinberg 1988, p. 323). In this section, I want to examine whether or not legal moralism is a good reason to prohibit entirely computer-generated child pornography. I wish to argue that it is if people have good reason to find entirely computer-generated child pornography morally objectionable. Yet the question arises whether or not they do.

According to McCormick virtue ethics "gives us the vocabulary to describe what seems intuitively wrong" about things like entirely computer-generated child pornography (McCormick 2001, p. 286). Therefore, I will study the above-mentioned question from a virtue ethics point of view. I will take Sara Ruddick's essay "Better Sex" (1975), which consists of a virtue ethics analysis of sex, as a starting point. I will show that feminists make use of arguments that resemble and extend Ruddick's arguments in the strong government policies against (adult) pornography that they endorse. In turn, I will extend these arguments to the case of entirely

computer-generated child pornography. At the end of this section, I will come to a reasoned conclusion on the question whether or not people have good reason to find entirely computer-generated child pornography morally objectionable, which would in turn provide a good reason to prohibit these behaviors on the basis of legal moralism.

4.4.1 'Thinking outside the box': a virtue ethics and feminist view of pornography

The roots of virtue ethics lie in the work of the ancient Greek philosophers Plato and Aristotle but it was reintroduced by the contemporary British philosopher MacIntyre in his book *After Virtue* (1984 [1981]). The key concepts of MacIntyre's virtue ethics are: virtue, practice and internal goods. MacIntyre defines a virtue as "an acquired human quality the possession and exercise of which tends to enable us to achieve those goods which are internal to practices and the lack of which effectively prevents us from achieving any such goods" (MacIntyre 1984, p. 191). By a "practice" he means "any coherent and complex form of socially established cooperative human activity through which goods internal to that form of activity are realized in the course of trying to achieve those standards of excellence which are appropriate to, and partially definitive of, that form of activity with the result that human powers to achieve excellence, and human conceptions to the ends and goods involved, are systematically extended" (Ibid., p. 187). Internal goods, at last, MacIntyre describes as those goods that can only be achieved by engaging in the practice (Ibid., p. 188).

I think that sex can be seen as a practice as defined by MacIntyre. I developed this idea after reading Sara Ruddick's essay titled "Better Sex" (1975). Interpreting her work in light of MacIntyre's definitions of virtue, practice and internal goods, Ruddick seems to argue that the virtue of respect for persons enables sex partners to achieve the good of "reflexive mutual recognition of desire by desire" which is internal to the practice of sex (Ruddick 1975, p. 89). By "reflexive mutual recognition of desire by desire" Ruddick means that the sex partners "actively desire and respond to each other's active desires", in other words: that they reach a level of reciprocity (Ibid., pp. 89-90). Sex practices in which the internal good of reciprocity is achieved through the virtue of respect for persons Ruddick calls "complete sex" (Ibid., p. 87).

Ruddick contrasts complete sex with incomplete sex, which lacks reflexive mutual recognition of desire by desire (i.e., reciprocity), because it is "private, essentially autoerotic, unresponsive, unembodied, passive, or imposed" (Ruddick 1975, pp. 100-101). Incomplete sex is not necessarily wrong, for "any sexual act that is pleasurable is *prima facie* good, though the

more incomplete it is –the more private, essentially autoerotic, unresponsive, unembodied, passive, or imposed – the more likely it is to be harmful to someone" (Ibid.). Ruddick does not mean harm as intended by the harm principle here but harm in the sense of virtue ethics, which can best be described as erosion of virtue (McCormick 2001, p. 285). Incomplete sex acts are "prone to violation of respect for, and often violence to, persons" (Ruddick 1975, p. 101). In other words: they erode the virtue of respect for persons which may, according to Ruddick, ultimately lead to violence.

In the strong government policies against (adult) pornography that they endorse, feminists make use of arguments that resemble and extend the above-mentioned assumption that the more private, essentially autoerotic, unresponsive, unembodied, passive, or imposed a sexual act is, the more likely it is to erode the virtue of respect for persons. Note that feminists distinguish between the sex acts *depicted* by pornographic images and the sex act of *watching* pornographic images. Except for initiatives to develop so-called "female-friendly" pornography, much pornographic material is prone to the feminist critique that it represents male dominance and female submission (e.g., Itzin 1992, p. 67; MacKinnon 1992, p. 461). According to MacKinnon, most of the sex acts depicted by pornographic images can be qualified as rape, battery, sexual harassment or prostitution (MacKinnon 1992, p. 461). Ruddick would say that these are all examples of incomplete –unresponsive and passive- sex acts. Most of them are imposed as well. The dominance and submission that is, according to feminists, common to these sex acts Ruddick would describe as a lack of the reciprocal recognition of the other as a person (in Kantian terms an end rather than a means to one's own sexual ends) that characterizes complete sex and its fostering of the primary virtue of respect for persons.

Applying Ruddick's theory to the sex act of watching pornography, it cannot be complete either, since it lacks embodiment. Therefore, no reciprocity can occur. Moreover, this sex act is essentially autoerotic, unresponsive and passive in nature. In sum, one could say that watching pornography is the incomplete sex act of watching incomplete sex acts (insofar as the sex acts depicted can be characterized as incomplete).[29] For Ruddick this would lead to the assumption that the sex act of watching pornography is likely to erode the virtue of respect for persons. Following feminist authors, the sex act of watching pornography erodes the virtue of respect for persons, because pornography celebrates, promotes, authorizes, and legitimizes sexual acts that involve rape, battery, sexual harassment, and prostitution and it "eroticizes the dominance and submission that is the dynamic common to them all" (MacKinnon 1992, p. 461). They believe

[29] Note that some consumers of pornography claim that watching it enhances their sex life. Although the sex act of watching pornography is incomplete (non-reciprocal) in itself, it might arouse couples to have complete (reciprocal) sex with each other.

that the message sent by pornography (i.e., non-reciprocal sex acts are erotic!) influences attitudes and behaviours towards a particular group of actual persons: namely, women. Pornographic images present to men "how it is permissible to look at and to see women"; they learn "to see women in terms of their sexuality and sexual inequality" (Ibid., p. 67).

Research conducted in experimental settings confirms that exposure to sexually violent pornography can lead to "antiwoman attitudes and antiwoman acts" but this research is criticized for its experimental setting (Fisher, Kohut, Di Gioacchino & Fedoroff 2013, p. 3). Non-experimental research suggests that gender-stereotyped sexual content negatively influences the sexual and psychological well-being of young people and that it might lead to acceptation of or even engagement in sexual harassment among them (Rutgers Nisso Groep / Nederlands Jeugdinstituut / Movisie 2008). Moreover, research mentioned before in section 3.3 suggests that degrading portrayals of women in computer games negatively influence people's attitudes and behaviors towards and their feelings about women in real life (Burgess, Stermer & Burgess 2007, p. 428).

But whether or not research can confirm the feminist assumption that pornography, or at least female-unfriendly pornography, can negatively influence attitudes and behaviours towards women is actually beyond the scope of this chapter. As was indicated in the introduction to this section, I do not wish to argue against (adult) pornography but I want to extend the above-mentioned arguments against (adult) pornography to the case of entirely computer-generated child pornography. For these purposes, it is important to note that the aforementioned arguments are rooted in the reproach that pornography shows women in terms of inequality (Boutellier 2000, p. 448). This reproach based upon in the equality norm that has been formulated in many legal documents, including the UN Universal Declaration of Human Rights, which states that "all human beings are born free and equal in dignity and rights" (article 1).

According to Itzin "the elimination of pornography is an essential part of the creation of genuine equality for women – and for men" (Itzin 1992, p. 70). MacKinnon is more modest. She argues that "women will never have that dignity, security, compensation that is the promise of equality so long as the pornography exists *as it does now*" (MacKinnon 1992, p. 486, emphasis added LS). The latter suggests that pornography does not need to disappear in order to comply with the equality norm but that it should depict sex acts in another, equal way. Following Ruddick this would be achieved if sex acts are no longer depicted as unresponsive, passive and thus non-reciprocal. Watching pornography would then become the incomplete sex act of watching complete sex acts instead of incomplete ones.

4.4.2 Entirely computer-generated child pornography in light of these criticisms

The above-mentioned possibility of changing female-unfriendly pornography in the direction of greater equality highlights a fundamental difference between adult pornography and child pornography, for "child pornography, actual or virtual, cannot depict children as equal participants in sexual activity with adults" (Levy 2002, p. 322). That is because "children are not equal" (Ibid.). As explained in section 4.2.1, children cannot consent to sex acts with adults and they are, therefore, always considered child abuse. Applying Ruddick's theory one could say that the sex acts depicted by child pornographic images cannot be complete, because the participants cannot reach a level of reciprocity. Child pornographic images depict sex acts that are incomplete, not only because they are, just like female-unfriendly pornographic images, unresponsive and passive but also because they are imposed.

With regard to entirely computer-generated child pornography there is an additional reason why it is impossible to change the sex acts depicted to more complete, reciprocal and thus equal ones. In order to make this clear, another comparison with adult pornography has to be made. Adult pornographic images do not only influence the way women are viewed by men but also the way women view themselves, for this reason Itzin calls them "mirror images" (Itzin 1992, p. 62). According to research especially young girls relate their self-objectification to pornographic images (Rutgers Nisso Groep / Nederlands Jeugdinstituut / Movisie 2008). However, no girl or woman could reach the beauty ideal many of them impose, for they are often photoshopped and present women with unnatural features. A much-discussed Dutch documentary (Bergman 2007) shows US women, including a 14-year-old girl, who undergo plastic surgery to look like the women they have seen depicted in pornographic images. They do not do so because they want to look like porn stars but because they consider those images realistic and think that they themselves are abnormal.

Applying Ruddick's theory, one could say that the sex acts depicted by pornographic images as described above lack embodiment. They do not show the participants engaged in a sex act but a photoshopped version of them. As stated in the last section, Ruddick thinks that the lack of embodiment is another indicator that a sex act is incomplete, besides unresponsiveness and passiveness. In comparison, entirely computer-generated child pornographic images have even further drifted apart from the embodied reality. They are not just photoshopped: they are entirely generated by a computer. From Ruddick's point of view, the sex acts depicted by entirely computer-generated child pornographic images thus lack one precondition for complete sex more

than *non*-virtual child pornographic images, for they are not only unresponsive, passive, and imposed but also unembodied.

Continuing the same line of reasoning that was followed in the last section with regard to the sex act of watching female-unfriendly pornography, it can be said that the sex act of watching child pornographic images is an incomplete sex act of watching incomplete sex acts that can never become complete. The sex acts concerned cannot be depicted in an equal way, because children are not equal; these sex acts are unresponsive, passive, and imposed per se, entirely computer-generated child pornographic images are also unembodied per se. I repeat that the more incomplete (i.e., the more private, essentially autoerotic, unresponsive, unembodied, passive, or imposed) a sex act is, the more likely it is to erode the virtue of respect for persons.

4.4.3 Concluding remarks

The lesson to be drawn from Ruddick's virtue ethics view and the feminist critique of pornography with regard to entirely computer-generated child pornographic images is that they depict unresponsive, passive, imposed, unembodied and thus non-reciprocal, unequal sex acts. Therefore, the production, distribution, and possession thereof flout our sexual mentality, which is based on equality. This leads to the conclusion that people have good reason to find these behaviors morally objectionable, which in turn provides good reason to prohibit them on the basis of legal moralism.

4.5 Conclusion

In the first section of this chapter, I defined the term "child pornography" and explained that there are actually three categories of child pornography. The first category of child pornography consists of images (photos, videotapes, films) showing a minor engaged in sexually explicit conduct. The second category of child pornography consists of images showing an adult appearing to be a minor engaged in sexually explicit conduct. The third category of child pornography consists of images which, although realistic, do in fact not involve a real child engaged in sexually explicit conduct. The latter category includes images which are altered or even generated entirely by the computer: i.e., virtual child pornography (Council of Europe Convention on Cybercrime, article 9 (2); Expl. Report § 101). All three categories of child

pornography are commonly criminalized since the introduction of the Convention on Cybercrime.

In the second section of this chapter I studied on which grounds the criminalization of the three categories of child pornography can be legitimated. With regard to the first category of child pornography there is consensus that it harms children, because the production thereof involves child abuse, and that the criminalization of this material can, therefore, be legitimated on the ground of the harm principle. I argued that the criminalization of the second category of child pornography can also be legitimated on the ground of the harm principle, if one applies a more pragmatic-oriented interpretation of harm. When images showing an adult appearing to be a minor engaged in sexually explicit conduct are included into the definition of child pornography, authorities do not need to prove that there was indeed a minor involved in the production and that harm to an actual child has been done, which enables them to combat online child pornography and the harm it causes to children effectively.

With regard to the third category of child pornography it is important to draw a distinction between pseudo images (images of a minor which are manipulated or morphed to make it appear like the minor is engaged in sexual activities) and entirely computer-generated images. The criminalization of pseudo child pornographic images can, just like the other categories of child pornography, be legitimated on the ground of the harm principle. If one manipulates or morphs an innocent picture of an actual child into child pornography, the child depicted can be harmed in his or her reputation or privacy, because s/he can be haunted by the image later on (Levy 2002, p. 319). The production, distribution, and possession of entirely computer-generated child pornography turn out to be "victimless crimes" (as described by Bedau 1974) to which the harm principle does not apply.

According to Bedau, the criminalization of victimless crimes is based on either legal paternalism or legal moralism (Bedau 1974, p. 75). In the third section, I explored whether or not the prohibition on the production, distribution, and possession of entirely computer-generated child pornography can be based on legal paternalism. The answer is negative. Unless the images are specially aimed at them, there is no evidence that entirely computer-generated child pornographic images can encourage or seduce children into participating in sexual contacts with adults, which could legitimate their criminalization on the basis of soft paternalism. There is not enough evidence yet that entirely computer-generated child pornographic images can encourage or seduce pedophiles to commit child abuse, which could legitimate their criminalization on the basis of (pure or impure) hard paternalism. If (more) research could provide (more) evidence in the future that exposure to (entirely computer-generated) child pornographic images can have the

aforementioned effects on children or pedophiles, the moral ground for prohibition of these images could be based in the protection of children against the seduction or encouragement to engage into (harmful) sexual contacts with adults or the protection of pedophiles against the seduction or encouragement to commit child abuse, thereby defending children from harm from them. However, research has not come that far yet.

In the last section, I argued that the prohibition on the production, distribution or possession of entirely computer-generated child pornography can be defended on the basis of (impure) legal moralism. Legal moralism is rarely a good reason for prohibition, however. I argued that it is if people have good reason to find that the conduct at stake is morally objectionable. I studied whether or not people have good reason to find the production, distribution, and possession of entirely computer-generated child pornography morally objectionable in light of Ruddick's virtue ethics analysis of sex (Ruddick 1975), and the feminist critique of (adult) pornography, which resembles and extends Ruddick's arguments (Itzin 1992; MacKinnon 1992). The lesson to be drawn from them with regard to entirely computer-generated child pornographic images is that they depict unresponsive, passive, imposed, unembodied and thus non-reciprocal, unequal sex acts. Therefore, the production, distribution, and possession thereof flout our sexual mentality, which is based on equality. This leads to the conclusion that people have good reason to find these behaviors morally objectionable, which in turn provides good reason to prohibit them on the basis of legal moralism.

PART III: REFLECTION

CHAPTER 5 REGULATING VIRTUAL CYBERCRIME: A PHILOSOPHICAL, LEGAL-ECONOMIC, PRAGMATIC, AND CONSTITUTIONAL DIMENSION

A slightly different version of this chapter was published as a paper titled "Should virtual cybercrime be regulated by means of criminal law? A philosophical, legal-economic, pragmatic, and constitutional dimension." *Information & Communications Technology Law*, *Volume 23*, *Issue 1*, 31-60 (2014).

Introduction

In the first chapter of this dissertation, I have studied the question when virtual cybercrime should be brought under the scope of criminal law from a legal-ontological and a legal-philosophical perspective. In the second, third, and fourth chapter I have applied my findings from the first chapter to three particular instances of virtual cybercrime (i.e., theft of virtual items, virtual rape, and virtual child pornography) and dealt with specific issues they give rise to. In this last, reflective chapter, I will broaden my horizon and study the aforementioned question from other, non-philosophical perspectives.

Based on what has been written on the topic of criminalization (i.e., the general question of which conduct should be brought under the scope of criminal law and which not), I believe that the question when virtual cybercrime should be brought under the scope of criminal law has, besides a philosophical, also a legal-economic, a pragmatic, and a constitutional dimension (Hulsman 1972, pp. 87-88; Husak 2004, pp. 112-115). Below, I will briefly explain what the legal-economic, pragmatic, and constitutional dimension entail and how they are or are not relevant for the specific case of virtual cybercrime.

The legal-economic dimension of the question when virtual cybercrime should be brought under the scope of criminal law belongs to a separate field in legal studies, which can be called the law and economics approach (Posner 1985; Bowles, Faure & Garoupa 2008, p. 390; Husak 2008). In essence, the law and economics approach consists of a cost-benefit analysis: the appropriate domain for the use of criminal law is determined by the costs and benefits of using criminal law relative to non-criminal instruments such as administrative or civil law (Bowles, Faure & Garoupa 2008, p. 395). I think that a reflection on the costs and benefits of using criminal law for the regulation of virtual cybercrime relative to non-criminal instruments is a relevant addition to the philosophical analysis provided so far. Since virtual cybercrime often takes place in the virtual environments of computer games, specific attention will have to be paid to the rules of games as an alternative for criminal law in the regulation of virtual cybercrime.

The pragmatic dimension of the question when virtual cybercrime should be brought under the scope of criminal law has to do with the overall capacity of the criminal justice system. As a rule, the criminalization of conduct should not overload the criminal justice system. When conduct involves the use of ICTs, as does virtual cybercrime, there is a high risk that its criminalization will overload the criminal justice system, because ICTs have a couple of features which facilitate crime and hamper law enforcement. In this chapter, I will discuss the aforementioned features. I will focus on their meaning for virtual cybercrime.

The constitutional dimension of the question when virtual cybercrime should be brought under the scope of criminal law focuses on the burden that is imposed on the (fundamental) liberties of citizens. When conduct constituting virtual cybercrime is brought under the scope of criminal law, people are no longer at liberty to perform it and, more importantly, they are subjected to punishment if they do. Both the restriction of liberties and punishment need legitimization in liberal, democratic societies (Husak 2004, pp. 115-116). The constitutional dimension will turn out to overlap with the philosophical and the legal-economic dimension, because the restriction of liberties and punishment are often legitimated on the basis of philosophical and legal-economic arguments.

The structure of this chapter will be as follows. In the first section, I will summarize my findings from the previous sections. Together they form the philosophical dimension of the question when virtual cybercrime should be brought under the scope of criminal law. In the second, third, and fourth section, I will respectively study the legal-economic, pragmatic, and constitutional dimension of that question. At the end of each section, I will concretize my analysis into absolute and relative negative criteria for the criminalization of virtual cybercrime. They will indicate when virtual cybercrime should *not* be brought under the scope of criminal law and they can be used to decide on actual cases. I will explain that these criteria are not conflicting but that they complement each other: one should test a particular instance of virtual cybercrime against all criteria together if one wants to answer the question of whether or not it should be brought under the scope of criminal law. In the last section, I will test all (putative) instances of virtual cybercrime that have been discussed throughout this dissertation against the aforementioned criteria.

5.1 Philosophical dimension

In this section, I will first repeat what is to be understood by the term “virtual cybercrime”. Then, I will briefly summarize the findings from the legal-ontological and the legal-philosophical

analysis of virtual cybercrime that were provided in the first chapter (sections 1.2 and 1.3). I will also refer to the findings with regard to specific instances of virtual cybercrime from chapters 2, 3, and 4. Together, these findings form the philosophical dimension of the question when virtual cybercrime should be brought under the scope of criminal law. At the end of this section, I will formulate philosophical criteria for the criminalization of virtual cybercrime, which can be used to decide on actual cases.

