SHOULD VIRTUAL CYBERCRIME BE BROUGHT UNDER THE SCOPE OF THE CRIMINAL LAW?

Litska Strikwerda

Introduction

The advent of computer technology has given rise to a new type of crime: cybercrime, which is crime that involves the use of computers or computer networks. Examples of cybercrime are: the spread of computer viruses, e-fraud and the distribution of child pornography by means of the Internet. The newest generation of cybercrime is virtual cybercrime. Virtual cybercrime is crime that involves a specific aspect of computers or computer networks: computer simulation. For example, virtual child pornography, which does not consist of photographs or film material of real children engaged in sexually explicit conduct, but of entirely computer-simulated images. And in the Netherlands, for instance, several minors were convicted of theft for the stealing of virtual items in the virtual worlds of the online multiplayer computer games *Habbo* and *RuneScape*. One of these cases was decided by the highest court in the Netherlands (Hoge Raad, 31 January 2012, LJN: BQ9251). In Japan, finally, the police investigated the case of a woman who "killed" an avatar (a virtual person) in the virtual world of the online multiplayer computer game *MapleStory* (http://news.sky.com/home/world-news/article/15127170). But should acts like the aforementioned really be treated as crimes under criminal law? This paper aims to answer that question.

The abovementioned question belongs to the field of legal ontology. 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 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 paper will study when the new phenomenon of virtual cybercrime should be categorized as crime under criminal law. This study will consist of the following three steps:

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

The first section of this paper will be concerned with the first step. It will study how cybercrime is treated within existing legal systems, provide a definition of cybercrime and determine the scope of the term. Then it will study the different meanings of the term "virtual" and define the term so that it can be explained what the new legal phenomenon of virtual cybercrime entails. At last, it 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 paper 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 virtual cybercrime from the point of view of ontology

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

and legal philosophy. I will establish that it is a necessary condition for a virtual cybercrime that it has an extravirtual consequence (a consequence outside the virtual environment). And that that is also a sufficient condition if the consequence is of such a nature that it can legitimate an interference with the liberty of citizens by means of penal law on the basis of one of Feinberg's liberty-limiting principles: the harm principle, the offense principle, legal paternalism or 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 the criminal law when it results in extravirtual harm to others, offense, harm to the self or evils of other kinds.

1 Virtual cybercrime: legal positioning, definition and scope

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 study the different meanings of the term "virtual" and define the term so that I can explain what the new legal phenomenon of virtual cybercrime entails. Next, I will examine how virtual cybercrime is treated within existing legal systems. At last, 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 the definition in principle applies to any country or jurisdiction worldwide.

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; Convention on Cybercrime, Expl. Report, § 8). Cybercrime thus consists of any human act that involves the use of computers or computer networks and 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 penal 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, 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 (Goodman & Brenner 2002, pp. 152-153; Clough 2010, p. 10; Convention on Cybercrime, Expl. Report § 5; Tavani 2007, pp. 205-206). Legislators continuously need to determine which of the new and different forms of human activity that the use of computers and computer networks allows for have to be prohibited and which not. They have to enact new legal prohibitions in order to prohibit the new forms of human activity that computers or computer networks allow for or make existing legal prohibitions sufficiently broad as 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 are some common grounds (Goodman & Brenner 2002, p. 165).

The legal reforms that have taken place in many countries in order to respond to the developments in the field of cybercrime have followed four waves. The first wave of law reform started in the 1970s and addressed the protection of privacy. It was a response to the emerging capabilities for collecting, storing and transmitting data by means of computer equipment. Administrative, civil and penal legislation was enacted to protect data and the associated right to privacy. The second wave of law reform originated in the 1980s and was targeted against economic crimes. Traditional penal laws were extended to the new opportunities for economic crimes, such as fraud, that computers provide. The third wave of law reform also took place in the 1980s and was directed toward the protection of intellectual property. The fourth wave of law reform concerned illegal and harmful content, such as child pornography, hate speech and defamation. It started in the 1980s, but began to expand significantly once the Internet became ubiquitous in the mid-1990s (Goodman & Brenner 2002, pp. 161-165).