5.1.1 Virtual cybercrime: definition and meaning

As argued previously in section 1.1.5, virtual cybercrime can be defined as a computer-simulated human act or a human act made possible by computer simulation that is prohibited by the extension of an existing law. In section 1.1.4, a computer-simulated human act has been described as an act that is performed in a virtual environment through an input device (Søraker 2010, p. 147). An example of a computer-simulated human act is gambling on a virtual slot machine in a virtual casino. Such a computer-simulated human act consists of three steps. First, a human being performs a bodily action, e.g., the pressing of a button or the clicking of the mouse. Second, the computer simulation interprets the bodily action as a particular command, e.g., "spin the reel". Third, the computer simulation makes the changes to the virtual environment, and possibly to the non-virtual world as well, that are required by the command (Ibid., p. 137). In this case the reels of the virtual slot machine will spin and stop at a certain point. If the reels show a winning combination of symbols, the player is paid money and if they do not, the player loses money. The money may be won or lost within the virtual environment but it is also possible that it is won or lost in the non-virtual world. Depending on the situation, the computer-simulated human act of gambling on a virtual slot machine in a virtual casino thus may or may not have real financial consequences for the player. In countries where gambling is prohibited (e.g., New Zealand) it can be brought under the scope of existing criminal law.

A human act made possible by computer simulation has been described as an act that is defined in terms of a virtual object. Computer simulation is the condition of possibility for such an act and the nature of that act is partly determined by features of the computer simulation (Søraker 2010, pp. 33-34). The production, possession, and distribution of virtual child pornography are examples of human acts made possible by computer simulation. The aforementioned acts are not virtual in themselves but defined in terms of a virtual object: virtual child pornography. Virtual child pornographic images are child pornographic images which, although realistic, do not involve a child really engaged in sexually explicit conduct. They are

either photoshopped pictures of real children or entirely computer-generated images (Council of Europe Convention on Cybercrime, Expl. Report § 101). Computer simulation is thus the condition of possibility for the production and the inherent distribution and possession of virtual child pornographic images. The nature of these acts is partly determined by the features of the computer simulation, because they do not involve (the profiting from) child abuse, as opposed to the production, distribution, and possession of *non*-virtual child pornographic images. The Convention on Cybercrime's prohibition on child pornography includes the production, distribution, and possession of virtual child pornography in its scope (Council of Europe Convention on Cybercrime, article 9 (2) c).

5.1.2 Ontology

In section 1.2.1, I discussed the social ontology of the American philosopher Searle. He distinguishes a special class of facts: institutional facts. Institutional facts are special, because they are ontologically subjective but epistemically objective: they only exist by human agreement or acceptance but the truth or falsity of statements about them can be ascertained without reference to their attitudes or feelings. Institutional facts come into being, because human institutions impose status functions on entities that they cannot perform solely in virtue of their physical structure (Searle 1995, p. 1; Searle 2010, p. 7). Status functions are imposed by means of constitutive rules (or: declarations). Many declarations are not applicable to one specific entity but to an indefinite number of entities that all share the same feature(s). They are called "Standing Declarations" and generally take the following form: for any x that satisfies a certain set of conditions p, x has status Y in C (Searle 2010, p. 99). (Standing) Declarations have a double function: they do not only assign status to entities but they also confer rights, duties, and obligations ("deontic powers") upon people (Ibid., p. 8, 106). For the purposes of this dissertation, it should be highlighted that penal provisions are Standing Declarations. They typically indicate that a human act (X) with certain features (p) counts as a crime (Y) in a particular jurisdiction (C) and can apply to an indefinite number of such acts. Penal provisions do not only assign the status of crime to certain human acts, but they also confer the deontic power of criminal liability upon people.

It was explained in section 1.2.2 that in legal terms, the conditions that a human act needs to satisfy in order to count as a crime are called elements. The specific elements required vary depending on the crime but there are two basic elements that are required by each crime: an *actus reus* (an unlawful act or failure to act) and a *mens rea* (a blameworthy mental state; usually

such that the actor acts knowingly, purposely or recklessly).[30] In fact, all crimes also require, implicitly or explicitly, that the actus reus must have a certain consequence, e.g., the death or injury of a person or a loss of property. This common element is called *causation*.

I argued that, in the case of virtual cybercrime, the basic elements of a crime can be satisfied "intravirtually" (within the virtual environment where the act takes place) or "extravirtually" (outside its virtual environment).[31] It is of crucial importance where the element of causation is satisfied, intravirtually or extravirtually, because that determines the context (C) in which the crime status (Y) of the virtual cybercrime holds. A computer-simulated human act or human act made possible by computer simulation (X) that satisfies the element of causation (p) *intravirtually* cannot count as a crime (Y) in the context of the non-virtual world (C) but may count as a crime (Y) in the context of its virtual environment (C). A computer-simulated human act or human act made possible by computer simulation (X) that satisfies the element of causation (p) *extravirtually* cannot only count as a crime (Y) in the context of its virtual environment but also in the context of the non-virtual world (C). Consider the following example. In chapter 2, I discussed the act of stealing virtual items in an online multiplayer computer game through deceit or physical violence, which is a human act made possible by computer simulation. I established that this act (X) counts as the crime of theft (Y) in the context of the non-virtual world (C), provided that it satisfies the element of causation of that crime (p) i.e., loss of valuable property, *extravirtually*.

Sometimes, a computer-simulated human act or human act made possible by computer simulation (X) can satisfy the actus reus element and the attendant element of causation of one crime intravirtually and, thereby, satisfy the actus reus element and the attendant element of causation of another crime extravirtually. Such an act counts, therefore, as crime Y in the context of its virtual environment (C) and as crime Z in the context of the non-virtual world (C).[32] Consider the following example. In chapter 3, I discussed the computer-simulated human act of virtual rape in a virtual world. I established that this act (X) counts as the crime of rape (Y) in the context of its virtual environment (C) but as the crime of sexual harassment (Y) in the context of the non-virtual world (C).

The context (C) in which the crime status (Y) of an act of virtual cybercrime (X) holds, its virtual environment or the non-virtual world, determines whether or not the act can be included in the scope of an existing penal provision, for criminal law does not apply *within*

[30] The terms "actus reus" and "mens rea" derive specifically from Anglo-American jurisprudence. But these elements are, under a different name, also found in other legal systems.
[31] The distinction between "intravirtual" and "extravirtual" derives from Søraker 2012, pp. 504-509.
[32] The distinction among the three above-mentioned types of virtual human acts and the different contexts in which their status function holds, derives from Brey 2014, pp. 49-50.

virtual environments. On the basis of this legal ontological analysis it can thus be concluded that an act of virtual cybercrime can only be brought under the scope of a penal provision if it satisfies the element of causation of the crime extravirtually. But, depending on the stand one takes in the legal philosophical debate between legal positivists and natural law theorists, there are also other conditions to be met. This will be explained below.

5.1.3 Legal philosophy

As explained in section 1.2.3, there are two main, rival, theories about the content of the law in legal philosophy: legal positivism and natural law theory. Legal positivists claim that laws may have any content. They would thus say that legislators and judiciaries are free to bring any virtual cybercrime that satisfies the element of causation of the crime extravirtually under the scope of criminal law. By contrast, natural law theorists think that the content of laws is determined by their relation to morality. Natural law theorists would say that a virtual cybercrime that satisfies the element of causation of the crime extravirtually can only be brought under the scope of criminal law if the extravirtual consequence consists of a violation of a moral principle.

Searle's framework is neutral with respect to the debate between legal positivists and natural law theorists. He leaves it open *why* human institutions impose the status function of crime on human acts by means of penal provisions, i.e., he leaves it open whether or not they might do so *because of* moral principles. In this dissertation I have not chosen sides in the debate between legal positivists and natural law theorists either but I have focused on their common ground.

The contemporary debate on the content of the law has reached such a level of subtlety and sophistication that the traditional labels of legal positivism and natural law theory hardly apply anymore (Murphy & Coleman 1990, p. 36). Nowadays there is consensus that the law is open to arguments that are grounded in moral principles. Feinberg's work *The Moral Limits of Criminal Law* (1984, 1985, 1986, 1988), which consists of four separate books and is discussed in section 1.2.4, extensively treats the general question of what moral principles are of importance to determine which human conduct should be criminalized and which not.

Feinberg points out that when legislators or judiciaries bring a certain human act under the scope of a penal provision, citizens are no longer at liberty to perform that act (Feinberg 1984, p. 7). According to Feinberg such an interference with the liberty of citizens by means of criminal law is usually legitimated on the basis of one of the following four liberty-limiting

principles: the harm principle, the offense principle, legal paternalism or legal moralism (Feinberg 1985, p. ix). It should be added that, to my knowledge, no writer in legal philosophy denies the validity of the harm principle as a good and relevant reason in support of a penal provision. Most writers acknowledge the offense principle as well. But legal paternalism and especially legal moralism are contested (Feinberg 1984, pp. 14-15). Feinberg himself thinks that they are "at most sometimes (but rarely) good reasons" for the criminalization of conduct (Feinberg 1988, p. 323).

The first liberty-limiting principle is the harm principle, which originally derives from Mill (Mill 1865). This liberty-limiting principle and its implications for virtual cybercrime are thoroughly discussed in section 1.3.1. Here, it suffices to repeat that harm, as intended by the harm principle, consists of a wrongful setback to a person's interest, including the interest in the continuance of one's life for a foreseeable interval, the interest in bodily integrity and the interest in the security of property (Feinberg 1984, p. 37). Harm can also consist of a wrongful setback to a public interest such as the interest in political and economic stability or the interest in a clean environment (Ibid., pp. 11, 63-64).

The second liberty-limiting principle is the offense principle. This liberty-limiting principle and its implications for virtual cybercrime are thoroughly discussed in section 1.3.2. Here, it suffices to repeat that offense refers to all kinds of disliked mental states such as disgust, shame, embarrassment, and fear, when caused by the wrongful conduct of others (Feinberg 1985, pp. 1-2).

The third liberty-limiting principle is legal paternalism. This liberty-limiting principle and its implications for virtual cybercrime are thoroughly discussed in section 1.3.3. Here, it suffices to repeat that legal paternalism is, just like the harm principle, concerned with harm. But contrary to the harm principle, legal paternalism is not concerned with harm to other persons but with harm to the self (Feinberg 1986, p. 4).

The last liberty-limiting principle is legal moralism. This liberty-limiting principle and its implications for virtual cybercrime are thoroughly discussed in section 1.3.4. Here, it suffices to repeat that legal moralism is not concerned with harm or offense but with evils of other kinds (Feinberg 1988, p. 3).

5.1.4 Philosophical criteria for the criminalization of virtual cybercrime

As was indicated at the beginning of this section, I will conclude my philosophical analysis of virtual cybercrime by establishing criteria for its criminalization, which can be used to decide on

actual cases. The criteria will be negative criteria i.e., they will indicate when virtual cybercrime should *not* be brought under the scope of criminal law. I will distinguish between absolute and relative negative criteria for the criminalization of virtual cybercrime. The absolute negative criteria will indicate when criminalization of virtual cybercrime should be omitted. The relative negative criteria will be warnings; the more of these criteria are applicable, the less appropriate it is to criminalize the virtual cybercrime concerned. They can thus be seen as contraindications for criminalization.[33]

On the basis of the philosophical analysis of virtual cybercrime contained in this section, two absolute negative criteria for the criminalization of virtual cybercrime can be established. The first absolute negative criterion follows from section 5.1.2 and entails that, from an ontological point of view, criminalization of a virtual cybercrime should be omitted if it does not have an extravirtual consequence. The second absolute negative criterion follows from section 5.1.3 and entails that, from a legal-philosophical point of view, criminalization of a virtual cybercrime should be omitted if its extravirtual consequence cannot be brought under the scope of one of Feinberg's liberty-limiting principles (i.e., the harm principle, the offense principle, legal paternalism, or legal moralism).

Moreover, four relative negative criteria for the criminalization of virtual cybercrime can be established. None of them concerns the ontological part of my analysis[34]; they all derive from the legal-philosophical part of my analysis. The first relative negative criterion entails that it is a contraindication for the criminalization of a virtual cybercrime if its extravirtual consequence does not consist of harm (as intended by the harm principle). The second relative negative criterion entails that it is a contraindication for the criminalization of a virtual cybercrime if its extravirtual consequence does not consist of offense (as intended by the offense principle). The third relative negative criterion entails that it is a contraindication for the criminalization of a virtual cybercrime if its extravirtual consequence does not consist of harm to the self (as intended by legal paternalism). The fourth relative negative criterion entails that it is a contraindication for the criminalization of a virtual cybercrime if its extravirtual consequence does not consist of an evil of another kind (as intended by legal moralism). The more of the aforementioned relative

[33] The distinction between absolute and relative negative criteria for criminalization derives from Hulsman 1972, pp. 89-90.
[34] The ontology of virtual cybercrime seems to have an all-or-nothing character: from an ontological point of view a virtual cybercrime either has an extravirtual consequence legitimating its criminalization or not.

negative criteria are met, the less (acceptable[35]) liberty-limiting principle is applicable and the less appropriate it is to criminalize the virtual cybercrime concerned.

5.2 Legal-economic dimension

In this section, I will study the legal-economic dimension of the question of when virtual cybercrime should be brought under the scope of criminal law. I will first make some general remarks about the economic analysis of criminal law. Note that some of the points made are not only made by scholars in the field of economic analysis of criminal law, but are shared by scholars in other fields, although they do not translate them into the economic terms of costs and benefits. Next, I will discuss the specific case of virtual cybercrime. At the end of this section, I will concretize my analysis by establishing legal-economic criteria for the criminalization of virtual cybercrime.

5.2.1 General remarks

The legal philosophers Beccaria and Bentham are often mentioned as the forerunners of the economic analysis of criminal law (e.g., Posner 1985, p. 1193; Becker 1968, p. 209). They analyzed criminal law in utilitarian terms. The core insight of utilitarianism is that one ought to strive for the greatest amount of happiness for the greatest number (Driver 2009). Both Beccaria and Bentham believed that criminal law is rooted in this insight and claimed, therefore, that conduct should only be treated as a crime when society as a whole is better off by treating it as such (Beccaria 1986 [1764]; Bentham 1988 [1789]; Moohr 2005, p. 786; Posner 1985, p. 1193).

The contemporary law and economics approach, which started in 1968 with Gary Becker's article on the economics of crime and punishment, has introduced the cost-benefit analysis as a method to calculate if the criminalization of certain conduct makes society as a whole better off (Becker 1968). A cost-benefit analysis proceeds though three stages. In the first stage, costs, or negative consequences are identified. The second stage identifies benefits or positive consequences. In the third stage, weights are assigned to the costs and benefits and they are balanced against each other (Moohr 2005, p. 787). Scholars in the field of law and economics generally determine the costs and benefits of regulation via criminal law by comparing them to

[35] It was explained in section 5.1.3 that, to my knowledge, no writer in legal philosophy denies the validity of the harm principle as a good and relevant reason in support of a penal provision and most writers acknowledge the offense principle as well but legal paternalism and especially legal moralism are contested.

those of regulation via other means, i.e., civil or administrative law (Bowles, Faure & Garoupa 2008, p. 395). The main difference between regulation via criminal law on the one hand and regulation via civil or administrative law on the other hand lies in the available sanctions: where civil and administrative law only allow for monetary sanctions (e.g., torts and fines), criminal law allows for other, more severe, types of sanctions such as imprisonment and community service.

The costs associated with the use of criminal law can be divided into two main categories. The first category consists of the costs of apprehending and convicting offenders (broadly: criminal law enforcement). Here, one can think, for example, of the costs of funding police, courts, and defenders. Criminal law enforcement is more expensive than civil law or administrative law enforcement. Since criminal law is more powerful and any mistake is more harmful, the interests of innocent defendants need to be protected and, therefore, criminal procedures are lengthier and costlier (Bowles, Faure & Garoupa 2008, p. 398, 407). The second category consists of the costs of imposing sanctions, think of the costs of collecting fines, constructing and maintaining prisons, probation officers etc. The execution of criminal sanctions is usually more expensive than the execution of civil or administrative sanctions as well. Where the execution of civil or administrative sanctions (e.g., torts and small fines) is close to a costless transfer payment, the execution of criminal sanctions, even when they take the form of fines and especially when they take the form of imprisonment, is not (Posner 1985, p. 1214).

Moreover, the use of criminal law also has several costs which go far beyond the obvious components mentioned above and which are generally overlooked, especially when the criminal sanction of imprisonment is concerned (Brown 2004, p. 325, 343). First of all, a criminal record harms the offender's job stability. Lawyers or doctors, for example, might lose their licenses to practice their professions. Others can be kept away from positions that rely on trust or otherwise involve fiduciary duty (Cohen 2009, p. 360). Imprisonment, in particular, leaves the offender with large gaps in work history, while removing him or her from a culture that builds responsible work habits. Imprisonment similarly strains personal relationships and makes released offenders less appealing marriage prospects. Secondly, imprisonment negatively affects the offender’s family and, especially, children, for it removes a parent or family member who could otherwise have provided financial or another form of support such as babysitting or child supervision, and has a stigmatizing effect among neighbors and other social groups. Thirdly, high imprisonment rates have severe effects on the social capital of the neighborhoods or networks to which the offenders belong. They aggravate the preexisting problem of youth's differential access to positive opportunities through work, family, and community social networks and the

stigmatizing effects of imprisonment may spill over to those without criminal histories (Brown 2004, pp. 345-348).

Finally, the use of criminal law can cost innovation and creativity. In emerging areas, especially the area of emerging technology, the scope of criminal law and definitions of criminal activity are largely untested and might, therefore, be unclear. As a result, well-meaning and law-abiding individuals and businesses might not act out their innovative and creative ideas, because they are afraid that they will violate criminal law, where in reality they would not (Cohen 2009, p. 357). This is sometimes called the overdeterrence problem, because the deterrent effect of criminal law, which will be discussed as a benefit below, in fact becomes too broad, for criminal law deters activities that it does not aim to deter. The overdeterrence problem is of particular concern in the area of new technology crimes and deserves, therefore, special attention with regard to virtual cybercrime.

The main benefit of regulation via criminal law rather than via civil or administrative law is that, as indicated before, criminal law offers the possibility to impose another type of sanctions (Bowles, Faure & Garoupa 2008, p. 398). These sanctions may be more appropriate than administrative or civil sanctions, for several reasons. First of all, criminal sanctions do, contrary to non-criminal sanctions, not aim to compensate for the wrongdoing but to punish the offender (Ibid., p. 403; Brown 2004, p. 325). The latter is called retribution. Retribution is generally more appropriate than compensation with regard to crimes of violence such as murder, battery, and rape, because it is difficult or even impossible to translate losses like pain and bodily injury into monetary terms (Posner 1985, p. 1202; Husak 2004, p. 112). Another reason why retribution can be more appropriate than compensation has to do with the problem of insolvency: the majority of persons who inflict losses on others lack sufficient financial means to fully compensate their victims and they cannot resort to insurance, because it is generally not allowed to buy insurance against the risk of performing conduct that the state prohibits (Posner 1985, p. 1204; Husak 2004, p. 113; Bowles, Faure & Garoupa 2008, p. 411). In cases of “public” harm, e.g., the environmental crime of air pollution (see section 1.2.4), retribution is more appropriate than compensation because there are no (easily) identifiable victims who can be compensated (Bowles, Faure & Garoupa 2008, p. 400).

Secondly, criminal sanctions have, more than non-criminal sanctions, a preventive effect. Obviously, the imprisonment of offenders can prevent their further offending (Brown 2004, p. 325). But criminal sanctions can also prevent potential offenders from offending at all, for it is assumed that threatening a potential perpetrator with serious punishment such as imprisonment or a high fine, will deter the intended crime. The deterrent effect of criminal sanctions can be a

reason for criminalization in cases where there may be a relatively high degree of damage and a relatively low chance of catching the perpetrator (Bowles, Faure & Garoupa 2008, p. 402).