The most familiar and most important international initiative to develop penal law aimed at cybercrime is the Convention on Cybercrime (Budapest, 23 November 2001, ETS No. 185), which has been signed by almost all member states of the Council of Europe and some other states, i.e. the United States of America, Japan, South Africa and Canada. It is the only binding international instrument on this issue to have been adopted to date (<http://www.coe.int>). The Convention on Cybercrime establishes "a common minimum standard of relevant offences" (Convention on Cybercrime, § 33 Expl. Report). It defines nine types of new and different human activities involving the use of computers or computer networks and State Parties to the Convention agree to establish them as criminal offences under their domestic law, if they have not yet done so (Ibid.). The Convention on Cybercrime thus provides a list of behaviors that are considered cybercrime worldwide.

The first offence category listed in the Convention on Cybercrime is illegal access or "hacking", which is the unauthorized intrusion of the whole or any part of a computer system (article 2 Convention on Cybercrime, § 44 Expl. Report). The second offence category, illegal interception, consists of the stealing of computer data (article 3 Convention on Cybercrime, § 51 Expl. Report; Goodman & Brenner 2002, p. 189). The third offence category, data interference, refers to the damaging, deletion, deterioration, alteration or suppression of computer data without right (article 4 Convention on Cybercrime). The alteration of computer data includes the input of malicious codes, such as viruses (Convention on Cybercrime, Expl. Report § 61). The fourth offence 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 (article 5 Convention on Cybercrime, § 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 offence 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 (article 6 Convention on Cybercrime, § 71 Expl. Report). The sixth offence category, computer-related forgery, involves the false making or altering of computer data (article 7 Convention on Cybercrime, § 81 Expl. Report). The seventh offence category, computer-related fraud, consists of electronic deceit: the undue manipulation in the course of data processing in order to obtain money or other property illegally, e.g. credit card fraud (article 8 Convention on Cybercrime, § 86 Expl. Report). The eighth offence category, offences related to child pornography, concerns the electronic production, distribution or possession of child pornographic images

(article 9 Convention on Cybercrime). The last offence category, offences 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 (article 10 Convention on Cybercrime, § 107 Expl. Report).

The first five offence 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 offence categories concern new forms of human activity, they require signatory states to enact new legal prohibitions, if they did not prohibit these activities yet (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 offence categories (computer-related forgery, computer-related fraud, offences related to child pornography and offences 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 offence categories require them to make their existing laws sufficiently broad to extend to situations involving computers or computer networks if they did not do so yet (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 penal philosophy responsible for them (Goodman & Brenner 2002, p. 216). Most of the computer crimes that are listed in the Convention on Cybercrime are, although they are new crimes, consistent with existing legal prohibitions and the penal philosophy responsible for them, because they are in essence "electronic versions of existing property crimes" (Ibid., p. 189). Illegal access is the electronic version of trespass. Illegal interception can be seen as an electronic invasion of privacy or burglary offence. And data interference is an electronic property damage offence. System interference and the misuse of devices are entirely new offences that have no analogue in traditional crime, however (Ibid.). 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 (Convention on Cybercrime, Expl. Report § 65). The prohibition on misuse of devices aims to prohibit the aforementioned offences 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 (Strasbourg, 24 January 2001, ETS No. 178) and EU Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional legal access (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 responsible for them, because they relate to traditional offences that most signatory states have already criminalized (Convention on Cybercrime, Expl. Report § 79). The provision on computer-related forgery creates a parallel offence to the forgery of tangible documents (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 deposit money (Convention on Cybercrime, Expl. Report § 86). The provision on offences 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 offences against children (Convention on Cybercrime, Expl. Report § 91). And, finally, the

provision on offences 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 (Convention on Cybercrime, Expl. Report § 107).

Many states that have signed the Convention on Cybercrime have also signed its Additional Protocol (Strasbourg, 28 January 2003, ETS No. 189), 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 the penal law that already exists in most signatory states to the commission of traditional crimes through the Internet (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 easily and widely expressions containing such ideas. It builds upon the UN International Convention on the Elimination of All Forms of Racial Discrimination (adopted and opened for signature and ratification by General Assembly resolution 2106 (XX) of 21 December 1965) and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4 November 1950) (Additional Protocol, Expl. Report §10).

The first offence category listed in the Additional Protocol is the dissemination of racist and xenophobic material trough 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" (article 2 Additional Protocol). 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 (Additional Protocol, Expl. Report § 28, 31). The second offence 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 (article 4 Additional Protocol, § 35 Expl. Report). The third offence category, racist and xenophobic motivated insult, consists of the offence 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 (article 5 Additional Protocol, § 36 Expl. Report). The last offence category is denial, gross minimisation, approval or justification of genocide or crimes against humanity. It refers to the dissemination of material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity committed through a computer system (article 6 Additional Protocol). 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 second World War. The scope of this provision is not limited to the crimes committed by the Nazi regime during the second World War, but also covers genocides and crimes against humanity committed by other regimes, e.g. in Yugoslavia or in Rwanda (Additional Protocol, Expl. Report § 39, 40).

Last, there is another international initiative that establishes a common relevant offence: the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote, 25 October 2007, ETS No. 201), which has been signed by most of the member states of the Council of Europe. 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 (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 (Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 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. § 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 (Ibid. § 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 for parents and for legal authorities (Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Expl. Report § 159).

1.1.1 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, offences related to child pornography, offences related to infringements of copyright and related rights, acts of a racist and xenophobic nature that are committed through computer systems and "grooming."

1.2 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 paper.

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 world". 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 3-D visuals. The vast majority of MMORPGs can 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, e.g. cars.

Lastly, the term "virtual" can be used in the context of "virtual reality." Virtual reality 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. Secondly, virtual realities do not offer multi-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). 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 2003, 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 2003, 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 of 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 paper, 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.

1.2.1 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 the shooting of a bear in the virtual environment of a computer game. 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. Second, the computer simulation interprets the bodily action as a particular command, e.g. "shoot the bear". 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, e.g. the bear in the virtual environment is death (Ibid., p. 137). 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 (Ibid., pp. 33-34). The production, possession or distribution of virtual child pornography is an example of a human act made possible by computer simulation. The aforementioned act is not virtual in itself, 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 morphed pictures of real children or entirely computer-generated images (Convention on Cybercrime, Expl. Report § 101). Virtual child pornographic images are thus made possible by computer simulation. The nature of the act of producing, distributing and possessing them is partly determined by the features of the computer simulation, because it does not involve (the profiting from) child abuse, as opposed to the production, distribution and possession of non-virtual child pornographic images.

In fact, the production, possession or distribution of virtual child pornography is the only human act involving computer simulation that is 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 (Convention on Cybercrime, article 9 (2) c). Not all signatory states to the Convention on Cybercrime have criminalized the production, possession and distribution of virtual child pornography, however. Iceland, Scotland and the United States of America have reserved the right not to apply the prohibition on virtual child pornography (List of declarations made with respect to treaty No. 185 Convention on Cybercrime, retrieved from <http://conventions.coe.int>). The production, possession and distribution of virtual child pornography is thus not as commonly prohibited as the production, possession or distribution of non-virtual child pornography.

Dutch case law provides another example of a human act made possible by computer simulation that has been brought under the scope of penal law. In 2009 Dutch judges have 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 the stealing of virtual furniture in the virtual world of the online multiplayer computer game *Habbo* (Rechtbank Amsterdam, 2 April 2009, LJN: BH9789, BH9790, BH9791). *Habbo* is a metaverse and consists of a virtual hotel where players have their own room, which they can furnish. By means of deceit the perpetrators obtained the usernames and passwords of other *Habbo* players, so that they could access the other players' accounts and transfer their virtual furniture to their own *Habbo* 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* (Gerechtshof Leeuwarden, 10 November 2009, LJN: BK2773, BK2764). This judgement was confirmed by the Dutch Supreme Court (Hoge Raad, 31 Janaury 2012, LJN: BQ9251). *RuneScape* 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* to give them access to his account, so that they could transfer his virtual amulet and virtual mask to their own *RuneScape* accounts. The acts of stealing in these cases were not virtual in themselves, because they involved out-of-the-game infractions (deceit, violence). But they were defined in terms of virtual objects (the virtual items stolen). There have not yet been comparable penalties in other jurisdictions (Hoge Raad, 31 January 2012, Concl. Adv.-Gen., LJN: BQ9251).