Thirdly, criminal sanctions, even monetary criminal sanctions, are able to create more stigma than non-criminal sanctions, which can be seen as non-monetary disincentive (Bowles, Faure & Garoupa 2008, p. 406; Posner 1985, p. 1205; Ogus 2009, p. 94). Therefore, they may be more appropriate than non-criminal sanctions in the case of severe crimes. The idea that the perpetrators are harshly punished, may provide victims and others with emotional comfort (Brown 2004, p. 325).

Another benefit of using criminal law that is sometimes mentioned is the educative effect of criminalizing conduct, which is closely related to the preventive effect of the imposition of criminal sanctions. The idea that the criminalization of conduct has an educative effect was introduced in a paper by Jean Hampton (Hampton 1984). The theory is that a formal legislative statement in the form of a penal prohibition, issued in the name of the community, educates both the offender and the public and, thereby, forms new social norms against infringement, even among those who do not share its underlying value (Ibid.; Moohr 2005, p. 796). Consider the following example. A while after the car was invented, the prohibition on drunk driving was enacted. This penal prohibition has taught the public that driving while drunk is dangerous and has created the new social norm that one ought to stay sober when one still has to drive. In other words, criminal law can be seen as an expression and enforcement of certain public values (Brown 2004, p. 325).

Which weights are assigned to the costs and benefits of using criminal law and how they are balanced against each other, depends on the case. But in general the benefits of using criminal law will probably outweigh the costs when the losses are diffuse (i.e., because they are difficult to translate into monetary terms or because there is no easy identifiable victim) and relatively large (Bowles, Faure & Garoupa 2008, p. 411). It was explained in this section that retribution via criminal law is a more appropriate way of sanctioning behaviors which cause diffuse and relatively large losses than compensation via non-criminal instruments. That is because, given the diffuseness of the losses, compensation is difficult or even impossible and, given the extent of the losses, insolvency is likely to be a problem and prevention or education to deter the crime and the imposition of stigma as an additional disincentive are necessary. I will now turn to the specific case of virtual cybercrime, which will be discussed in the next section.

5.2.2 The specific case of virtual cybercrime

When I apply the general principle that the benefits of using criminal law outweigh the costs when the losses are diffuse and relatively large to the specific case of virtual cybercrime, the question arises whether or not virtual cybercrime can cause losses which are diffuse and relatively large in the first place. Throughout this dissertation, I have discussed several instances of virtual cybercrime. Mostly, they result in losses that are diffuse, either because they are difficult to translate into monetary terms or because there is no easy identifiable victim. Consider the two examples below.

The first example concerns virtual rape in a virtual world. As explained in chapter 3, a user can feel shocked in real life when his or her avatar is raped by another user's avatar in the virtual world of a computer game. I believe it can constitute sexual harassment, for that includes in its scope the unwanted showing of pornography and that is how one could see virtual rape in a virtual world, provided that one includes virtual pornography in the definition of pornography (UN General Recommendation No. 19 to the Convention on the Elimination of all Forms of Discrimination Against Women, § 18). Sexual harassment causes a mental or emotional type of harm. That is a diffuse loss, because it is difficult to translate into monetary terms. The second example concerns the production, distribution, and possession of virtual child pornography. These crimes result in a diffuse loss, because there is no easy identifiable victim. In fact, there is no victim at all: the production, distribution, and possession of virtual child pornography are so-called “victimless crimes” (see section 4.2.2).

Let us now turn to the question whether or not the losses caused by virtual cybercrime are also large enough to legitimate regulation via criminal law. If the loss that a virtual cybercrime causes consists of harm, the question of whether or not that loss is large enough to justify regulation via criminal law overlaps with the question of whether or not that loss can be brought under the scope of the harm principle, which belongs to the philosophical dimension of the question when virtual cybercrime should be brought under the scope of criminal law. As stated in section 1.3.1, the harm principle can only be invoked if enough well-being is under threat (Feinberg 1984, p. 189). The quantity of well-being that is under threat varies proportionally with the severity of the sanction that is to be imposed. If the amount of well-being that is under threat is so minor it cannot even legitimate the imposition of a small fine, the harm principle cannot be invoked at all (Holtug 2002, p. 366). If a virtual cybercrime results in a harm that is large enough to invoke the harm principle, it is also large enough to legitimate regulation via criminal law.

If the loss that a virtual cybercrime causes consists of offense, there is a similar connection. It was stated in section 1.3.2 that, given the high degree of avoidability of offense on the Internet in general and in virtual environments in particular, only very serious offenses can tip the scales so that the offense principle can be invoked (Weckert 2000). Offenses that are serious enough to invoke the offense principle, are also large enough to legitimate regulation via criminal law.

If the loss that a virtual cybercrime causes consists of harm to the self there is a slightly different connection. As stated in sections 1.2.4 and 1.3.3, there is always a public interest involved; at least to a small extent, when people harm themselves as intended by legal paternalism (Feinberg 1986, pp. 21-22). Here, it is not the harm to the self but the public interest involved that must be large enough to legitimate regulation via criminal law. Feinberg states: "A nonproductive life devoted entirely to lotus-eating, opium smoking, or heroin shooting, in which all of one's waking moments are spent cultivating or enjoying dreamy euphoric states, may be "no one else's business" [quotation marks in original text] when one, or a hundred, or ten thousand self-supporting persons do it of their own free choice. But when ten percent of the whole population choose to live that way, they become parasitical, and the situation approaches the threshold of serious public harm" (Ibid., p. 23). Feinberg only considers the costs of the loss of (labor) productivity here, but there are also other costs involving a public interest that have to be taken into account. Self-harming activities including drug abuse can, for example, lead to increased use of public services such as mental health, primary health, and criminal justice, which are funded with tax money (see section 1.3.3). Interpreting and extending Feinberg's reasoning, the threshold of public harm that is not yet serious but large enough to legitimate regulation via criminal law is approached if a substantial part of the community[36] engages in a self-harming activity that leads to loss of labor productivity, increased use of public services or other costs involving a public interest.

It was established in section 1.3.3 that the three instances of virtual cybercrime resulting in extravirtual harm to the self that have been discussed throughout this dissertation: namely, gambling on a virtual slot machine, unlicensed practice of medicine through an avatar in *Second Life* (2003) and excessive gaming, can all lead to increased use of public services, which are costs involving a public interest. But is there also a substantial part of the community engaging in them? Internet gambling, including gambling on virtual slot machines in virtual casinos, is a growing concern, especially among adolescents (Derevensky & Gupta 2007, p. 95). For most adolescents gambling is a form of entertainment without serious negative consequences but

[36] According to Feinberg this is somewhere between ten thousand persons and ten percent of the whole population but I assume the starting point depends on the size of the population.

research shows that 18.8% of the adolescent Internet gamblers are pathological gamblers (i.e., their gambling causes harm, including costs involving a public interest) and an additional 22.5% of them is identified as at-risk for pathological gambling (Ibid., pp. 93, 97). The example of unlicensed practice of medicine through an avatar in *Second Life* (2003) was hypothetical, no cases have been reported yet, and, therefore, it cannot be established whether or not a substantial part of the community engages in this activity. Computer and video game addiction is also a growing problem. Studies estimate that 10 % to 15 % of gamers "exhibit signs that meet the World Health Organization's criteria for addiction" (<http://www.video-game-addiction.org>).

If the loss that a virtual cybercrime causes consists of an evil of another kind as intended by legal moralism, there is no such connection. In these cases, the question of whether or not the loss is large enough to legitimate regulation via criminal law should be given separate thought. Consider for example the production, distribution, and possession of virtual child pornography, which results in an evil of another kind (see chapter 4). Whether or not the losses they cause are large enough to legitimate regulation via criminal law is open to debate. Virtual child pornography is frequently compared to *non*-virtual child pornography in this respect. It goes without saying that the losses caused by the production, distribution, and possession of *non*-virtual child pornography, which involve child abuse, are much larger than the losses caused by the production, distribution, and possession of virtual child pornography, in which no actual children are involved. But although some states have reserved the right not to apply the Convention on Cybercrime's prohibition on virtual child pornography, many other states have agreed to incorporate this prohibition in their domestic law and there thus seems to be a broad consensus that the losses caused by virtual child pornography are large enough to legitimate regulation via criminal law tools (see section 4.2). With regard to the production, distribution, and possession of virtual animal pornography there is a lot less consensus on this, for only a couple of countries, e.g., the UK and the Netherlands, prohibit these behaviors (see section 1.1.4).

As was indicated in the last section, special attention needs to be paid to the "overdeterrence problem" when weights are assigned to the costs and benefits of using criminal law to regulate virtual cybercrime. It was explained before that in emerging areas, the scope of criminal law and definitions of criminal activity might be unclear and, therefore, well-meaning and law-abiding individuals and businesses might be afraid that they will violate criminal law when they act out their innovative and creative ideas, where in reality they would not. The overdeterrence problem is of particular relevance with regard to virtual cybercrime which is committed within the virtual environments of computer games, because the wide palette of

opportunities they offer to users fosters a great amount of creativity. In computer games with a pre-designed content, users engage in creative expression primarily through controlling the appearance of their online representations (their avatars), the shape and characteristics of which they can usually customize. In computer games that also allow for content which is not pre-designed, e.g., *Second Life* (2003), users have endless opportunities; they do not only have almost limitless control of their avatars' appearance but they can also craft their own interactive objects and come up with their own storylines (Marcus 2007/2008, pp. 72-75).

The creative opportunities of users within the virtual environments of computer games are in principle protected from the influence of criminal law (Hickman & Hickman 2012, p. 539). As explained in sections 1.2.2 and 2.2.1, there is a kind of metaphorical line, called the ''magic circle'', between the fantasy realms of the virtual worlds of computer games and the non-virtual world. The magic circle entails that conduct that is performed in a (computer) game setting can in principle not be sanctioned by criminal law but is to be sanctioned by the rules of the game instead.

Breaches of the explicit and hard-coded rules of a game are usually sanctioned with a temporary or permanent ban from the game, i.e., a suspension or termination of the user's account (see e.g., the ToS of *Second Life* (2003) or the Terms and Conditions of *RuneScape* (2001)). In addition, players often have the possibility to block other players in order to sanction breaches of community norms inside or outside the game. Blocking entails that the blocked player will not be able to contact the player who blocked him or her anymore via voice chat, text messages etc. (Ibid.). Contrary to civil or administrative sanctions, these sanctions are not aimed at compensation; they seem to be aimed at retribution, just like criminal law. The main reason to (temporarily or permanently) ban or block a user seems to be prevention: a banned or blocked user cannot continue to breach the rules of the game. Since criminal law and the rules of games both serve the goal of retribution, things have to be weighed up differently when it is to be established which of the two is a more appropriate means of regulation than when criminal law is compared with civil or administrative law. After all, civil and administrative law serve a different goal than retribution: namely, compensation. Reasons that make the cost-benefit analysis strike in favor of the use of criminal law when it is weighed against civil or administrative law, because compensation is found to be less appropriate than retribution, do thus not apply when criminal law is compared to the rules of games.

How to make a cost-benefit analysis of regulation via criminal law versus regulation via the rules of games then? As explained in section 2.2.1, an act that is performed in a (computer) game can be brought under the scope of criminal law instead of the rules of the game if it (a)

constitutes such a grave violation of the rules of the game that they do not provide an adequate punishment or (b) if it is (partly) performed outside the game setting. The first type of situation can occur if a player abuses the chat function of a computer game to express racist language. The second type of situation occurred in the two Dutch cases of theft of virtual items in online multiplayer computer games, which I have thoroughly discussed in chapter 2. Both of these cases involved infractions outside the game: in the one case the perpetrators gained access to the virtual items concerned by means of deceit in the non-virtual world, in the other case by means of violence in the non-virtual world. Note that the idea that an act which is (partly) performed outside the game setting should not be regulated by the rules of the game but by criminal law, is similar to the philosophical idea discussed in section 5.1.2 that an act that satisfies the element of causation of a crime extravirtually (i.e., has an extravirtual consequence) should not (only) be regulated by means of the rules of the game but by means of criminal law.

5.2.3 Legal-economic criteria for the criminalization of virtual cybercrime

I will now concretize the above-mentioned legal-economic analysis of virtual cybercrime into absolute and relative negative criteria for its criminalization, which can be used to decide on actual cases. Note that these criteria are in addition to the philosophical criteria for the criminalization of virtual cybercrime as established in section 5.1.4. There is one absolute negative criterion that follows from the current section. It entails that criminalization of a virtual cybercrime should be omitted if the benefits of using criminal law for regulation do not outweigh the costs. In addition, two relative negative criteria for the criminalization of virtual cybercrime can be established. It was claimed that the benefits of using criminal law for regulation will probably outweigh the costs when the losses are diffuse (i.e., because they are difficult to translate into monetary terms or because there is no easy identifiable victim) and relatively large. Contraindications for the criminalization of virtual cybercrime thus arise in the opposite situation: when the losses are clear (i.e., because they are easy to translate into monetary terms or because there is an easy identifiable victim) and relatively small. The clearer and smaller the losses are, the less appropriate it is to regulate the virtual cybercrime concerned by means of criminal law; regulation can then better take place by means of civil or administrative law or, if the act was performed in a game setting, the rules of the game.[37]

[37] I have not included the extra considerations for criminalization that apply when a virtual cybercrime is committed within the virtual environment of a computer game and the rules of the game are thus an alternative for regulation via criminal law, because, as explained above, they overlap with the criteria as established here, and in section 5.1.4.

5.3 Pragmatic dimension

In this section, I will discuss the pragmatic dimension of the question of when virtual cybercrime should be brought under the scope of criminal law. As was indicated in the introduction, this dimension focuses on the overall capacity of the criminal justice system; would it be able to handle the extra workload that the criminalization of virtual cybercrime would bring about? The aforementioned question is a topical one, because virtual cybercrime involves the use of ICTs, which have a couple of features that facilitate crime and hamper law enforcement. Below, I will first discuss these features. I will focus on their meaning for virtual cybercrime. Taking the aforementioned features into account, I will then establish whether or not the criminal justice system would be able to handle the extra workload that the criminalization of virtual cybercrime would bring about. At the end of this section, I will concretize my analysis by establishing pragmatic criteria for the criminalization of virtual cybercrime.

5.3.1 Features of ICTs that facilitate crime and hamper law enforcement

First of all, ICTs and especially the Internet allow crimes to be committed on a scale that could not be achieved offline (Clough 2010, p. 5). Until the last century, crime consisted of unlawful acts that were directed against a single victim or a few victims. Some offenders committed unlawful acts repetitively but their activities remained small-scale (Goodman & Brenner 2002, p. 150). ICTs allow users to communicate with many people all over the world simultaneously (Clough 2010, p. 5). Therefore, crimes involving the use of ICTs can, contrary to traditional forms of crime, be targeted at multiple, geographically dispersed victims at the same time, think for instance of the dissemination of computer viruses (Goodman & Brenner 2002, p. 151).

With regard to virtual cybercrime, consider the following example. In 2012, hackers committed a “gameocide”; they massacred thousands of avatars in the virtual environment of the computer game *World of Warcraft* (2004) in about four hours time. The avatars belonged to players all over the world. In 2005, something similar happened when *World of Warcraft* (2004) was struck by a virtual plague, which was caused by a computer virus (Van Ammelrooy 2012).

Moreover, ICTs allow offenders to automate certain processes by the use of software called “bots”, which means that they can commit even more crimes faster (Clough 2010, p. 5). In the virtual environments of computer games, bots can be used to turn a user's avatar into a robot so that it can act on its own and the user does not need to operate it anymore. Such an autonomously operating avatar can be programmed to commit crimes. In Japan, for example, a

man made his avatar violently rob multiple other avatars in the online computer game *Lineage II* (2004) using a bot (Knight 2005).

Secondly, accessibility plays a role. Nowadays, ICTs are ubiquitous and increasingly easy to use, which ensures their availability to both offenders and victims (Clough 2010, p. 5). The ease of accessibility and searchability of information on the Internet has led to an explosive growth in the amount of information available and the knowledge that can be drawn from it, including information and knowledge that can be exploited for criminal purposes (Council of Europe Convention on Cybercrime, Expl. Report § 4). On the Internet one can, for example, find instructions how to make a bomb, which can be used to carry out a terrorist attack. Instructions how to commit a virtual cybercrime, e.g., how to make virtual child pornographic images or how to kill another user's avatar in the virtual environment of a computer game, can also be found online.

Moreover, offenders who would otherwise be isolated in their offending, can now find like-minded people and form virtual communities to further their offending (Clough 2010, p. 5). As discussed in section 4.3.2, the Internet allows, for instance, pedophiles to form a subculture favoring child abuse, because it is the primary instrument for trading (virtual) child pornographic images and it is also used for other online practices such as the exchange of ideas, fantasies, and advice among pedophiles, which play a role in supporting, encouraging, and facilitating sexual crimes against children (Council of Europe Convention on Cybercrime, Expl. Report § 93, 102). In 2007, there was a lot of fuss about the discovery of "Wonderland": a community within the virtual environment of *Second Life* (2003) where users could, through their avatars, have sex with child-like avatars (see e.g., "Paedophiles Target Virtual World". *SkyNews* 31 October 2007.).[38]

Thirdly, ICTs provide anonymity in a number of ways, which is an obvious advantage for offenders. The networked nature of ICTs in themselves means that data will routinely be routed through a number of nations before reaching their destination, which makes the tracing of communications extremely difficult and time sensitive. Offenders can also deliberately conceal their identity online, for example, by means of the use of spoofed (untraceable) IP addresses. Using wireless networks, with or without authorization, may conceal their identity as well, even if the location can be identified (Clough 2010, pp. 6-7). Moreover, offenders can make use of more advanced technologies such as encryption (coding of information) or steganography (hiding information in an image). Encryption and/or steganography are, for example, sometimes used to distribute (virtual) child pornography (Ibid., p. 250). With regard to virtual cybercrime

[38] Note that this could be seen as the production of entirely computer-generated child pornography as was discussed in chapter 4.

inside a game there only is an anonymity problem when the identity of those who set up a game account is not verified. If users have to pay for certain services by means of a credit card, their identity could be traced back through their credit card details, unless the credit card (number) is stolen.

Fourthly, the portability and transferability of data that ICTs allow for is of importance. ICTs enable users to store enormous amounts of data in a small space and to replicate data without diminution of quality (Clough 2010, p. 7). These opportunities pose a threat to copyrighted materials. The reproduction and dissemination of protected works, e.g., literary, photographic, musical, and audio-visual works, without approval of the copyright holder are extremely frequent on the Internet. The ease with which unauthorized copies can be made and the scale on which they can be disseminated, have made infringements of intellectual property rights, in particular of copyright, the most commonly committed crimes on the Internet (Council of Europe Convention on Cybercrime, Expl. Report § 107). The ability of ICTs to store enormous amounts of data and to replicate them without diminution of quality also facilitates the production, distribution, and possession of (virtual) child pornography; there has been a significant rise in the number of child-pornography prosecutions since ICTs have become more widely available and the Internet more pervasive (Clough 2010, pp. 247-249).