Examples of computer-simulated crime are only found in the legal literature as opposed to in actual law (e.g. Brenner 2008; Clough 2010, pp. 16-21; Kerr 2008). The most well-known example of a computer-simulated crime is the virtual "rape" that was described by Julian Dibbel in a much-debated 1993 paper. Dibbel describes how a user represented by an avatar named Mr. Bungle took control over other users' avatars in the virtual environment of *LambdaMOO* and forced their avatars, through his own avatar, to engage in sexual activities they did not consent to (Dibbel 1993). *LambdaMOO* was a text-based MOO-MUD: a MUD that mainly aimed at social interaction with other users (Brenner 2008, p. 21). There have not been penalties with regard to computer-simulated crime yet.

Unlike the virtual worlds of computer games, virtual reality technologies 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-access or at least not beyond a very limited degree. Except for rare cases of "victimless" crimes, such as gambling or drunk-driving, crimes generally victimize another person. And thus virtual realities are not likely to provide new opportunities for crime until they become multi-accessible on a larger scale.

Finally, it is important to note that none of the virtual cybercrimes listed above concern new human activities; they are all different forms of traditional crimes. Virtual cybercrime consists either of a computer-simulated traditional crime or of a traditional crime that is defined in terms of a computer-simulated person or object. Therefore, it only requires legislators to extend existing laws and not to enact new ones.

1.2.2 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. Currently, the production, possession and distribution of virtual child pornography is the only virtual

cybercrime that is commonly prohibited, although not as commonly as non-virtual child pornography. Putative virtual cybercrimes are, for example, virtual rape, virtual killing and theft of virtual items. These computer-simulated human acts and human act made possible by computer simulation are not (commonly) prohibited yet. 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".

2 Virtual cybercrime: necessary and sufficient conditions

It was established in the last section that the production, distribution and possession of virtual child pornography is the only virtual cybercrime that is commonly prohibited. Since it would be a fallacy to make a general statement about virtual cybercrime on the basis of one specific instance of virtual cybercrime, an empirical study of the law 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 to obtain in order to be prohibited under existing law. Therefore, I will study virtual cybercrime from a different point of view. As was stated in the introduction, the study of virtual cybercrime belongs to the field of legal ontology. Applied forms of ontology often put to use the tools of philosophical ontology in order to categorize things within a specific domain. I will make use of this method and put to use the tools of the philosophical ontology of the American philosopher Searle 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 make use of legal philosophy to reflect on the outcome of the ontological analysis.

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 (Ibid., p. 27). 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 (Searle 1995, 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 (Searle 2010, 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 status of money on pieces of paper and metal. These pieces of paper and metal cannot perform the function of money (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". Institutional facts are special because they do not need to have a physical structure; they only exist because humans believe them to exist (Searle 1995, p. 1).

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. Humans have, for instance, imposed the status function of President of the United States on Barack Obama and the status function of marriage on a certain ceremony (Searle 2010, p. 7). 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 in a community 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" (Searle 2010, p. 10). They regulate antecedently existing forms of behavior (Searle 2010, p. 9). 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). The latter can be explained as follows. Constitutive rules are "Declarations": a special kind of statements (Searle 2010, p. 11). Some statements purport to represent how things are in the world, e.g. "The cat is on the mat" (Ibid.). They have the "word-to-world direction of fit" (Ibid.). Other statements try to change the world to match the content of the speech act, e.g. if you order someone to leave the room. They have a "world-to-word direction of fit" (Searle 2010, pp. 11-12). Declarations combine the word-to-world and the world-to-word direction of fit: they have both directions of fit simultaneously in one statement. Declarations change reality to match its propositional content, but succeed in doing so because they represent the reality as being so changed. They declare that a state of affairs exists and, thereby, bring that state of affairs into existence (Searle 2010, p. 12).

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" (Searle 2010, p. 97).

Law is a typical example where constitutive rules function as standing Declarations (Searle 2010, p. 13). Penal provisions, for instance, 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). They 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). The US penal prohibition on murder, for instance, 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 United States (C) (18 USC § 1111, retrieved from <http://www.law.cornell.edu/uscode/text>).

(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). Searle explains: "We collectively recognize that a Y status function exists in context C, and because a human subject S stands in a certain appropriate relations R to the status function Y in C, we further recognize that S has the power to do A, the acts determined by the status function" (Searle 2010, p. 103). So, if a (standing) Declaration in the form of a legal provision, for example, assigns the status of property (Y) to an object in a certain jurisdiction (C) it, thereby, also creates property rights (A) for the property owner (S), because s/he stands in a relation of ownership (R) to the property.

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 this particular country and does it, therefore, give rise to criminal liability?" can arise. Such questions have to be answered by "human institutions" (Ibid.). Examples of common human institutions are: the legislature, judiciary and other governmental institutions (Searle 2010, p. 91). They have the power to decide whether a certain act, object, person or other entity falls within a certain constitutive rule (Searle 2010, p. 103). The judiciary can, for instance, decide whether a certain act falls within a constitutive rule that declares it a crime under the jurisdiction of a certain country and whether it gives rise to criminal liability.

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 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 people or authorities 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" that have the form "X counts as Y (in context C)." 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". (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. Whether or not a (Standing) Declaration applied to a certain entity is decided by human institutions. For the purposes of this paper it should be highlighted that the (criminal) law consists of Standing Declarations. After all, penal provisions 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 criminal liability upon people.

2.1.1 Applications of Searle's ontology

Following Searle, a human act is considered to be a crime when human institutions (legislatures, judiciaries) have decided that a penal provision applies to it and, thereby, have imposed the status function of crime (Y) on the act (X) in the context of the jurisdiction of a particular country (C). As was explained above, 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 (2010, p. 99). So when legislators or judiciaries decide that a particular human act (X) counts as a crime (Y) in the jurisdiction of a particular country (C) they do so because they find that the set of conditions (p) for that crime has been satisfied.

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 it is required that the actor acts knowingly, purposely or recklessly).[2] 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*.

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).[3] The element of actus reus can be satisfied either intravirtually or 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 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. 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) 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. 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 *SecondLife* users can

[2]The terms "actus reus" and "mens rea" derive specifically from Anglo-American jurisprudence. But these elements are, although under a different name, also found in other legal systems.
[3]The distinction between "intravirtual" and "extravirtual" derives from Søraker 2010, p. 143.

produce, trade, possess and use a drug called "Seclimine" through their avatars (See <http://www.youtube.com/watch v=OQvgWros 7TY>). The computer-simulated human act of producing, trading or possessing Seclimine in *SecondLife* 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 *SecondLife* 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 *SecondLife* (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 *SecondLife* 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. Some countries prohibit gambling. Gambling can be defined as the unlawful betting or wagering of money or something else of value. The actus reus of gambling implies a certain consequence: financial gain or loss. On the Internet one can find virtual casino's within which one can gamble on virtual slot machines with real, non-virtual money. The computer-simulated human act of gambling on a virtual slot machine within a virtual casino 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. The act of gambling on a virtual slot machine within a virtual casino with real money (X) thus satisfies the element of causation (p) extravirtually and , therefore, counts as a crime (Y) not only in the context of its virtual environment, but also in the context of the non-virtual world (C).

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). Consider the following example. Several media reported the case of a 43-year-old Japanese woman who killed the avatar her own avatar was married to in the virtual world of the online multiplayer computer game *MapleStory*, 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 even arrested the woman at her home, but she was never formally charged (see e.g. http://news.sky.com/home/world-news/article/15127170). We could say that the act of the Japanese woman satisfies both the actus reus element (killing) and the element of causation (the death of the avatar) of the crime of manslaughter, but only intravirtually. After all, both the act of killing and the death of the avatar occurred within the virtual environment of *MapleStory*. But the death of the avatar in *MapleStory* also had a consequence in the non-virtual world; for the user who was represented by the avatar lost his virtual alter ego. As was explained in section 1.1.1 countries also commonly prohibit the deterioration of computer data without right (article 4 Convention on Cybercrime). Since an avatar consists of computer data, we could 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. By satisfying the elements of the crime of manslaughter intravirtually, the Japanese woman who killed another user's avatar in *MapleStory* thus satisfied 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).[4]

[4]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 (forthcoming).