Fifthly, crime involving ICTs (cybercrime) is, contrary to traditional crime, of a global nature (Goodman & Brenner 2002, p. 143). As indicated above, ICTs allow offenders to target their criminal activities at geographically dispersed victims. This does not only provide, literally, a world of opportunity for offenders, it also presents enormous challenges to law enforcement. Criminal law is traditionally regarded as local in nature; it is restricted to the legal territory (the jurisdiction) of the nation which enacted it (Clough 2010, p. 7). The most common basis for the exercise of criminal jurisdiction is the principle of territoriality; nations are entitled to prosecute crimes under their criminal law when these are committed within their territory. But a nation may, for example, also establish jurisdiction when the offender is a national of that nation or when the victim is within its territory (Ibid., pp. 406-407). In the case of cybercrime, this can give rise to competing jurisdictional claims, since the offender and the victim can be in different nations (Ibid., p. 411). If a nation wants to prosecute a person who does not reside in its territory, it needs to request extradition from the nation where that person resides. Extradition is a process whereby one state formally surrenders a person for prosecution in another state. Extradition typically requires that there must be “dual criminality”: the crime must be a crime under the criminal laws of both jurisdictions, usually it also has to be subject to a minimum level of

penalty (Ibid., p. 414). In addition, the complexity and cost of the extradition process ensure that extradition is typically reserved for serious crimes (Ibid., p. 416).

Finally, the features mentioned above have resulted in an absence of capable guardians with regard to cybercrime (i.e., there are not enough qualified policemen to investigate and not enough prosecutors and judges to prosecute cybercrime). Therefore, the perceived risk of detection and prosecution is generally low. The perceived risk of detection and prosecution of a crime is an important factor affecting criminal behavior. When it is high, it acts as a powerful deterrent to commit the crime. When it is low, however, (potential) offenders will be inclined to commit the crime more easily (Clough 2010, pp. 7-8). The amount of (virtual) cybercrimes that will be committed in the future is thus only expected to increase.

5.3.2 Implications for the criminalization of virtual cybercrime

Taking the above-mentioned crime facilitating and law enforcement hampering features that characterize ICTs into consideration, it seems unlikely that the criminal justice system would be able to handle the extra workload that the criminalization of virtual cybercrime would bring about. Due to the scale on which virtual cybercrime can be committed, the numbers of victims are simply too large to identify and, therefore, it will be impossible to prosecute every virtual cybercrime that occurs (Goodman & Brenner 2002, p. 157). The accessibility and searchability of information on the Internet, which can be exploited for criminal purposes, and the possibility for offenders to form virtual communities in order to further their offending, will only increase the scale on which virtual cybercrime can be committed. The portability and transferablity of data, which, among other things, facilitates the production, distribution, and possession of (virtual) child pornography, also adds to that, as does the absence of capable guardians resulting in a low perceived risk of detection and prosecution.

Not only does the scale on which virtual cybercrime can be committed make the identification of each and every victim practically impossible, the identification of the perpetrator might be very difficult as well, since that is a hard and time consuming process if s/he made use of one or more of the anonymity features that ICTs offer. Obviously, prosecution of a virtual cybercrime will be impossible when the perpetrator is unknown. But even if the identity of the perpetrator is revealed, the global nature of virtual cybercrime can still challenge prosecution. When the victims are geographically dispersed, several nations can claim jurisdiction at the same time, which might cause conflicts. And if the perpetrator does not reside

in the nation claiming jurisdiction, prosecution will be dependent on extradition, which is a very complex and costly process.

The above-mentioned problems that stand in the way of prosecuting virtual cybercrime can be avoided, however, by making practical choices in which virtual cybercrimes one will prosecute and which not. Although in some countries, e.g., Germany, the prosecutor is in principle obliged to prosecute every crime reported to him or her, in other countries, e.g., the Netherlands, the prosecutor has the freedom to decide not to prosecute a crime if s/he thinks prosecution is not in the public interest, because it is not feasible or not desirable (articles 167 and 242 Wetboek van Strafvordering). It may, for instance, not be feasible to prosecute a crime if there is a lack of evidence. And it may, for example, not be desirable to prosecute a very minor crime.

Moreover, if an offender has committed multiple crimes the Dutch legal system allows the prosecutor to limit the charge to some crimes, but to inform the court about the other crimes committed in an informal way ("voeging ad informandum"). The court can take these non-charged crimes into account when fixing the sentence, provided that the accused does not deny that s/he committed these crimes and that they can be proven (<http://www.euro-justice.com>). The prosecutor is given these opportunities from an efficiency point of view; when the prosecutor has a choice in which crimes to prosecute and which not, s/he can prevent an overload of the criminal justice system.

Overload of the criminal justice system by the criminalization of virtual cybercrime can thus be prevented if prosecutors make use of the above-mentioned opportunities. They can reduce the number of cases by deciding not to prosecute every virtual cybercrime committed but just a few, in order to set the example. Other cases can be added informally then. The number of cases can be reduced even more if prosecutors choose not to prosecute minor virtual cybercrimes. Also, jurisdictional conflicts and extradition can be avoided if virtual cybercrimes are prosecuted in the nation where the offender resides, although the double criminality principle might still pose a problem then. It should be added, however, that these practical considerations are not the only considerations prosecutors have to take into account, for they should not lose sight of the philosophical and the legal-economic dimension of the question of when virtual cybercrime should be brought under the scope of criminal law, which have been discussed in the previous sections.

5.3.3 Pragmatic criteria for the criminalization of virtual cybercrime

I will now concretize the above-mentioned pragmatic analysis of virtual cybercrime into absolute and relative negative criteria for its criminalization, which can be used to decide on actual cases. Note that these criteria are in addition to the philosophical and legal-economic criteria for the criminalization of virtual cybercrime established in sections 5.1.4 and 5.2.3. There is one absolute negative criterion that follows from the current section. It entails that criminalization of a virtual cybercrime should be omitted if that would overload the criminal justice system.

The following three factors indicate that the criminalization of a virtual cybercrime might overload the criminal justice system and can thus be seen as relative negative criteria or contraindications for criminalization. First, the virtual cybercrime concerned is committed on a tremendous scale. Second, the virtual cybercrime concerned is generally committed by making use of one or more of the anonymity features that ICTs offer. Third, the virtual cybercrime concerned is of a global nature (i.e., victims and perpetrators are geographically dispersed). The more of these factors apply, the more likely it is that regulation of the virtual cybercrime concerned by means of criminal law will overload the criminal justice system and is thus inappropriate. However, as was pointed out at the end of section 5.3.2, prosecutors can avoid that the aforementioned factors overload the criminal justice system by making practical choices in which virtual cybercrimes they will prosecute and which not, provided that they have the opportunity to do so under their legal system.

5.4 Constitutional dimension

In this section, I will study the constitutional dimension of the question of when virtual cybercrime should be regulated by means of criminal law. As was indicated in the introduction, this dimension focuses on the burden that the criminalization of virtual cybercrime imposes on the (fundamental) liberties of citizens. Under constitutional law, the restriction of citizens' liberties always needs justification. This section will be shorter than the other sections, for I will claim that the constitutional dimension of the question of when virtual cybercrime should be regulated by means of criminal law overlaps with the philosophical and legal-economic dimension of that question. Because of this overlap there will be no need to establish constitutional criteria for the criminalization of virtual cybercrime.

5.4.1 Criminal law, the restriction of liberties, and the justification of punishment

Just like Feinberg, whose views were discussed in section 5.1.3, the American legal-philosopher Husak points out that most criminal laws limit or restrict the liberties of citizens. Reasoning from a US perspective, the liberties of citizens can be divided into two kinds: fundamental (i.e., explicitly enumerated in the US Constitution e.g., freedom of speech) and non-fundamental (Husak 2004, p. 115). Husak emphasizes that the restriction of a fundamental or non-fundamental liberty by means of criminal law always needs legitimization.

Under US law the legitimacy of a criminal law that limits a fundamental liberty is evaluated by applying the "compelling state interest" test (Husak 2004, p. 116). This means that the law must be necessary to achieve a compelling government purpose (Ibid.). European countries apply a similar kind of test. The European Convention for the Protection of Human Rights and Fundamental Freedoms states that the liberties that are explicitly enumerated in that Convention can only be restricted by (criminal) law if that is "necessary in a democratic society" to protect certain pressing interests (see e.g., Council of Europe European Convention for the Protection of Human Rights and Fundamental Freedoms, article 10 (2)). The legitimacy of a criminal law that limits a non-fundamental liberty is generally less strictly evaluated. In the US, for example, the legitimacy of a criminal law that limits a non-fundamental liberty is evaluated by applying the "rational basis" test, which means that the law must be substantially related to a legitimated government purpose (Husak 2004, p. 116).

The above-mentioned evaluative tests overlap with Feinberg's liberty-limiting principles as discussed in section 5.1.3. The compelling government purpose, pressing interest or rational basis that legitimates the restriction of a respectively fundamental or non-fundamental liberty by means of criminal law consists of harm (as intended by the harm principle), offense (as intended by the offense principle), harm to the self (as intended by legal paternalism), or an evil of another kind (as intended by legal moralism). The US *Ashcroft v. Free Speech Coalition* case (535 U.S. 234 2002), which was about the question of whether or not the prohibition on virtual child pornography legitimately restricts the freedom of speech, illustrates this, for the case was argued on the basis of arguments grounded in the harm principle (see section 4.2.2).

I want to repeat that some liberty-limiting principles provide a better legitimization than others, however. As stated in section 5.1.3, the validity of the harm principle as a good and relevant reason in support of a penal provision has, to my knowledge, not been denied. The offense principle is widely acknowledged as well. But legal paternalism and especially legal

moralism are contested: they are "at most sometimes (but rarely) good reasons" for the criminalization of conduct (Feinberg 1988, p. 323).

Husak further argues that we should not focus on the interest citizens have in exercising their (non-) fundamental liberties but on the interest they have in not being punished when they exercise these liberties. He believes that, even though a state may have a good reason to restrict a certain liberty, it may lack good reason to subject persons who exercise that liberty "to the hard treatment and stigma inherent in the penal sanction" (Husak 2004, p. 117). Before they bring conduct under the scope of the criminal law, legislators or judiciaries must be reasonably confident that the state would be justified in punishing people who perform that conduct (Ibid., p. 118).

Whether or not it is also justified to subject people who exercise liberties that have been restricted by means of criminal law to the hard treatment and stigma inherent in penal sanctions, is in essence a proportionality issue (i.e., the punishment of a certain crime should be in proportion to the severity of the crime itself). The proportionality issue is also part of the legal-economic dimension of the question of when virtual cybercrime should be regulated by means of criminal law as discussed in section 5.2. After all, from a legal-economic point of view the size of the loss (i.e., the harm, offense, harm to the self, or evil of another kind caused by a crime) must be large enough to legitimate regulation via criminal law, because criminal sanctions lead to costs (in a broad sense), for the defendant him- or herself, his or her family, and society at large.

In section 5.2.2, I suggested that the supplementary principles that guide the application of Feinberg's liberty-limiting principles in practical contexts can be used to determine whether or not the loss a crime causes is large enough to legitimate regulation via criminal law. I would suggest that they can also be used to determine whether or not it is proportional to subject people who exercise liberties that have been restricted by means of criminal law to the hard treatment and stigma inherent in penal sanctions. Note that, as mentioned before in section 5.2.2, the application of legal moralism in practical contexts is not guided by a supplementary principle. If the criminalization of conduct is legitimated on the basis of legal moralism, the proportionality issue must be given separate thought.

In conclusion, the constitutional dimension of the question of when virtual cybercrime should be brought under the scope of criminal law overlaps with the philosophical and legal-economic dimension of that question. Therefore, there is no need to establish separate constitutional criteria for the criminalization of virtual cybercrime.

5.5 Conclusion

In this dissertation, I dealt with the question of when virtual cybercrime should be brought under the scope of criminal law. In the first chapter, I argued that this question belongs to the field of legal ontology (i.e., a particular branch of philosophy) and provided a legal-ontological study of virtual cybercrime. In the second, third, and fourth chapter, I applied my findings from the first chapter to three particular instances of virtual cybercrime (i.e., theft of virtual items, virtual rape, and virtual child pornography) and dealt with specific issues they give rise to. In this last chapter, I argued that the question of when virtual cybercrime should be brought under the scope of criminal law does not only have the aforementioned philosophical but also a legal-economic, a pragmatic, and a constitutional dimension. I summarized the previous chapters which together form the philosophical dimension, discussed the other three dimensions and on the basis of my analyses I established philosophical, legal-economic, and pragmatic absolute and relative negative criteria for the criminalization of virtual cybercrime. Because of the overlap between the constitutional and the philosophical and legal-economic dimension, there was no need to establish separate constitutional criteria for the criminalization of virtual cybercrime.

The absolute negative criteria indicate when criminalization of virtual cybercrime should be omitted. The relative negative criteria are contraindications for criminalization; the more of them apply, the less appropriate it is to criminalize the virtual cybercrime concerned. Below, I will establish whether or not the philosophical, legal-economic, and pragmatic absolute and relative negative criteria for criminalization apply to the (putative) instances of virtual cybercrime discussed throughout this dissertation. They include the three above-mentioned instances of virtual cybercrime this dissertation focuses on: namely, theft of virtual items, virtual rape and the production, distribution, and possession of virtual child pornography.

As established in section 5.1.4, the philosophical absolute negative criteria entail that criminalization of a virtual cybercrime should be omitted if it does not have an extravirtual consequence at all or if its extravirtual consequence cannot be brought under the scope of one of Feinberg's liberty-limiting principles (i.e., the harm principle, the offense principle, legal paternalism, or legal moralism). Contraindications (philosophical relative negative criteria) for the criminalization of a virtual cybercrime arise when it does not result in extravirtual harm (as intended by the harm principle), offense (as intended by the offense principle), harm to the self (as intended by legal paternalism), or an evil of another kind (as intended by legal moralism). The more of the aforementioned philosophical relative negative criteria are met, the less (acceptable) liberty-limiting principle is applicable and the less appropriate it is to criminalize

the virtual cybercrime concerned, for, to my knowledge, no writer in legal philosophy denies the validity of the harm principle as a good and relevant reason in support of a penal provision and most writers acknowledge the offense principle as well but legal paternalism and especially legal moralism are contested.

Most (putative) instances of virtual cybercrime discussed throughout this dissertation result in an extravirtual consequence which can be brought under the scope of one of Feinberg's liberty-limiting principles, which means neither of the philosophical absolute criteria applies. The majority results in an extravirtual consequence which can be brought under the scope of the harm principle (i.e., Feinberg's first liberty-limiting principle). They will be summed up below.

First, the "killing" (deleting) of an avatar in the virtual world of *MapleStory* (2003), which counts as the deterioration of computer data without right in the non-virtual world, results in extravirtual harm to property (see section 1.2.2). Second, the posting of a computer-generated animation designed to trigger seizures in both photosensitive and pattern-sensitive epileptics on the Epilepsy Foundation's website results in extravirtual bodily harm (see section 1.3.1). Third, the sexual harassment of Ailin Graef, whose avatar was swarmed by flying pink phalluses and photographs of Graef herself that were digitally altered to make her look like she was holding a giant phallus in the virtual world of *Second Life* (2003), results in extravirtual mental harm (Ibid.). Fourth, the threat to shoot up a local high school a US teen made through the chat function of an online multiplayer computer game results in extravirtual harm to security (Ibid.). Fifth, the publication of an image that is digitally altered or generated to show a public person, e.g., a Prime Minister, kissing another woman than his wife would result in extravirtual harm to reputation (Ibid.). Sixth, the defamation of an avatar through which a person makes real money in a virtual world, e.g., the avatar of *Second Life's* millionaire Ailin Graef, can result in an extravirtual economic harm if the defamation reduces the credibility of the avatar so that no one is willing to do business with it anymore (see section 1.3.1). Seventh, the hitting, kicking, or otherwise physically hurting of a person in a (future) virtual reality environment would result in extravirtual bodily harm (see section 1.3.5). Eighth, theft of virtual items results in extravirtual harm to property, provided that the items represent extravirtual (pecuniary or hedonistic) value (see chapter 2). Ninth, virtual rape in a virtual reality environment involving a haptic device or robotics results in extravirtual harm to bodily integrity, and virtual rape in a virtual world can result in extravirtual harm to mental health (see chapter 3).

A couple of (putative) instances of virtual cybercrime discussed throughout this dissertation result in an extravirtual consequence which can be brought under the scope of one of Feinberg's other, less commonly acknowledged, liberty-limiting principles. Two (putative)

instances of virtual cybercrime discussed throughout this dissertation result in extravirtual offense as intended by the offense principle (i.e., Feinberg's second liberty-limiting principle): namely, the publication of a digitally altered image of a teenage shooting victim and making one's avatar do the Nazi salute when it meets a black avatar in a virtual world (see section 1.3.2). Three (putative) instances of virtual cybercrime discussed throughout this dissertation result in extravirtual harm to the self as intended by legal paternalism (i.e., Feinberg's third liberty-limiting principle). First, gambling on a virtual slot machine in a virtual casino can result in an economic harm to the self if one looses non-virtual money (see sections 1.1.4, 1.2.2, and 1.3.3). Second, the unlicensed practice of medicine through an avatar in *Second Life* (2003) could result in extravirtual bodily harm to the self (see section 1.3.3). Third, excessive gaming also results in extravirtual bodily and/or mental harm but there is no law which prohibits that (Ibid.). Two (putative) instances of virtual cybercrime discussed throughout this dissertation result in extravirtual offense at bare thought, which is an evil of another kind as intended by legal moralism (i.e., Feinberg's fourth liberty-limiting principle): namely, the production, distribution, and possession of virtual animal pornography (see sections 1.1.4 and 1.3.4) and virtual child pornography (see chapter 4).

Throughout this dissertation I also discussed several (putative) instances of virtual cybercrime to which one or both philosophical absolute criteria do apply. The first philosophical absolute criterion applies to the following three (putative) instances of virtual cybercrime discussed throughout this dissertation, because they do not result in an extravirtual consequence at all. First, the production, trading, and possession of the drug Seclimine in the virtual world of *Second Life* (2003) (see section 1.2.2). Second, the driving of a motorcycle without a safety helmet, swimming at an unguarded beach, committing suicide or dueling through an avatar in a virtual world (see section 1.3.3). Third, "cross-world" bigamy i.e., being married to one person in the non-virtual world and another person in the virtual world of *Second Life* (2003) (see section 1.3.4).

The second philosophical absolute criterion applies to the following four (putative) instances of virtual cybercrime discussed throughout this dissertation, because they result in an extravirtual consequence that cannot be brought under the scope of one of Feinberg's liberty-limiting principles. First, the sexual harassment of Monica Kanto in the virtual world of *Second Life* (2003), whose in-world neighbor covered his land with giant purple phalluses, results in extravirtual mental harm but since the aforementioned act would probably not have the same effect on the standard person, it cannot be brought under the scope of the harm principle (see section 1.3.1). Second, the stalking, unauthorized filming or unauthorized photography of avatars

in a virtual world, e.g., "upskirt pictures", result in a harm to privacy which may spill into the non-virtual world when the perpetrator knows who the person behind the avatar is, but generally there will not be enough well-being under threat to invoke the harm principle (Ibid.). Third, assault or torture of an avatar can be felt as mental harm to the person behind it when that person is attached to and identifies with his or her avatar, but generally there will not be enough well-being under threat here to invoke the harm principle either (Ibid.). Finally, prostitution in *Second Life* (2003) or *The Sims* (2000), which counts as pornography in the non-virtual world, is not serious enough to invoke the offense principle (see sections 1.3.2 and 1.3.4).

As established in section 5.2.3, the legal-economic absolute negative criterion entails that criminalization of a virtual cybercrime should be omitted if the benefits of using criminal law for regulation do not outweigh the costs. The benefits of using criminal law for regulation are likely to outweigh the costs when the losses are diffuse (i.e., because they are difficult to translate into monetary terms or because there is no easy identifiable victim) and relatively large. Contraindications (legal-economic relative negative criteria) for the criminalization of virtual cybercrime thus arise in the opposite situation: when the losses are clear (i.e., because they are easy to translate into monetary terms or because there is an easy identifiable victim) and relatively small. The clearer and smaller the losses are, the less appropriate it is to regulate the virtual cybercrime concerned by means of criminal law; regulation can then better take place by means of civil or administrative law or, if the act was performed in a game setting, the rules of the game. Most (putative) instances of virtual cybercrime discussed throughout this dissertation result in losses to which neither the first, nor the second legal-economic relative criterion applies, which means that the legal-economic absolute criterion does not apply to them either.