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. I think that lawyers will commonly agree that penal 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 (X) that satisfies the element of causation (p) intravirtually and can, therefore, not count as a crime (Y) in the context of the non-virtual world (C), although it may count as such in its virtual environment. But an existing penal provision may include in its scope a computer-simulated human act or human act made possible by computer simulation (X) that satisfies the element of causation (p) extravirtually and, therefore, counts as a crime (Y) not only in the context of its virtual environment, but also in the context of the non-virtual world (C). And it may also include in its scope a computer-simulated human act or human act made possible by computer simulation (X) that satisfies the element of causation of one crime intravirtually, thereby satisfying the element of causation 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).

In conclusion, a computer-simulated human act or human act made possible by computer simulation that satisfies the elements of a crime can only be brought under the scope of an existing penal provision if it has an extravirtual consequence and, therefore, counts as a crime in the non-virtual world. It is thus a *necessary* condition for the computer-simulated human act or a human act made possible by computer simulation that it has an extravirtual consequence. But is that also a sufficient condition for a computer-simulated human act or a human act made possible by computer simulation that satisfies the elements of a crime in order to be brought under the scope of existing penal law? Or are there other conditions 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.

2.2 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, 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 penal 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 penal 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 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 (Murphy & Coleman 1990, p. 40). 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. 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:

> "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 paper, 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 that are grounded in moral principles. Taking this assumption as a starting point, Van der Burg argues that the law is most strongly open to moral argument with regard to special fields or issues that are still developing, such as biotechnology or ICT (2010, pp. 22, 25). This claim can be explained as follows. As was discussed in the section 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 penal law, such as virtual cybercrime. It is not always clear how penal 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 the penal 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 the penal law should deal with virtual cybercrime. Answering this question will be the aim of the next subsection.

2.2.1 Which moral principles can help to determine how the penal law should deal with virtual cybercrime?

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 voluminous work *The Moral Limits of the 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 (1984, p. 7). According to Feinberg such an interference with the liberty of citizens by means of penal law is usually legitimated on the basis of one of the following liberty-limiting principles: the harm principle, the offense principle, legal paternalism or legal moralism (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 (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 (Ibid., 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 and economic stability or 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 (Ibid., p. 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 when caused by the wrongful conduct of others. Only offense in this latter sense is intended in 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 that are based on the offensive 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 is 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 nonvoluntary when the choice to perform it stems from coercion, drugs or other voluntariness-vitiating factors and is, therefore, 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). Feinberg, therefore, focuses on hard paternalism (Ibid., p. 6). Examples of penal provisions that are based on legal paternalism are: prohibitions on the possession and 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 (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 that are based on legal moralism are: prohibitions on prostitution and bigamy (Feinberg 1984, p. 13).

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 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 (...)" (1988, p. 323).

From an empirical point of view, it can be established that the harm principle is the most commonly and the most frequently used ground for criminalization. Although there are differences across countries and societies in how criminal behaviors are viewed and treated, the core of the criminal law, across geography and across time, consists of crimes that produce direct and serious harm to individual persons or groups. The 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). Penal provisions that are based on the offense principle, legal paternalism or legal moralism deviate across geography and across time.

In conclusion, the following moral principles can help to determine how the penal 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. We can now establish that that 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.

3 When do computer-simulated human acts or human acts made possible by computer simulation result in extravirtual harm, offense or evils of other kinds?

In this section I will take a so-called top-down approach[5]: 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. That way I 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.

3.1 Can computer-simulated human acts or human acts, made possible by computer-simulation result in extravirtual harm to others?

As was 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 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 the criminal law. Yet the question arises when a computer-simulated human act or a human act

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

made possible by computer simulation causes a wrongful setback to a welfare interest. Before answering this question, it is important to point at two supplementary principles that guide the application of the harm principle in practical contexts, however.

First, the harm principle makes sure that the criminal law does not concern itself with trivia. 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 the 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.

Second, and this supplementary principle is closely connected to the first, 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.