The first economic relative criterion does not apply to any of the (putative) instances of virtual cybercrime mentioned above which cause extravirtual harm to bodily integrity or mental health, because they result in a loss that is not clear but diffuse, as (mental or bodily) pain is difficult to translate into monetary terms (see sections 5.2.1 and 5.2.2). A loss that consists of extravirtual offense (i.e., all kinds of disliked mental states such as disgust, shame, embarrassment, and fear) is difficult to translate into monetary terms as well. At first sight, the extravirtual harm caused by theft of virtual items seems easy to translate into monetary terms and, therefore, clear; after all the perpetrator could simply reimburse the victim for the loss of property. However, the loss caused by theft does not solely lie in the loss of property but also and merely in the form of appropriation, which constitutes a significant breach of trust, and that loss is difficult to translate into monetary terms and, therefore, diffuse (Steel 2008, pp. 726-727). A similar line of reasoning applies to the killing (deleting) of an avatar through hacking, which

counts as the deterioration of computer data without right in the non-virtual world (see section 1.2.2), for the loss does not solely lie in the loss of the avatar but also in the way of accessing the avatar, i.e., without right, which constitutes a significant breach of trust as well.

The production, distribution, and possession of virtual child and animal pornography also result in diffuse losses, because there is no easy identifiable victim or actually no victim at all: they are victimless crimes (see sections 1.1.4, 1.3.4, 4.2.2 and 5.2.2). Bedau includes crimes that cause harm to the perpetrator him- or herself, e.g., gambling (on a virtual slot machine in a virtual casino), into the definition of victimless crimes (Bedau 1974, p. 61, 85). This means that these crimes also result in a diffuse loss, because there is no easy identifiable victim or at least not a victim who can be compensated, which is the aim of (most) other means of regulation than criminal law, for a person cannot compensate him- or herself.

The only (putative) virtual cybercrimes to which the first legal-economic relative negative criterion for criminalization might apply, are those that result in extravirtual harm to reputation (defamation). Consider the two examples of defamation mentioned above. It was stated that the defamation of an avatar through which a person makes real money in a virtual world, e.g., the avatar of *Second Life's* millionaire Ailin Graef, can ultimately result in an extravirtual economic harm, if the defamation reduces the credibility of the avatar so that no one is willing to do business with it anymore (see section 1.3.1). This is not a diffuse loss, because it is easy to translate into monetary terms, for the person can be compensated for the foregone earnings. It was also mentioned that the publication of an image that is digitally altered or generated to show a public person, e.g., a Prime Minister, kissing another woman than his wife, would result in extravirtual harm to reputation (Ibid.). This loss is not easy to translate into monetary terms. The latter case of defamation should thus be regulated by means of criminal law; the first can better be regulated by other means, provided that the loss is relatively small. In most jurisdictions defamation can be treated both as a crime and as a civil wrong (see <http://legal-dictionary.thefreedictionary.com>).[39]

When they result in harm or offense, the question of whether or not the second legal-economic relative negative criterion applies to the above-mentioned (putative) instances of virtual cybercrime overlaps with the question of whether or not the second philosophical absolute criterion applies to them. If the loss that a virtual cybercrime causes is large or serious enough to invoke the harm or offense principle, it is also large enough to justify regulation via criminal law. If a virtual cybercrime results in harm to the self, there is a slightly different connection, for here, it is not the extravirtual harm to the self but the public interest involved that

[39] In the Netherlands, for example, libel can be prosecuted as a crime (article 261 Wetboek van Strafrecht) but it can also be treated as a civil wrong (article 6:162 Burgerlijk Wetboek).

must be large enough to legitimate regulation via criminal law. The public interest is large enough to legitimate regulation via criminal law if a substantial part of the community engages in the self-harming activity and it leads to loss of labor productivity, increased use of public services or other costs involving a public interest (see section 5.2.2).

All of the abovementioned (putative) instances of virtual cybercrime resulting in extravirtual harm to the self can lead to increased use of public services such as mental health, primary health and criminal justice (see section 1.3.3). Both gambling and computer and video game addiction are prevalent in current society and, therefore, it can be concluded that a substantial part of the community engages in these self-harming activities. The example of unlicensed practice of medicine through an avatar in *Second Life* (2003) was hypothetical, no cases have been reported yet, and, therefore, it cannot be established whether or not substantial part of the community engages in this activity (see section 5.2.2).

If a virtual cybercrime results in an evil of another kind, the question of whether or not the second legal-economic relative negative criterion applies, needs to be given separate thought (see section 5.2.2). With regard to the first instance of virtual cybercrime resulting in an evil of another kind that has been discussed in this dissertation - the production, distribution, and possession of virtual child pornography - there seems to be a broad consensus that the losses are large enough to legitimate regulation via criminal law tools, for these behaviors are commonly prohibited. With regard to the second - the production, distribution, and possession of virtual animal pornography - there is a lot less consensus on this, for only a couple of countries, e.g., the UK and the Netherlands, prohibit these behaviors (Ibid.).

As established in section 5.3.3, the pragmatic absolute negative criterion entails that criminalization of a virtual cybercrime should be omitted if that would overload the criminal justice system. Contraindications (pragmatic relative negative criteria) for the criminalization of a virtual cybercrime arise when it is committed on a tremendous scale, generally committed by making use of one or more of the anonymity features that ICTs offer, or if the virtual cybercrime is of a global nature (i.e., victims and perpetrators are geographically dispersed). The more of these criteria apply, the more likely it is that regulation of the virtual cybercrime concerned by means of criminal law will overload the criminal justice system and this is thus inappropriate.

Whether or not the pragmatic relative negative criteria apply to the above-mentioned (putative) instances of virtual cybercrime depends on the specific case. As stated in the introduction, the field of virtual cybercrime is largely unexplored. Only a handful of virtual cybercrimes have been brought under the scope of criminal law. Therefore, I was not able to discuss many specific cases of virtual cybercrime in this dissertation; most examples are either

hypothetical or never went to court, which means there are not much details available. The only instances of virtual cybercrime that went to court and were discussed in detail in this dissertation are the two Dutch cases of theft of virtual items in the virtual worlds of the online multiplayer computer games *Habbo* (2001) and *RuneScape* (2001) (see chapter 2). As will be explained below, none of the pragmatic relative negative criteria apply to them, which means the pragmatic absolute criterion does not apply either.

Both of these cases concerned single incidents; the thefts were thus not committed on a tremendous scale. As far as I am aware the perpetrators did not make use of (many of) the anonymity features that ICTs offer. In the *Habbo* case the perpetrators made use of phishing techniques in order to accomplish the theft (see chapter 2, introduction). The verdict does not mention the use of any anonymity features. It does mention that the IP-address the perpetrators mainly used, belonged to the home computer of one of them, which means they must have been easy to track down (Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791). In the *RuneScape* case the perpetrators did not make use of ICTs at all to accomplish the theft; they made use of physical violence instead (see chapter 2, introduction). Finally, the victims and perpetrators were not geographically dispersed: they resided in the same country. In conclusion, the pragmatic absolute negative criterion does not apply to these instances of virtual cybercrime either: their prosecution did not overload the criminal justice system.

There is one general conclusion that can be drawn with regard to the applicability of the pragmatic relative negative criteria. The third pragmatic relative negative criterion (i.e., the question of whether or not the victims and perpetrators are geographically dispersed) never applies to victimless crimes such as the production, distribution, and possession of virtual child or animal pornography. The same is true for instances of virtual cybercrime which result in extravirtual harm to the self, since victim and perpetrator are then the same person, except for instances of unlicensed practice of medicine, where there are two persons involved: the unlicensed practitioner and the client or patient.

Throughout this dissertation I also discussed two (putative) instances of virtual cybercrime to which one of the pragmatic relative negative criteria applies. Both the "gameocide" that took place in the virtual world of *World of Warcraft* (2004) and the multiple violent robberies that took place in the virtual world of *Lineage II* (2004) were committed on such a tremendous scale that prosecution of every single killing or robbery would overload the criminal justice system, which means the pragmatic absolute negative criterion applies to them as well (see section 5.3.1). However, as will be explained below, it does not need to be an

insurmountable problem if the aforementioned or one of the other pragmatic relative negative criteria apply, for there might be practical solutions available.

Provided that they have the opportunity to do so under their legal system, prosecutors can make practical choices in which virtual cybercrimes they will prosecute and which not. They can, for example, reduce the number of cases by deciding not to prosecute every virtual cybercrime committed but just a few, in order to set the example. Others can be added informally then. The number of cases can be reduced even more if prosecutors choose not to prosecute minor virtual cybercrimes. Also, jurisdictional conflicts and extradition can be avoided if virtual cybercrimes are prosecuted in the nation where the offender resides, although the double criminality principle might still pose a problem then. Despite these solutions, the pragmatic absolute and relative negative criteria remain likely to apply to instances of virtual cybercrime and are thus the biggest hindrance when we want to bring virtual cybercrime under the scope of criminal law (see section 5.3.2).

In conclusion, virtual cybercrime should not be brought under the scope of criminal law when the absolute negative criteria for criminalization apply. The more relative negative criteria for criminalization apply, the less appropriate it is to bring virtual cybercrime under the scope of criminal law. This dissertation presents several examples of (putative) virtual cybercrimes to which the philosophical and legal-economic absolute negative criteria for criminalization do in principle not apply. Whether or not the pragmatic absolute negative criterion for criminalization applies to them, depends on the specific case. In general, the aforementioned criterion more often applies to instances of virtual cybercrime than the other two and is, therefore, the biggest hindrance when we want to bring virtual cybercrime under the scope of criminal law.

It is important to add that countries can decide differently on the applicability of the absolute and relative negative criteria for criminalization to a specific instance of virtual cybercrime. As stated before in section 1.2.4, criminal law does not contain everywhere and at any time penal provisions defining crimes in the same way. The core of criminal law, across geography and across time, consists of crimes that produce direct and serious harm to individual persons or groups. Penal provisions based on the offense principle, legal paternalism, and especially legal moralism deviate across geography and across time (Goodman & Brenner 2002, p.178).

EPILOGUE

In this dissertation, I studied the question when virtual cybercrime should be brought under the scope of criminal law. At the end of this journey, the question arises how to go forward. In this epilogue I will formulate forward-looking policies with regard to virtual cybercrime. I will also state suggestions for future research.

Forward-looking policies

I suggest that, from now on, the framework I have set up in this dissertation is used to decide when virtual cybercrime should be brought under the scope of criminal law. I repeat that the framework consists of philosophical, legal-economic, and pragmatic absolute and relative negative criteria for criminalization. The absolute negative criteria indicate when criminalization of virtual cybercrime should be omitted. The relative negative criteria are contraindications for criminalization; the more of them apply, the less appropriate it is to criminalize the virtual cybercrime concerned. They can be found in the table below.

	Absolute negative criteria for criminalization	**Relative negative criteria for criminalization**
Philosophical dimension	Criminalization of a virtual cybercrime should be omitted if (1) it does not have an extravirtual consequence at all or (2) if its extravirtual consequence cannot be brought under one of Feinberg's liberty-limiting principles (i.e., the harm principle, the offense principle, legal paternalism, or legal moralism).	Contraindications for the criminalization of a virtual cybercrime arise when it does not result in (1) harm (as intended by the harm principle), (2) offense (as intended by the offense principle), (3) harm to the self (as intended by legal paternalism), or (4) an evil of another kind (as intended by legal moralism).
Legal-economic dimension	Criminalization of a virtual cybercrime should be omitted if the benefits of using criminal law for regulation do not outweigh the costs.	Contraindications for the criminalization of a virtual cybercrime arise when the loss is (1) clear (i.e., because it is easy to translate into monetary terms or because there is an easy identifiable victim) and (2) relatively small.

Pragmatic dimension	Criminalization of a virtual cybercrime should be omitted if that would overload the criminal justice system.	Contraindications for the criminalization of a virtual cybercrime arise when it is (1) committed on a tremendous scale, (2) committed by means of one or more of the anonymity features that ICTs offer or (3) is of a global nature.

Table 3 Absolute and relative negative criteria for criminalization

In order to check whether or not my framework functions satisfactorily, I will now discuss two (putative) instances of virtual cybercrime that have not been discussed before. I will test them against the above-mentioned criteria and decide whether or not they should be brought under the scope of criminal law.

Case 1: Holocaust Tycoon

There is an Internet hoax claiming a German company has developed an online computer game titled *Holocaust Tycoon*. Players would successfully have to manage a World War II concentration camp whilst avoiding the attention of invading Allied Forces. There even is a demo of this fake game available on *YouTube*. It consists of a computer-simulated video of a concentration camp with an arch stating "Jews only" and gas ovens with smoking chimneys. At a certain moment the text "Looks like most of them have been dealt with, there were a lot more here, earlier" appears (http://www.youtube.com/watch?v=guqM9Deqqaw). Should the dissemination of this video, which is a human act made possible by computer simulation, be brought under the scope of criminal law?

The dissemination of the video described and depicted above results in an extravirtual consequence, for it is likely to offend the person who is confronted with it. Offense can be brought under the scope of Feinberg's second liberty-limiting principle, which is commonly acknowledged. The philosophical absolute negative criteria do thus not apply.

As was noted in section 5.4, a loss that consists of offense is difficult to translate into monetary terms, which means that it is not clear but diffuse and that the first economic relative negative criterion does not apply. The second economic relative negative criterion does not apply either, for only relatively large offenses are serious enough to invoke the offense principle, especially on the Internet. As mentioned in section 1.3.2, the seriousness of the offense caused (e.g., its intensity and duration) has to be balanced against the independent reasonableness

(avoidability) of the offender's conduct when the offense principle is invoked. On the Internet, the degree of avoidability is high. After all, one can always choose not to visit a particular website or turn off the computer. Therefore, only the most serious offenses can tip the scales. The dissemination of racist material is among the most serious offensive behaviors we know and frequently committed through computer systems. On the international level, it is prohibited by the Additional Protocol to the Convention on Cybercrime (see section 1.1). This Protocol explicitly includes in its scope the dissemination of material which denies, grossly minimizes, approves or justifies acts constituting genocide or crimes against humanity such as the serious crimes that occurred during World War II. The video at stake belongs to this category. Since both economic relative negative criteria do not apply, we can conclude the economic absolute negative criterion does not apply either.

All three pragmatic relative negative criteria might apply. As far as I am aware, the video at stake has not been published on a tremendous scale. As mentioned before, it can be found on *YouTube* ("Second Life Seclimine VB Sample". *YouTube* 16 May 2007.). But due to the global nature of the Internet, there are potentially millions of people who can be confronted with and offended by this video.

The global nature of the dissemination of this video is also problematic from another point of view. Not all countries have ratified the Additional Protocol to the Convention on Cybercrime, which, as mentioned above, prohibits this type of material. Not every country will thus have an applicable penal provision. In the US, for example, the dissemination of a video like this is not illegal (Brenner 2008, p. 95). This means that, if the perpetrator is a US citizen, not only prosecution in the US but also extradition to a country where the aforementioned behavior is illegal, are impossible.

It cannot be established whether or not the perpetrators have made use of one or more of the anonymity features that ICTs offer without a police investigation, which has, as far as I am aware, not (yet) been conducted. But it is definitely possible. The video could, for instance, be put on *YouTube* using a spoofed (untraceable) IP address. Since all three pragmatic relative negative criteria might apply, the pragmatic absolute negative criterion might apply as well.

In conclusion, the dissemination of the demo of the fake online computer game *Holocaust Tycoon* should be brought under the scope of criminal law from a philosophical and legal-economic point of view but from a pragmatic point of view prosecution might not be feasible. Especially the global nature of this human act made possible by computer simulation constitutes a problem.

Case 2: The World of Warcraft funeral massacre

Many authors in the areas of computer ethics and law discuss the *World of Warcraft* (*WoW*) funeral massacre (see e.g., Humphreys & De Zwart 2012, pp. 525-527). In short, this incident is about a group of *WoW* players (a "guild") which had one of its long-standing members die in real life and decided to hold a memorial service for her in the virtual world of the game. Another guild disrupted the memorial service when they swarmed into it and massacred the avatars of the mourning guild, which deeply grieved them (Ibid., p. 525). Should the disruption of a memorial service held in *WoW* by means of massacring the avatars present, which is a computer-simulated human act, be brought under the scope of criminal law?

For reasons of clarity, it should first be noted that in many countries, the disruption of a memorial service would not be illegal, although it would probably be considered immoral. In these jurisdictions the question of whether or not the event described above could be brought under the scope of (existing) criminal law would thus not arise at all. But some countries, e.g., the USA, prohibit the disruption of funerals of (former) members of the armed forces (18 USC § 1388 and 38 USC § 2413) or civilians (under the law of certain US States). These laws seek to protect the dignity of (military) funerals, the privacy of the attendees and their emotional well-being (Ruane 2011, p. 5).

The *WoW* funeral massacre resulted in an extravirtual consequence: namely, grief, which can be considered mental harm. But can it also be brought under the scope of the harm principle (i.e., Feinberg's first liberty-limiting principle)? It was established in section 1.2.4 that harm, as intended by the harm principle, can be defined as a wrongful setback to interest. The grief or mental harm caused by the *WoW* funeral massacre can be seen as a setback to the interest in emotional wellbeing of the members of the mourning guild. It is questionable, however, whether or not this setback was wrongful.

According to the rules of *WoW* the massacre was legitimate. The members of the mourning guild either expected that other players would consent to a temporary rule change (i.e., no killing during the memorial service) or agree that a real-world norm (i.e., the prohibition on the disruption of funerals that some countries apply) would overrule the rules of the game. Whether or not the setback to the interest in emotional wellbeing caused by the *WoW* funeral massacre was wrongful, depends on the reasonableness of that expectation (Humphreys & De Zwart 2012, p. 526).

I wish to argue that the above-mentioned expectation was not reasonable. In chapter two I discussed the Dutch convictions for theft of virtual items in the virtual worlds of the online

multiplayer computer games *Habbo* (2001) and *Runescape* (2001). I claimed that the perpetrators in these cases crossed the metaphorical line of the magic circle (i.e., the line between the fantasy realms of the virtual worlds of computer games and the non-virtual world), because they committed the thefts through infractions outside the game (respectively phishing and violence). In the *WoW* funeral massacre case it was the other way around: the alleged victims crossed the metaphorical line of the magic circle, because "they brought real-world issues into the gamespace without the consent of other players" (Humphreys & De Zwart 2012, p. 526). Since the alleged perpetrators did not cross the metaphorical line of the magic circle themselves, they could not reasonably expect that criminal law would apply instead of the rules of the game and it should not be applied either.

In conclusion, the second philosophical absolute negative criterion applies, for the grief or mental harm caused by the *WoW* funeral massacre does not constitute harm as intended by the harm principle. Therefore, this event should not be brought under the scope of criminal law.

Concluding remarks

In conclusion, my framework of absolute and relative criteria for the criminalization of virtual cybercrime provides a clear (respectively: positive and negative) answer to the question of whether or not the two (putative) instances of virtual cybercrime discussed above should be brought under the scope of criminal law.

Suggestions for Future Research

As was indicated in the introduction to this dissertation, the field of virtual cybercrime is largely unexplored. This dissertation provides one of the first explorations but more research is required. During the process of writing this dissertation, I came across two particular areas where (empirical) data are lacking. They will be discussed below.

At the end of chapter two, I came to the conclusion that it is unclear how to measure the amount of hedonistic (non-pecuniary) value that a particular virtual item represents for a particular player. Further discussion and analysis from academics in the fields of computer ethics, law, and psychology are required. The amount of hedonistic value a virtual item represents is of importance, because it determines whether or not that item can count as an object that can be stolen under criminal law. As argued previously, the stealing of a virtual item can

only be brought under the scope of the prohibition on theft if that item represents real, non-virtual value.

The issue of virtual child pornography, which was discussed in chapter four, is in need of further research in the field of psychology/psychiatry, for it remains unclear whether or not entirely computer-generated child pornography can encourage or seduce pedophiles to commit child abuse. If so, the prohibition on the production, distribution, and possession of virtual child pornography could be legitimated by legal paternalism instead of legal moralism. The former is a more acceptable ground for criminalization than the latter.

Furthermore, this dissertation shows that the criminalization of (virtual) cybercrime is problematic from a pragmatic point of view. Further legal research is needed in order to establish how to overcome the pragmatic problems the prosecution of (virtual) cybercrime gives rise to. Especially the global nature of (virtual) cybercrime deserves attention. It was established in section 1.2.4 that, although the core of criminal law is similar everywhere, there are differences across countries and across societies in how criminal behaviors are viewed and treated. In section 3.3, I concluded, for example, that countries apply different definitions of rape, which means that virtual rape in a virtual reality environment involving a haptic device or robotics counts as the crime of rape in some countries but as another crime in others. And I came across many behaviors which are treated as crimes in some countries but not in others (e.g., gambling, bigamy, prostitution, pornography, and the disruption of funerals). Given its global nature, this particularly hampers the prosecution of (virtual) cybercrime.

SUMMARY

The advent of computer technology has given rise to a new type of crime: cybercrime, which can, in broad terms, be defined as crime that involves the use of computers or computer networks. Examples of cybercrime are hacking (in legal terms: illegal access) and e-fraud.
The newest generation of cybercrime is virtual cybercrime. Virtual cybercrime involves a specific aspect of computers or computer networks: namely, virtuality, which can in essence be described as computer simulation.

Consider, for example, the prohibition on virtual child pornography (Council of Europe Convention on Cybercrime, article 9). Virtual child pornography does not consist of photographs or film material of real children engaged in sexually explicit conduct but of computer-simulated children, for the images are photoshopped or even entirely computer-generated (Council of Europe Convention on Cybercrime, Expl. Report § 101). And in the Netherlands, for instance, several minors were convicted of theft for stealing virtual items in the virtual worlds of the online multiplayer computer games *Habbo* (2001) and *RuneScape* (2001) (Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791; Gerechtshof Leeuwarden, 10 November 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764). The latter case was ultimately decided by the highest court in the Netherlands (Hoge Raad, 31 January 2012, ECLI: NL: HR: 2012: BQ9251). A case that was never brought to court but highly debated in the media and in (legal) academic literature is the "virtual rape" (rape of an avatar, i.e., a user's virtual representation in a computer game) that was described by Julian Dibbell in the New York newspaper the *Village Voice* as early as 1993.

The field of virtual cybercrime is largely unexplored. Only a handful of virtual cybercrimes have been brought under the scope of criminal law; they include the production, distribution, and possession of virtual child pornography and theft of virtual items. In addition, there are a couple of putative virtual cybercrimes that have been discussed in the media or (legal) academic literature; they include the above-mentioned example of virtual rape. This dissertation explores the field of virtual cybercrime, mainly from a philosophical point of view but other viewpoints (i.e., a legal-economic, a pragmatic, and a constitutional viewpoint) are also briefly taken into account. It focuses on the question when virtual cybercrime should be brought under the scope of criminal law.

The structure is as follows. This dissertation is divided into three parts: an introductory chapter (part I), three case studies (part II), and a reflection (part III). In total there are five

chapters and an epilogue. The first chapter is the introductory chapter; the three case studies form chapter 2, 3, and 4, and, finally, the reflection constitutes chapter 5.

The first chapter provides a legal-ontological study of virtual cybercrime. Drawing from (interpretations of) the work of the American philosopher Searle (Searle 1995; Searle 2001; Searle 2010), I argue in this chapter that virtual cybercrime should only be brought under the scope of criminal law if it has an extravirtual consequence (i.e., a consequence outside its virtual environment). Not any extravirtual consequence suffices, however: it needs to be of such a nature that it falls under the scope of one of the liberty-limiting principles (i.e., the harm principle, the offense principle, legal paternalism, or legal moralism) that have been distinguished by the legal philosopher Feinberg in his famous work *The Moral Limits of the Criminal Law* (1984, 1985, 1986, 1988). In the second, third, and fourth chapter, I apply these findings to the three particular instances of virtual cybercrime mentioned before; namely, theft of virtual items, virtual rape, and virtual child pornography.

The second chapter takes the Dutch convictions for theft of virtual items in the virtual worlds of the online multiplayer computer games *Habbo* (2001) and *RuneScape* (2001) as a starting point (Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791; Hoge Raad, 31 January 2012, ECLI: NL: HR: 2012: BQ9251). In this chapter I argue that the act of stealing (a) virtual item(s) in the virtual world of an online multiplayer computer game results in extravirtual harm as intended by the harm principle (i.e., Feinberg's first liberty-limiting principle) and can, therefore, be brought under the scope of the prohibition on theft, if the virtual item(s) stolen can be considered another player's valuable property in the non-virtual world. The value the property represents can be pecuniary or hedonistic.

In the third chapter I distinguish between two types of virtual rape: virtual rape in a virtual world, like Dibbell described, and virtual rape in a (future) virtual reality environment through a haptic device or robotics. Both can do extravirtual harm (as intended by the harm principle): the first may emotionally hurt the user; the latter results in an injury to the user's bodily integrity. According to my framework, they should thus be brought under the scope of criminal law but it is questionable whether they can count as the crime of rape. I study both types of virtual rape in light of three categories of legal philosophical theories on the nature of rape; namely, conservative, liberal, and feminist theories. I come to the conclusion that virtual rape in a virtual reality environment involving a haptic device or robotics can be seen as the crime of rape as interpreted by liberal theories on the nature of rape which have shaped the prohibition on rape in many, though not in all countries. Virtual rape in a virtual world cannot be seen as the crime of rape as interpreted by liberal theories but it can be seen as the crime of rape as

interpreted by feminist theories on the nature of rape which criticize liberal theories. Virtual rape in a virtual world also re-actualizes the conservative view on the nature of rape which used to dominate the law in the Middle Ages. Virtual rape in a virtual world can thus not count as the crime of rape under current law, unless the law is changed according to feminist theories. But such a radical change of the law is not necessary to make virtual rape in a virtual world count as a crime in contemporary society. Sometimes, a virtual act counts as one crime within its virtual environment and as another crime in the non-virtual world. I claim that this is the case with regard to virtual rape in a virtual world. Although it cannot count as rape in the non-virtual world under current law, it can be brought under the scope of another penal prohibition: namely, the prohibition on sexual harassment.

The fourth chapter is about virtual child pornography. Its focus is on entirely computer-generated child pornographic images. As opposed to *non*-virtual child pornographic images, these images do not involve a child really engaged in sexually explicit conduct and, therefore, the production, distribution, and possession thereof do not involve (the profiting from) child abuse. They are "victimless crimes" (as described by Bedau 1974) to which the harm principle does not apply. According to Bedau, the criminalization of victimless crimes is based on either legal paternalism or legal moralism (Bedau 1974, p. 75). Drawing from virtue ethics and feminism, I argue that the production, distribution, and possession of entirely computer-generated child pornographic images belong to the rare class of behaviors which can legitimately be prohibited on the basis of legal moralism. They result in offense at bare thought, because entirely computer-generated child pornographic images flout our sexual mentality, which is based on equality. Offense at bare thought is considered an immorality and falls under the scope of legal moralism (Feinberg 1988, p. 15). If (more) research could provide (more) evidence in the future that entirely computer-generated child pornographic images can encourage or seduce children to engage into harmful sexual contacts with adults or pedophiles to commit child abuse, the prohibition of these images could be based on legal paternalism. This would be a stronger ground for prohibition. However, research has not come that far yet.

In the fifth chapter, I argue that the question when virtual cybercrime should be brought under the scope of criminal law does not only have the philosophical dimension discussed so far in the dissertation, but also a legal-economic, a pragmatic, and a constitutional dimension. The legal-economic dimension of the question when virtual cybercrime should be brought under the scope of criminal law in essence consists of a cost-benefit analysis. The costs and benefits of using criminal law for the regulation of virtual cybercrime are to be determined relative to non-criminal instruments such as administrative or civil law (Bowles, Faure & Garoupa 2008, p.

395). The pragmatic dimension of the question when virtual cybercrime should be brought under the scope of criminal law has to do with the overall capacity of the criminal justice system, which should not be overloaded. When conduct involves the use of Information and Communication Technologies (ICTs), as does virtual cybercrime, there is a high risk that its criminalization will overload the criminal justice system, because ICTs have a couple of features which facilitate crime and hamper law enforcement. The constitutional dimension of the question when virtual cybercrime should be brought under the scope of criminal law focuses on the burden that is imposed on the (fundamental) liberties of citizens by the criminalization of conduct. Under constitutional law, the restriction of citizens' liberties always needs justification. This dimension turns out to greatly overlap with the philosophical and the legal-economic dimension of the aforementioned question and is, therefore, not further discussed.

At the end of the fifth chapter I establish philosophical, legal-economic, and pragmatic absolute and relative negative criteria for the criminalization of virtual cybercrime. The absolute negative criteria indicate when criminalization of virtual cybercrime should be omitted. The relative negative criteria are contraindications for criminalization; the more of them apply, the less appropriate it is to criminalize the virtual cybercrime concerned.

The philosophical absolute negative criteria entail that criminalization of a virtual cybercrime should be omitted if it does not have an extravirtual consequence at all or if its extravirtual consequence cannot be brought under the scope of one of Feinberg's liberty-limiting principles (i.e., the harm principle, the offense principle, legal paternalism, or legal moralism). Contraindications (philosophical relative negative criteria) for the criminalization of a virtual cybercrime arise when it does not result in extravirtual harm (as intended by the harm principle), offense (as intended by the offense principle), harm to the self (as intended by legal paternalism), or an evil of another kind (as intended by legal moralism).

The legal-economic absolute negative criterion entails that criminalization of a virtual cybercrime should be omitted if the benefits of using criminal law for regulation do not outweigh the costs. The benefits of using criminal law for regulation are likely to outweigh the costs when the losses are diffuse (i.e., because they are difficult to translate into monetary terms or because there is no easy identifiable victim) and relatively large. Contraindications (legal-economic relative negative criteria) for the criminalization of virtual cybercrime thus arise in the opposite situation: when the losses are clear (i.e., because they are easy to translate into monetary terms or because there is an easy identifiable victim) and relatively small.

The pragmatic absolute negative criterion entails that criminalization of a virtual cybercrime should be omitted if that would overload the criminal justice system.

Contraindications (pragmatic relative negative criteria) for the criminalization of a virtual cybercrime arise when it is committed on a tremendous scale, generally committed by making use of one or more of the anonymity features that ICTs offer, or if the virtual cybercrime is of a global nature (i.e., where victims and perpetrators are geographically dispersed).

Finally, in the epilogue, I formulate forward-looking policies with regard to virtual cybercrime. I suggest to use, from now on, the framework of absolute and relative negative criteria for criminalization I have set up in this dissertation to decide when virtual cybercrime should be brought under the scope of criminal law. I also state suggestions for future research.

SAMENVATTING

De opkomst van de computertechnologie heeft geleid tot het ontstaan van een nieuwe vorm van criminaliteit, cybercrime of computercriminaliteit, die omschreven kan worden als criminaliteit waarbij gebruik gemaakt wordt van een computer of computernetwerk. Voorbeelden van computercriminaliteit zijn "hacking" (in juridische termen: computervredebreuk) en internetfraude. De nieuwste generatie computercriminaliteit is virtuele computercriminaliteit. Virtuele computercriminaliteit is criminaliteit waarbij gebruik gemaakt wordt van een specifiek aspect van computers of computernetwerken, namelijk: virtualiteit, hetgeen nader omschreven kan worden als computersimulatie.

Denk bijvoorbeeld aan het verbod op virtuele kinderpornografie (artikel 9 Cybercrimeverdrag). Virtuele kinderpornografie bestaat niet uit foto's of filmmateriaal van echte kinderen die betrokken zijn bij een seksuele gedraging, maar uit door de computer gesimuleerde kinderen: de afbeeldingen zijn gefotoshopt of zelfs geheel middels de computer vervaardigd (Cybercrimeverdrag, Memorie van Toelichting § 101). En in Nederland is een aantal minderjarigen veroordeeld voor diefstal, omdat zij virtuele goederen gestolen hadden van medespelers in de virtuele werelden van de online computerspellen *Habbo* (2001) en *RuneScape* (2001) (Rechtbank Amsterdam, 2 april 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791; Gerechtshof Leeuwarden, 10 november 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764). In de laatste zaak is uiteindelijk door de Hoge Raad beslist (Hoge Raad, 31 januari 2012, ECLI: NL: HR: 2012: BQ9251). Een zaak die nooit voor de rechter is gekomen, maar wel uitgebreid is besproken in de media alsmede in de (juridische en filosofische) literatuur, is de virtuele verkrachting (verkrachting van een avatar: het virtuele alter ego van een speler in een computerspel) die voor het eerst werd omschreven door Julian Dibbell in de New Yorkse krant "*Village Voice*" in 1993.

Virtuele computercriminaliteit is een nog grotendeels onontgonnen gebied. Slechts een handvol virtuele gedragingen is onder het bereik van het strafrecht gebracht, waaronder het produceren, verspreiden en bezitten van virtuele kinderpornografie en diefstal van virtuele goederen. Daarnaast zijn enkele putatieve gevallen van virtuele computercriminaliteit besproken in de media en de literatuur, waaronder de eerdergenoemde virtuele verkrachting. Dit proefschrift verkent het terrein van de virtuele computercriminaliteit, vooral vanuit filosofisch oogpunt, maar er wordt ook kort aandacht besteed aan andere gezichtspunten, te weten: een juridisch-economisch, een praktisch en een constitutioneel gezichtspunt. De nadruk ligt op de vraag wanneer virtuele computercriminaliteit strafrechtelijk gereguleerd dient te worden.

Dit proefschrift is als volgt opgebouwd. Het bestaat uit drie delen: een inleidend hoofdstuk (deel I), drie casussen (deel II) en een reflectie (deel III). In totaal zijn er vijf hoofdstukken en een epiloog. Het eerste hoofdstuk bestaat uit het inleidende hoofdstuk, de casussen vormen hoofdstuk twee, drie en vier en de reflectie wordt tot slot gevonden in hoofdstuk vijf.

Het eerste hoofdstuk verschaft een juridisch-ontologische beschouwing van virtuele computercriminaliteit. In navolging van (interpretaties van het werk van) de Amerikaanse filosoof Searle (Searle 1995; Searle 2001; Searle 2010) stel ik in dit hoofdstuk dat virtuele computercriminaliteit alleen strafrechtelijk gereguleerd dient te worden, indien het een extravirtuele consequentie heeft (hiermee bedoel ik een consequentie buiten haar virtuele omgeving). Dit alleen is echter niet voldoende; het moet tevens gaan om een extravirtuele consequentie die van dien aard is dat strafrechtelijk ingrijpen moreel verantwoord is. Dit is het geval, indien een van de vier morele principes (respectievelijk het schadebeginsel, het aanstootbeginsel, paternalisme en moralisme) van toepassing is, die de Amerikaanse rechtsfilosoof Feinberg in zijn bekende werk *The Moral Limits of the Criminal Law* (1984, 1985, 1986, 1988) omschrijft en die strafrechtelijk ingrijpen legitimeren. In het tweede, derde en vierde hoofdstuk pas ik voornoemd idee toe op de drie eerder omschreven verschijningsvormen van virtuele computercriminaliteit, te weten: diefstal van virtuele goederen, virtuele verkrachting en virtuele kinderpornografie.

In het tweede hoofdstuk staan de Nederlandse veroordelingen voor diefstal van virtuele goederen in de virtuele werelden van de online computerspellen *Habbo* (2001) en *RuneScape* (2001) centraal (Rechtbank Amsterdam, 2 april 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791; Hoge Raad, 31 januari 2012, ECLI: NL: HR: 2012: BQ9251). In dit hoofdstuk stel ik dat het stelen van virtuele goederen in de virtuele wereld van een online computerspel een extravirtuele consequentie heeft waarop Feinberg's eerste morele principe, het schadebeginsel, van toepassing is en daarom als strafbare diefstal gezien kan worden, indien de virtuele goederen beschouwd kunnen worden als eigendommen van een andere speler en waarde vertegenwoordigen. Deze waarde kan geldelijk zijn, maar ook hedonistisch.

In het derde hoofdstuk onderscheid ik twee typen virtuele verkrachting: virtuele verkrachting in een virtuele wereld, zoals omschreven door Dibbell, en virtuele verkrachting in een (toekomstige) virtual realityomgeving middels een robot of een haptisch apparaat. Beiden kunnen resulteren in extravirtuele schade waarop het schadebeginsel van toepassing is: het eerstgenoemde type virtuele verkrachting kan de gebruiker emotionele schade berokkenen, het tweede type kan zijn of haar lichamelijke integriteit aantasten. Volgens de hierboven omschreven

gedachtegang zouden ze dus strafrechtelijk gereguleerd dienen te worden, maar het is onduidelijk of de omschreven handelingen onder de strafrechtelijke definitie van verkrachting vallen. In dit hoofdstuk bestudeer ik beide typen virtuele verkrachting in het licht van drie verschillende categorieën rechtsfilosofische theorieën over verkrachting, te weten: conservatieve, liberale en feministische theorieën.

Ik kom tot de conclusie dat virtuele verkrachting in een (toekomstige) virtual realityomgeving middels een robot of een haptisch apparaat valt onder de definitie van verkrachting die binnen de liberale theorieën over verkrachting gehanteerd wordt en die in veel landen, doch niet alle, de huidige bepaling die verkrachting strafbaar stelt, gevormd heeft. Virtuele verkrachting in een virtuele wereld valt niet onder voornoemde definitie, maar wel onder de definitie van verkrachting als gehanteerd wordt binnen de feministische theorieën over verkrachting, die de liberale theorieën bekritiseren. Virtuele verkrachting in een virtuele wereld reactualiseert ook het conservatieve concept van verkrachting, dat stamt uit het middeleeuwse recht. Virtuele verkrachting kan niet onder het bereik van de hedendaagse strafbaarstelling van verkrachting gebracht worden, tenzij besloten wordt de feministische definitie van verkrachting in plaats van de liberale te gaan hanteren. Maar zo'n radicale verandering van het recht is niet nodig om virtuele verkrachting strafrechtelijk te kunnen aanpakken in de huidige maatschappij. Soms telt een virtuele gedraging als het ene strafbare feit in de virtuele omgeving waarbinnen deze plaatsvindt en als een ander strafbaar feit in de niet-virtuele wereld. Ik beargumenteer dat dit het geval is met betrekking tot virtuele verkrachting in een virtuele wereld: hoewel deze virtuele gedraging niet onder het bereik van de strafbaarstelling van verkrachting gebracht kan worden, kan zij wel onder het bereik van een andere strafbaarstelling gebracht worden, te weten: de strafbaarstelling van seksuele intimidatie.[40]

Het vierde hoofdstuk gaat over virtuele kinderpornografie. De nadruk ligt op volledig computergeënsceneerde virtuele kinderpornografische afbeeldingen. In tegenstelling tot *niet*-virtuele kinderpornografische afbeeldingen geven deze afbeeldingen geen echt kind dat betrokken is bij een seksuele gedraging weer en daarom kan niet gezegd worden dat de productie, verspreiding of het bezit daarvan (verkapte) vormen van kindermisbruik zijn. Het zijn "slachtofferloze delicten" (als omschreven door Bedau 1974) waarop het schadebeginsel niet van toepassing is. Volgens Bedau is de strafbaarstelling van slachtofferloze delicten gebaseerd op paternalisme of moralisme (Bedau 1974, p. 75). Redenerend vanuit een deugdethisch en

[40] In Nederland is er geen overkoepelende strafbepaling die seksuele intimidatie strafbaar stelt, maar zijn verschillende seksueel intimiderende gedragingen afzonderlijk strafbaar gesteld. Virtuele verkrachting in een virtuele wereld zou gezien kunnen worden als het ongevraagd toezenden van een afbeelding die aanstotelijk is voor de eerbaarheid (artikel 240 Sr).

feministisch perspectief stel ik dat het verbod op de productie, verspreiding en het bezit van volledig computergeënsceneerde virtuele kinderpornografie behoort tot de zeldzame groep van gedragingen die legitiem strafbaar zijn gesteld op moralistische gronden. De gedachte alleen dat deze gedragingen plaatsvinden is aanstootgevend, omdat volledig computergeënsceneerde virtuele kinderpornografische afbeeldingen in strijd zijn met onze seksuele moraal, die is gebaseerd op gelijkheid. Indien (meer) wetenschappelijk onderzoek in de toekomst (meer) bewijs zou kunnen leveren voor de stelling dat volledig computergeënsceneerde virtuele kinderpornografische afbeeldingen kinderen kunnen aanzetten tot het aangaan van seksuele contacten met volwassenen of pedofielen kunnen aanzetten tot kindermisbruik, zou het verbod op de productie, verspreiding en het bezit van dergelijke afbeeldingen gebaseerd kunnen worden op paternalisme. Dat zou een meer solide grond voor strafbaarstelling zijn. Echter, die bewijzen zijn er tot op heden nog niet.

In het vijfde hoofdstuk stel ik dat de vraag wanneer virtuele computercriminaliteit strafrechtelijk gereguleerd dient te worden niet alleen de filosofische dimensie heeft die tot nu toe in het proefschrift besproken is, maar ook een juridisch-economische, een praktische en een constitutionele dimensie. De juridisch-economische dimensie van voornoemde vraag bestaat in essentie uit een kosten-batenanalyse. De kosten en baten van het strafrechtelijk reguleren van virtuele computercriminaliteit moeten worden afgewogen tegen de kosten en baten van regulering via andere wegen, zoals het civiel of administratief recht (Bowels, Faure & Garoupa 2008, p. 395). De praktische dimensie van de vraag wanneer virtuele computercriminaliteit strafrechtelijk gereguleerd dient te worden heeft te maken met de capaciteit van het strafrechtelijk systeem, dat niet overbelast moet raken. Wanneer bij het plegen van strafbare feiten gebruik wordt gemaakt van informatie- en communicatietechnologie (ICT), zoals in het geval van virtuele computercriminaliteit, is het risico dat het strafrechtelijk systeem overbelast raakt hoog, omdat ICT een aantal eigenschappen bezit die het plegen van strafbare feiten vergemakkelijken en de opsporing daarvan bemoeilijken. De constitutionele dimensie van de vraag wanneer virtuele computercriminaliteit strafrechtelijk gereguleerd dient te worden legt de nadruk op de beperkingen die burgers opgelegd worden indien gedrag strafbaar gesteld wordt, immers zij zijn dan niet meer vrij om dit gedrag te vertonen. Deze dimensie blijkt grotendeels te overlappen met de filosofische en de juridisch-economische dimensie van de eerdergenoemde vraag en wordt daarom verder niet besproken.

Ik besluit het vijfde hoofdstuk met het opstellen van filosofische, juridisch-economische en praktische absolute en relatieve criteria voor de strafbaarstelling van virtuele computercriminaliteit. De absolute negatieve criteria geven aan wanneer de strafbaarstelling van

virtuele computercriminaliteit achterwege gelaten moet worden. De relatieve negatieve criteria vervullen de rol van gevaartekens; des te meer van deze criteria van toepassing zijn, des te minder legitiem het is om de betreffende virtuele computercriminaliteit strafbaar te stellen.

De filosofische absolute negatieve criteria houden in dat strafbaarstelling van virtuele computercriminaliteit achterwege gelaten moet worden indien er in het geheel geen extravirtuele consequentie is of een extravirtuele consequentie waarop geen van de door Feinberg onderscheiden morele principes van toepassing is die strafrechtelijk ingrijpen legitimeren (respectievelijk het schadebeginsel, het aanstootbeginsel, paternalisme en moralisme). Contra-indicaties (filosofische relatieve negatieve criteria) voor strafbaarstelling bestaan indien de virtuele computercriminaliteit niet resulteert in schade (waarop het schadebeginsel ziet), aanstoot (waarop het aanstootbeginsel ziet), schade aan zichzelf (waarop paternalisme ziet) of een ander kwaad (waarop moralisme ziet).

De juridisch-economische absolute negatieve criteria houden in dat strafbaarstelling van virtuele computercriminaliteit achterwege gelaten moet worden, indien de baten van regulering middels strafrechtelijke middelen niet opwegen tegen de kosten. De baten van regulering middels strafrechtelijke middelen wegen meestal op tegen de kosten indien het geschonden rechtsgoed diffuus is (omdat de schending niet in geld uit te drukken is of omdat er geen duidelijk aanwijsbaar slachtoffer is) en relatief zwaarwichtig. Contra-indicaties (juridisch-economische relatieve negatieve criteria) voor strafbaarstelling bestaan in de tegenovergestelde situatie: indien het geschonden rechtsgoed concreet is (omdat het in geld uit te drukken valt of omdat er een duidelijk aanwijsbaar slachtoffer is) en de schending niet ernstig van aard is.

De praktische absolute negatieve criteria houden in dat strafbaarstelling van virtuele computercriminaliteit achterwege gelaten moet worden, indien dit het strafrechtelijk systeem zou overbelasten. Contra-indicaties (praktische relatieve negatieve criteria) voor strafbaarstelling bestaan indien de betreffende gedraging op grote schaal wordt vertoond, er gebruik is gemaakt van een of meer van de mogelijkheden tot anonimiteit die ICT biedt of indien de gedraging op mondiaal niveau heeft plaatsgevonden (wanneer slachtoffer en dader niet in hetzelfde land wonen).

In de epiloog, tenslotte, formuleer ik richtlijnen hoe in de toekomst met virtuele computercriminaliteit om te gaan. Ik stel voor om het hierboven omschreven kader te gebruiken om te bepalen wanneer virtuele computercriminaliteit strafrechtelijk gereguleerd dient te worden. Ik doe ook een aantal aanbevelingen voor toekomstig onderzoek.

BIBLIOGRAPHY

Allen, C. (2010). Artificial life, artificial agents, virtual realities: technologies of autonomous agency. In L. Floridi (Ed.), *The Cambridge Handbook of Information and Computer Ethics* (pp. 219-233). Cambridge: Cambridge University Press.

Austin, J. (1954). *The Province of Jurisprudence Determined*. London: Weidenfeld and Nicolson. (Original work published in 1832).

Australian Psychological Society (2012). Gambling-related harm. A Position Statement prepared for the Australian Psychological Society. Retrieved from <http://www.psychology. org.au>.

Beauchamp, T. L. (2003). The Nature of Applied Ethics. In R.G. Frey & C.H. Wellman (Eds.), *A Companion to Applied Ethics* (pp. 1-16). Malden (MA): Blackwell Publishers.

Beccaria, C. (1986 [1764]). *On crimes and punishments*, translated by D. Young, Indianapolis: Hackett Publishing Company.

Becker, G. (1968). Crime and Punishment: An Economic Approach. *The Journal of Political Economy*, *76*, 169-217.

Bedau, H. A. (1974). Are there really "crimes without victims"?. In E. M. Schur & H. A. Bedau, *Victimless Crimes / Two Sides of a Controversy* (pp. 55-105). Englewood Cliffs N.J.: Prentice-Hall Inc.

Bentham, J. (1988 [1789]). *An Introduction to the Principles of Morals and Legislation*, New York: Prometheus Books.

Bergman, S. (Producer). (2007, March 8). *Beperkt Houdbaar* [Television Broadcast]. Hilversum: Viewpoint Productions & VPRO. Retrieved from <http://www.beperkthoudbaar. info>. (Available in Dutch only).

Bourke, M. L. & Hernandez, A. E. (2009). The 'Butner Study' Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders. *Journal of Family Violence*, *24*, 183-191.

Boutellier, H. (2000). The pornographic context of sexual offences: reflections on the contemporary sexual mentality. *European Journal on Criminal Policy and Research*, *8*, 441-457.

Bowles, R., Faure, M. & Garoupa, N. (2008). The Scope of Criminal Law and Criminal Sanctions: An Economic View and Policy Implications. *Journal of Law and Society*, *Volume 35*, *Number 3*, 389-416.

Brenner, S. W. (2008). Fantasy Crime: The Role of Criminal Law in Virtual Worlds. *Vanderbilt Journal Of Entertainment And Technology Law*, *Vol. 11*, *Nr. 1*, pp. 1-97.

Brey, P. (2003). The Social Ontology of Virtual Environments. *American Journal of Economics and Sociology*, *Vol. 62*, *No. 1*, 269-282.

Brey, P. (2008). Virtual Reality and Computer Simulation. In K. E. Himma & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 361-384). Hoboken (NJ): John Wiley and Sons Inc.

Brey, P. (2014). The Physical and Social Reality of Virtual Worlds. In: M. Grimshaw (Ed.), *The Oxford Handbook of Virtuality* (pp. 42-54). New York: Oxford University Press.

Brown, D. K. (2004). Cost-Benefit Analysis in Criminal Law. *California Law Review*, *Volume 92*, *Issue 2*, 323-372.

O'Brien, M. D., & Webster, S. D. (2007). The Construction and Preliminary Validation of the Internet Behaviours and Attitudes Questionnaire (IBAQ). *Sex Abuse*, *19*, 237-256.

Burgess-Jackson, K. (1996). *Rape: A Philosophical Investigation*. Aldershot: Dartmouth.

Burgess, M. C. R., Stermer, S. P. & Burgess, S. R. (2007). Sex, Lies, and Video Games: The Portrayal of Male and Female Characters on Video Game Covers. *Sex Roles*, *57*, 419-433.

Burman, M. (2010). Rethinking rape law in Sweden: coercion, consent or non-voluntariness? In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 196-208). Abingdon (Oxfordshire): Routledge.

-- "Chinese gamer sentenced to life". *BBC News* 8 June 2005. Retrieved from <http://news.bbc.co.uk/2/hi/technology/4072704.stm>.

Clough, J. (2010). *Principles of Cybercrime*, Cambridge: Cambridge University Press.

Cohen, M. A. (2009). Cyber Crime. In N. Garoupa (Ed.), *Criminal Law and Economics* (pp. 346-374). Cheltenham (UK): Edward Elgar.

Collste, G. (2000). The Internet-Doctor. In G. Collste (Ed.), *Ethics in the Age of Information Technology* (pp. 119-129). Linköping: Centre for Applied Ethics.

Coleman, J. (1982). Negative and Positive Positivism. *The Journal of Legal Studies, Vol. 11: 1*, 139-164.

Cowan, S. (2010). All change or business as usual? Reforming the law of rape in Scotland. In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 154-168). Abingdon (Oxfordshire): Routledge.

Crocco, A. G., Villasis-Keever, M. & Jadad, A. R. (2002). Analysis of Cases of Harm Associated With Use of Health Information on the Internet. *JAMA*, *Vol. 287*, *No. 21*, 2869-2871.

Davidson, N. (1991). Feminism and sexual harassment. *Society*, *Vol. 28*, *Issue 4*, 39-44.

DeAngelis, T. (2007). Children and the Internet / Web pornography's effect on children. *Monitor on Psychology, Vol. 38/No. 10,* 50-52.

Derevensky, J. L. & Gupta, R. (2007). Internet Gambling Amongst Adolescents: A Growing Concern. *International Journal of Mental Health and Addiction*, *5*, 93-101.

Devlin, P. (1965). *The Enforcement of Morals*. Oxford: Oxford University Press.

Diamond, M. et al (2010). Pornography and sex crimes in the Czech Republic. *Archives of Sexual Behavior*. doi: 10.1007/s10508-010-9696-y.

Dibbell, J. (1993). A rape in cyberspace / How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society. *The Village Voice*, Dec. 23. Retrieved from <http://www.juliandibbell.com/texts>.

Dillow, C. (2010). A Customizable, Anatomically Correct Robotic Girlfriend With Multiple Personalities. Retrieved from <http://www.popsci.com>.

Driver, J. (2009). The History of Utilitarianism. In *Stanford Encyclopedia of Philosophy*. Retrieved from <http://plato.stanford.edu/entries/utilitarianism-history>.

Duranske, B. (2007a). Reader Roundtable: "Virtual Rape" Claim Brings Belgian Police to Second Life. *Virtually Blind*. Retrieved from <http://virtuallyblind.com>.

Durankse, B. (2007b). 'Anshe Chung' Withdraws DMCA YouTube Complaint. *Virtually Blind*. Retrieved from <http://virtuallyblind.com>.

Dworkin, G. (1972). Paternalism. *The Monist*, *56/1*, 64-84.

Dworkin, R. M. (1976). Is Law a System of Rules? In R. S. Summers (Ed.), *Essays in Legal Philosophy* (pp. 25-60). Berkeley and Los Angeles: University of California Press.

European Cybercrime Center (EC3) and International Cyber Security Protection Alliance (ICSPA) (2013). Project 2020. Scenarios for the Future of Cybercrime – White Paper for Decision Makers. Retrieved from <http://www.europol.europa.eu>.

--"Evangeline: Interview with a Child cyber-Prostitute in TSO". *The Alphaville Herald* 8 December 2003. Retrieved from <http:alphavilleherald.com/2003/12/evangeline_inte.html>.

Fairfield, J. A. T. (2009). The Magic Circle. *Vanderbilt Journal of Entertainment and Technology Law*, *Vol. 11: 4*, 823-840.

Feinberg, J. (1984). *The Moral Limits of Criminal Law, Volume One, Harm to Others*. Oxford: Oxford University Press.

Feinberg, J. (1985). *The Moral Limits of Criminal Law, Volume Two, Offense to Others*. Oxford: Oxford University Press.

Feinberg, J. (1986). *The Moral Limits of Criminal Law, Volume Three, Harm to Self*. Oxford: Oxford University Press.

Feinberg, J. (1988). *The Moral Limits of Criminal Law, Volume Four, Harmless Wrongdoing*. Oxford: Oxford University Press.

Fisher, W. A., Kohut, T., Di Gioacchino, L. A. & Fedoroff, P. (2013). Pornography, Sex Crime, and Paraphilia. *Current Psychiatry Reports*, *15*: *362*, 1-8.

Franke, K. M. (1996-1997). What's Wrong With Sexual Harassment? *Stanford Law Review*, *49*, 691-772.

Goodman, M. D. & Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. *International Journal of Law and Information Technology*, *Vol. 10: 2*, 139-223.

Gillett, K. (2012). Internet ban for offensive image. *The Independent*. Retrieved from <http://www.independent.co.uk/news/uk/crime/internet-ban-for-offensive-image-7575915.html>.

Gotell, L. (2010). Canadian sexual assault law: neoliberalism and the erosion of feminist-inspired law reforms. In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 209-223). Abingdon (Oxfordshire): Routledge.

Gran Turismo 5 [Computer software]. (2010). Tokio, Japan: Sony Computer Entertainment.

Grand Theft Auto V [Computer software]. (2013). New York, USA: Rockstar Games.

Habbo (2001) [Computer software]. (2001). Helsinki: Sulake Corporation.

Hale, M. (1847) [1736]. *The History of the Pleas of the Crown*. London: E. and R. Nutt and R. Gosling.

Hall, R. C. W. & Hall, R. C. W (2009). A Profile of Pedophilia: Definition, Characteristics of Offenders, Recidivism, Treatment Outcomes, and Forensic Issues. *FOCUS*, *Vol. 7*, *No. 4*, 522-537.

Hamtpon, J. (1984). The moral education of punishment. *Philosophy & Public Affairs*, *Vol. 13*, *No. 3*, 208-238.

Hart, H.L.A. (1961). *The Concept of Law*. Oxford: Clarendon Press.

Heider, D. (2009). Identity and Reality: What Does It Mean to Live Virtually? In D. Heider (Ed.), *Living Virtually. Researching New Worlds* (pp. 131-143). New York: Peter Lang Publishing.

Herring, J. & Dempsey, M. M. (2010). Rethinking criminal law's response to sexual penetration. On theory and context. In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 30-43). Abingdon (Oxfordshire): Routledge.

Hickman, T. & Hickman, K. E. (2012). The Myth of the Magic Circle: Rejecting a Single Governance Model. *UC Irvine Law Review*, *Volume 2*, *Number 2* (pp. 537-574).

Hoekman, J. & Dirkzwager, C. (2009). Virtuele diefstal: hoe gegevens toch weer goederen werden. *Computerrecht*, *148*, 158-161.

Holtug, N. (2002). The Harm Principle. *Ethical Theory and Moral Practice*, *5*, 357-389.

Huff, C., Johnson, D. G. & Miller, K. (2003). Virtual Harms and Real Responsibility. *IEEE Technology and Society Magazine*, 12-19.

Huizinga, J. (1950). Homo ludens. Proeve eener bepaling van het spel-element der cultuur. In L. Brummel et al. (Eds.), *Johan Huizinga, Verzamelde werken V (Cultuurgeschiedenis III)* (26-246). Haarlem: H.D. Tjeenk Willink & Zoon. (Original work published in 1938).

Hulsman, L. H. C. (1972). Kriteria voor strafbaarstelling. In D. Chapman et al., *Strafrecht Terecht? over dekriminalisering en depenalisering* (pp. 80-92). Baarn: Uitgeverij In den Toren.

Hume, D. (1978). *A Treatise of Human Nature*. Oxford: Clarendon Press. (Original work published in 1739).

Humphreys, S. & De Zwart, M. (2012). Griefing, Massacres, Discrimination, and Art: The Limits of Overlapping Rule Sets in Online Games. *UC Irvine Law Review*, *Volume 2*, *Number 2*, 507-536.

Husak, D. (2004). Criminal Law Theory. In M. P. Golding & W. A. Edmundson (Eds.), *The Blackwell Guide to the Philosophy of Law and Legal Theory* (pp. 107-121). Hoboken: Wiley-Blackwell.

Husak, D. (2008). *Overcriminalization: The Limits of criminal law*. New York: Oxford University Press.

Itzin, C. (1992). Pornography and the Social Construction of Sexual Inequality. In C. Itzin (Ed.), *Pornography / Women, Violence and Civil Liberties* (pp. 57-75). New York: Oxford University Press.

--"Jilted Woman 'Murdered Avatar' ". *SkyNews* 23 October 2008. Retrieved from <http://news.sky.com/story/643071/jilted-woman-murdered-avatar>.

Johnson, M. & Rogers, K. M. (2009). Too far down the Yellow Brick Road- Cyber-hysteria and Virtual Porn. *Journal of International Commercial Law and Technology*, *Vol. 4/Issue 1*, 72-81.

Järvinen, A. (2009). Video Games as Emotional Experiences. In B. Perron & M. J. P. Wolf (Eds.), *The Video Game Theory Reader 2* (85-108). New York: Routledge.

Kerr, O. S. (2008) Criminal Law in Virtual Worlds. University of Chicago Legal Forum; GWU Law School Public Law Research Paper No. 391. Available at SSRN: http://ssrn.com/abstract=1097392

Knight, W. (2005). Computer characters mugged in virtual crime spree. *NewsScientist* 18 August 2005. Retrieved from <http://www.newscientist.com/article/dn7865- computer-characters- mugged-in-virtual-crime-spree.html>.

Koepsell, D. R. (2003). *The ontology of cyberspace: philosophy, law, and intellectual property*, Peru (Illinois): Open Court Publishing Company.

Koops, B. J. (2009a). Technology and the Crime Society: Rethinking Legal Protection. TILT Law & Technology Working Paper No. 010/2009 and Tilburg University Legal Studies Working Paper No. 006/2009. Available at SSRN: http://ssrn.com/abstract=1367189

Koops, B. J. (2009b). Sex, Kids and Crime in Cyberspace: Some Reflections on Crossing Boundaries. In A.R. Lodder & A. Oskamp (Eds.), *Caught in the Cyber Crime Act* (pp.63-76). Deventer: Kluwer. Available at SSRN: http://ssrn.com/abstract=1365986

Kreulen, E. (2012). Virtuele pedoporno als remedie. *Trouw* 29 October 2012. Retrieved from <http://www.trouw.nl/tr/nl/4516/Gezondheid/article/ detail/3339011/2012/10/29/Virtuele-pedoporno-als-remedie.dhtml>.

LambdaMOO [Computer software]. (1990). Palo Alto, CA: Xerox PARC.

Lastowka, G. & Hunter, D. (2004). Virtual Crime. 49 New York Law School Review 293. Available at SSRN: http://ssrn.com/abstract=564801

Legend of Mir 3 [Computer software]. (2004). Seoul, South Korea: WeMade Entertainment.

Levy, N. (2002). Virtual Child Pornography: The Eroticization of Inequality. *Ethics and Information Technology*, *4*, 319-323.

Lineage II [Computer software]. (2004). Seoul, South Korea: NCSOFT Corporation.

Locke, J. (2007). *Two Treatises of Government*. Saint Louis Park (US): Filiquarian Publishing. (Original work published in 1689).

Lynn, R. (2004). Ins and Outs of Teledildonics. *Wired*. Retrieved from <http://www.wired.com/culture/ lifestyle/commentary/sexdrive/2004/09/65064>.

MacIntyre, A. (1984-2nd). *After Virtue: A Study in Moral Theory*. Notre Dame (Indiana): University of Notre Dame Press. First published in 1981.

MacKinnon, C. A. (1992). Pornography, Civil Rights and Speech. In C. Itzin (Ed.), *Pornography / Women, Violence and Civil Liberties* (pp. 456-511). New York: Oxford University Press.

MacKinnon, R. (1997). Virtual Rape. *Journal of Computer-Mediated Communication*, *Vol. 2*, *No. 4*, 1-20.

MapleStory [Computer Software]. (2003). Seoul, South Korea: Nexon [Wizet].

Marcus, T. D. (2007/2008). Fostering Creativity in Virtual Worlds: Easing the Restrictiveness of Copyright for User-Created Content. *New York Law School Law Review*, *Volume 52*, 67-92.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, *6*, 175-183.

McCormick, M. (2001). Is it wrong to play violent video games?. *Ethics and Information Technology*, *3*, 277-287.

McGlynn, C. (2010). Feminist activism and rape law reform in England and Wales: a Sisyphean struggle? In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 139-153). Abingdon (Oxfordshire): Routledge.

McGlynn, C. & Munro, V. E. (2010). Rethinking Rape Law: an introduction. In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 1-14). Abingdon (Oxfordshire): Routledge.

Mill, J. S. (1865). *On Liberty*. London: Longmans, Green and Co.

Mills, S. W. (2010). Reforming the law of rape in South Africa. In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 251-263). Abingdon (Oxfordshire): Routledge.

Moerings, M. (1999). De verbeten strijd tegen pedoseks en kinderporno. In M. Moerings, C. M. Pelser & C.H. Brants (Eds.), *Morele kwesties in het strafrecht* (pp. 171-193). Deventer: Gouda Quint.

Moohr, G. S. (2005). Defining Overcriminalization Through Cost-Benefit Analysis: The Example of Criminal Copyright Laws. *American University Law Review*, *Vol. 54*, 783-807.

Mooradian, N. (2006). Virtual reality, ontology, and value. *Metaphilosophy*, *Vol. 37*, *No. 5*, 673-690.

Moore, A. (2004). Hedonism. In *Stanford Encyclopedia of Philosophy*. Retrieved from <http://plato.stanford.edu/entries/hedonism>.

Moszkowicz, Y. (2009). Een kritische noot bij de 'RuneScape (2001)'- en 'Habbohotel'- uitspraken: een illusie is geen goed. *Strafblad*, Sdu Uitgevers, 495-503.

Movisie. (2009). *Seksualisering: "Je denkt dat het normaal is…" / Onderzoek naar de beleving van jongeren*. Utrecht: Felten, H., Janssens, K. & Brants, L.

Munro, V. E. (2010). From consent to coercion. Evaluating international and domestic frameworks for the criminalization of rape. In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 17-29). Abingdon (Oxfordshire): Routledge.

Murphy, J. G. & Coleman, J. L. (1990). *Philosophy of Law: An Introduction to Jurisprudence*. Boulder (USA): Westview Press Inc.

New Zealand Government, Department of Internal Affairs (2007). Problem Gambling in New Zealand- A Brief Summary. Retrieved from <http://www.dia.govt.nz>.

Office of the Children's Commissioner (OCC) (2013). *Basically…porn is everywhere: A Rapid Evidence Assesment on the Effect that Access and Exposure to Pornography has on Children and Young People*. London: Horvath, M.A.H., Alys, L., Massey, K., Pina, A., Scally, M. & Adler, J.R.

Ogus, A. (2009). Criminal law and regulation. In N. Garoupa (Ed.), *Criminal Law and Economics* (pp. 90-110). Cheltenham (UK): Edward Elgar.

--"Paedophiles Target Virtual World". *SkyNews* 31 October 2007. Retrieved from <http:news.sky.com/story/549533/paedophiles-target-virtual-world>.

Pember, D. R. & Calvert, C. (2012). *Mass Media Law*. New York: McGraw-Hill.

Posner, R. (1985). An Economic Theory of criminal law. *Columbia Law Review*, *Vol. 85*, *No. 6*, 1193-1231.

Poulsen, K. (2008). Report: FBI Investigates Epilepsy Forum Attackers. *Wired*. Retrieved from <http://www.wired.com/2008/05/report-fbi-inve>.

Powers, T. M. (2003). Real wrongs in virtual communities. *Ethics and Information Technology*, *5*, 191-198.

Quayle, E. & Taylor, M. (2002). Pedophiles, Pornography and the Internet: Assessment Issues. *British Journal of Social Work*, *32*, 863-875.

Radačić, I. & Turković, K. (2010). Rethinking Croatian rape laws: force, consent and 'the contribution of the victim'. In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 169-182). Abingdon (Oxfordshire): Routledge.

Raz, J. (1986). *The Morality of Freedom*. Oxford: Clarendon Press.

RapeLay [Computer software]. (2006). Yokohama, Japan: Illusion Soft.

Rijna, F. (2010). Wat is een virtueel object en kun je het stelen? *Nederlands Juristenblad*, *Afl. 13*, *647*, 790-794.

Ruane, K. A. (2011). *Funeral Protests: Selected Federal Laws and Constitutional Issues*. Congressional Research Service. R41717. Retrieved from <http:opencrs.com>.

Ruddick, S. (1975). Better Sex. In R. Baker & F. Elliston (Eds.), *Philosophy and Sex* (pp. 83-104). Buffalo, NY: Prometheus Books.

RuneScape (2001) [Computer software]. (2001). Cambridge, UK: Jagex Ltd.

Rush, P. (2010). Criminal law and the reformation of rape in Australia. In C. McGlynn & V. E. Munro (Eds.), *Rethinking Rape Law. International and Comparative Perspectives* (pp. 237-250). Abingdon (Oxfordshire): Routledge.

Rutgers Nisso Groep, Nederlands Jeugdinstituut, Movisie. (2008). *Seksualisering: Reden tot zorg? / Een verkennend onderzoek onder jongeren*. Utrecht: De Graaf, H., Nikken, P., Felten, H., Janssens, K. & Van Berlo, W.

Salen, K. & Zimmerman, E. (2004). Rules of play. Game design fundamentals. Cambridge: MIT Press.

Sandin, P. (2004). Virtual child pornography and utilitarianism. *Journal of Information, Communication and Ethics in Society*, *Vol. 2*, *Iss: 4*, 217-223.

Schellekens, M. (2006). What holds off-line, also holds on-line? In B. J. Koops, M. Lips, C. Prins & M. Schellekens, *Starting Points for ICT Regulation* (pp. 51-75). The Hague: TMC Asser Press.

Searle, J. R. (1995). *The Construction of Social Reality*. New York: The Free Press.

Searle, J. R. (2001). *Rationality in Action*. Cambridge (Massachusetts): The MIT Press.

Searle, J. R. (2010). *Making the Social World. The Structure of Human Civilization*. New York: Oxford University Press.

Second Life [Computer software]. (2003). San Francisco, CA: Linden Research Inc.

--"Second Life Seclimine VB Sample". *YouTube* 16 May 2007. Retrieved from <http://www.youtube.com/watch?v=OQvgWros7TY>.

Soave, R. (2013). Second teen spends months in jail for sarcastic video game threat. *Daily Caller*. Retrieved from <http://dailycaller.com/2013/07/02/ second-teen-spends-months- in-jail-for-video-game-threat/>.

Steel, A. (2008). The Harms and Wrongs of Stealing: the Harm Principle and Dishonesty in Theft. *UNSW Law Journal*, *Volume 31 (3)*, 712-737.

Stewart, H. (2010). The Limits of the Harm Principle. *Criminal Law and Philosophy*, *4*, 17-35.

Strikwerda, L. (2011). Virtual Child Pornography Why Images Do Harm from a Moral Perspective. In C. Ess & M. Thorseth (Eds.), *Trust and Virtual Worlds Contemporary Perspectives* (pp. 139-161). New York: Peter Lang Publishing.

Strikwerda, L. (2012). Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. *Ethics and Information Technology*, *Volume 14*, *Issue 2*, 89-97.

Strikwerda, L. (2013). When Should Virtual Cybercrime Be Brought under the Scope of Criminal Law?. In M. K. Rogers and K. C. Seigfried-Spellar (Eds.), *Digital Forensics and Cyber Crime (LNICST), Vol. 114* (pp. 109-143). Berlin: Springer-Verlag.

Strikwerda, L. (2014). Should virtual cybercrime be regulated by means of criminal law? A philosophical, legal-economic, pragmatic, and constitutional dimension. *Information & Communications Technology Law*, *Volume 23*, *Issue 1*, 31-60.

Strikwerda, L. (2014). Present and future instances of virtual rape in light of three categories of legal philosophical theories on rape. *Philosophy & Technology*. doi: 10.1007/s13347-014-0167-6.

Sunstein, C. (2001). *Republic.com*, Princeton: Princeton University Press.

Søraker, J. H. (2007). Real norms, virtual cases: A rationalist, casuistic account of virtual rape. In L. Hinman, P. Brey, L. Floridi, F. Grodzinsky & L. Introna (Eds.), *Proceedings of CEPE 2007- The 7th International Conference of Computer Ethics: Philosophical Enquiry* (340-346). Enschede: Center for Telematics and Information Technology (CTIT).

Søraker, J. H. (2010). *The value of virtual worlds and entities. A philosophical analysis of virtual worlds and their potential impact on well-being* (doctoral dissertation). Enschede: Ipskamp.

Søraker, J. H. (2012). Virtual worlds and their challenge to philosophy: understanding the "intravirtual" and the "extravirtual". *Metaphilosophy*, *Vol. 43*, *No. 4*, 499-512.

Tavani, H. T. (2007-2). *Ethics & Technology. Ethical Issues in an Age of Information and Communication Technology*. Hoboken (NJ): John Wiley & Sons Inc.

Terdiman, D. (2007). The legal rights to your 'Second Life' avatar. *Cnet*. Retrieved from <http://news.cnet.com/The-legal-rights-to-your-Second-Life-avatar/2100-1047_3-6147700.html.

The Sims [Computer software]. (2000). Redwood City, CA: Electronic Arts.

Vanacker, B. & Heider, D. (2011). Ethical harm in virtual communities. *Convergence: The International Journal of Research into New Media Technologies*, *18 (1)*, 71-84.

Van Ammelrooy, P. (2012). Hackers richten bloedbad aan in World of Warcraft. *De Volkskrant* 8 October 2012. Retrieved from <http://www.volkskrant.nl/vk/nl/2694/TechMedia/article/detail/3328488/2012/10/08/Games-Hackers-richten-bloedbad-aan-in-World-of-Warcraft.dhtml>.

Van Beek, E. (2011). Het beest in ons: over fatsoen en bestialiteit. *Tijdschrift voor Seksuologie*, *35*, 89-96.

Van der Burg, W. (2010). Law and Ethics: The Twin Disciplines. Erasmus Working Paper Series on Jurisprudence and Socio-Legal Studies No. 10-02. Available at SSRN: http://ssrn.com/abstract=1631720.

Waldron, J. (2004). Property and Ownership. In *Stanford Encyclopedia of Philosophy*. Retrieved from <http://plato.stanford.edu/entries/property>.

Weckert, J. (2000). Offence on the Internet. In G. Collste (Ed.), *Ethics in the Age of Information Technology* (pp. 104-118). Linköping: Centre for Applied Ethics.

Whisnant, R. (2009). Feminist Perspectives on Rape. In *Stanford Encyclopedia of Philosophy*. Retrieved from <http://plato.stanford.edu/entries/feminism-rape>.

Wolfendale, J. (2007). My avatar, my self: Virtual harm and attachment. *Ethics and Information Technology*, *9*, 111-119.

World of Warcraft [Computer software]. (2004). Irvine, CA: Blizzard Entertainment.

Zaibert, L. & Smith, B. (2007). The varieties of normativity: an essay on social ontology. In S. L. Tsohatzidis (Ed.), *Intentional Acts and Institutional Facts / Essays on John Searle's Social Ontology* (pp. 157-173). Dordrecht: Springer.

Zhai, P. (1998). *Get Real. A Philosophical Adventure in Virtual Reality*. Lanham (USA): Rowman & Littlefield Publishers.

TABLE OF LEGAL DOCUMENTS (INTERNATIONAL)

Council of Europe

Council of Europe European Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950 as amended by Protocol No. 14 (CETS No. 194). Retrieved from <http://conventions.coe.int>.

Council of Europe Convention on Cybercrime, Budapest, 23 November 2001 (CETS No.185). Retrieved from <http://conventions.coe.int>.

Council of Europe Convention on Cybercrime, Explanatory Report. Retrieved from <http://conventions.coe.int>.

Council of Europe Convention on Cybercrime, List of declarations, reservations and other communications. Retrieved from <http://conventions.coe.int>.

Council of Europe Convention on Cybercrime, Summary. Retrieved from <http://conventions.coe.int>.

Council of Europe Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, Strasbourg, 28 January 2003 (CETS No.189). Retrieved from <http://conventions. coe.int>.

Council of Europe Additional Protocol to the Convention on cybercrime, Explanatory Report. Retrieved from <http://conventions. coe.int>.

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse , Lanzarote, 25 October 2007 (CETS No. 201). Retrieved from <http://conventions.coe.int>.

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse , Explanatory Report. Retrieved from <http://conventions.coe.int>.

UN

UN Universal Declaration of Human Rights. Adopted and proclaimed by General Assembly resolution 217A (III) of 10 December 1948. Retrieved from <http://www.ohchr.org>.

UN General Recommendation No. 19 to the Convention on the Elimination of all Forms of Discrimination Against Women, eleventh session 1992. Retrieved from <http://www.un.org/womenwatch/daw/cedaw/recommendations/recomm.htm>.

UN Optional Protocol to the UN Convention on the rights of the child, on the sale of children, child prostitution and child pornography. Adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000. Retrieved from <http://www.ohchr.org>.

Other

Commission of the European Communities Communication from the Commission of 2 February 2000 on the precautionary principle (COM (2000) 1). Retrieved from <http://europa.eu/legislation_summaries/consumers/ consumer_safety/l32042_en.htm>.

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Retrieved from <http://eur-lex.europa.eu>.

EU Consolidated version of the Treaty on the Functioning of the European Union, *Official Journal of the European Union*, 30.3.2010, C 83/47. Retrieved from <http://eur-lex.europa.eu>.

TABLE OF LEGAL DOCUMENTS (DOMESTIC)

Belgium

Strafwetboek. Retrieved from <http://www.belgischrecht.be>. (Available in Dutch only).

Germany

Strafgesetzbuch. Retrieved from <http://www.stgb.de>. (Available in German only).

Israel

Penal Law 5737-1977. Retrieved from <http://www.oecd.org/dataoecd/15/58/43289694.pdf>.

Korea

Game Industry Promotion Act. Retrieved from <http://www.grb.or.kr/english/enforcement/ act.aspx>.

The Netherlands

Burgerlijk Wetboek. Retrieved from <http://wetten.overheid.nl>. (Available in Dutch only).

Grondwet voor het Koninkrijk der Nederlanden. Retrieved from <http://wetten.overheid.nl>. (Available in Dutch only).

Wetboek van Strafrecht. Retrieved from <http://wetten.overheid.nl>. (Available in Dutch only).

Wetboek van Strafvordering. Retrieved from <http://wetten.overheid.nl>. (Available in Dutch only).

New Zealand

Crimes Act 1961 No 43. Retrieved from <http://www.legislation.govt.nz/act/public/1961/ 0043/ latest/whole.html#DLM3290>.

Gambling Act 2003 No. 51. Retrieved from <http://www.legislation.govt.nz/act/public/2003/ 0051/latest/whole.html>.

Norway

General Civil Penal Code. Retrieved from <http://www.un.org/depts/los/ LEGISLATION ANDTREATIES/PDFFILES/NOR_penal_code.pdf>.

South Africa

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007. Retrieved from <http://www.justice.go.za/legislation/acts/2007-032.pdf>.

UK

Sexual Offences Act 2003. Retrieved from <http://www.legislation.gov.uk/ukpga/2003/42>.

Criminal Justice and Immigration Act 2008. Retrieved from <http://www.legislation.gov.uk/ukpga/2008/4>.

USA

PROTECT Act, 108th Congress of the USA, 7 January 2003. Retrieved from <http://www.gpo.gov/fdsys/pkg/BILLS-108s151enr/pdf/BILLS-108s151enr.pdf>.

US Code (USC), Title 18: Crimes and Criminal Procedure. Retrieved from <http://www.findlaw.com/casecode>.

TABLE OF CASES

The Netherlands

Hoge Raad, 22 April 2008, ECLI: NL: HR: 2008: BB7087. Retrieved from <http://www.rechtspraak.nl>. (Available in Dutch only).

Hoge Raad, 31 January 2012, ECLI: NL: HR: 2012: BQ9251. Retrieved from <http://www.rechtspraak.nl>. (Available in Dutch only).

Gerechtshof 's-Gravenhage, 16 November 2010, ECLI: NL: GHSGR: 2010: BO4035. Retrieved from <http://www.rechtspraak.nl>. (Available in Dutch only).

Gerechtshof Leeuwarden, 10 November 2009, ECLI: NL: GHLEE: 2009: BK2773, BK2764. Retrieved from <http://www.rechtspraak.nl>. (Available in Dutch only).

Rechtbank Amsterdam, 2 April 2009, ECLI: NL: RBAMS: 2009: BH9789, BH9790, BH9791. Retrieved from <http://www.rechtspraak.nl>. (Available in Dutch only).

Rechtbank ’s-Hertogenbosch, 4 February 2008, ECLI: NL: RBSHE: 2008: BC3225. Retrieved from <http://www.rechtspraak.nl>. (Available in Dutch only).

USA

Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) Retrieved from <http://www.findlaw.com/casecode>.

USA v. Williams, 553 U.S. 285 (2008). Retrieved from <http://www.findlaw.com/casecode>.

Doe v. Boland 698 F. 3d 877 6th Cir. (2012). Retrieved from <http://www.findlaw.com/casecode>.