The 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 the criminal law protects interests of personality and interests of property. According to Feinberg standard interests of personality include absence of harmful bodily contacts or the apprehension thereof, freedom from confinement and absence of emotional distress. 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 the criminal law, however, some protect them instead by compelling compensation for harm to them under civil law (Feinberg 1984, pp. 61-62). Finally, as was mentioned earlier, the 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 e.g. through "stalking" or unpermitted disclosure of intimacies e.g. through unlawful 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 1.2.1 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 (http://www.wired.com/politics/security/news/2008/03/epilepsy). This was possibly the first human act made possible by computer simulation to inflict physical harm on persons and, to my knowledge, the only one. A computer-simulated human act could do the same type of harm if a user of a virtual environment, e.g. *SecondLife* or *MSN Messenger*, would, by the press of a button, make such a computer-generated animation designed to trigger seizures appear on the screen of another user, being a photo- and pattern-sensitive epileptic. And if virtual reality technologies would become multi-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 1.2, virtual reality technology allows a computer to give sensory feedback to a user through a dataglove or datasuit. If virtual reality technology would become multi-accessible in the future, one user could press a button and, thereby, command the computer to give certain harmful sensory feedback to another user, e.g. an electric shock causing a burn. In section 3.5 I will discuss the possibilities to do harm that virtual reality technologies might allow for in the future more in detail.

Much more often than harm to the bodily health of a person, computer-simulated human acts do harm to the "bodily health"[6] of a person's avatar. For example, a person can use his or her avatar to kill, 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

[6]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.

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 felt as mental harm to the person (Wolfendale 2007, p. 112, 114-115). 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 2.1.1 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).

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. Consider the following example. When Ailin Graef, the woman who became a millionaire by investing in virtual real estate in *SecondLife*, appeared through her avatar on a chat show in the virtual world of *SecondLife* 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 penises and photographs of Graef herself that were digitally altered to make her look like she was holding a giant penis. Graef felt sexually harassed (http://news.cnet.com/2100-1047-6147700.html). It is important to note that, in this case, the sexual harassment within the virtual world of *SecondLife* 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.

Mental harm to persons is not only done by computer-simulated human acts, but also by human acts made possible by computer simulation. For example, many virtual worlds (e.g. *SecondLife* and *World of Warcraft*) provide a chat interface, which users can abuse to send harassing messages to other users through their avatars. It should be added that 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. It is important to highlight that the harassment should be aimed at the user of the virtual world, not at the user's avatar. As became clear earlier, this can only be the case when the identity of the person behind the avatar is known to the perpetrator(s). It may be that the person behind the avatar has revealed his or her own identity, for instance in a chat conversation. It may also be that the perpetrator has unlawfully accessed the personal details of the person behind the avatar, e.g. by means of hacking.

It seems implausible that a computer-simulated human act or a human act made possible by computer simulation can cause extravirtual reductions of a person's liberty of movement through abduction or false imprisonment, at least I cannot think of an example. But a computer-simulated human act or a human act made possible by computer simulation can definitely cause a depletion of a person's material resources through larceny. I have extensively discussed this issue in my paper *Theft of virtual items in online mulitplayer computer games: an ontological and moral analysis* (2012). In short, if virtual property is purchased with funds having extravirtual value (value in the non-virtual world, e.g. pecuniary value), then the extortion thereof constitutes extravirtual harm. According to Brenner, the same will be true of other property deprivation crimes, such as robbery, fraud, arson or vandalism (2008, pp. 70-71).

Computer-simulated human acts or human acts made possible by computer simulation can raise privacy issues as well. One can, for example, think of stalking in a virtual world by means of following a person's avatar and repeatedly sending messages through a chat interface. One can also think of unauthorized filming within a virtual world. In *SecondLife*, for example, it is possible to film. Films made in *SecondLife* 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, unpermittedly disclose the avatar's intimacies. Just like with harassment, stalking or unauthorized filming in the virtual world can spill into the non-virtual world only when the perpetrator knows who the person behind the avatar is.

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 swastika's (Gerechtshof 's-Gravenhage, 16 November 2010, LJN: BO4035). One can also think of the defamation of avatars here, for example by means of a written statement on an Internet forum. Only when other users know who the person behind the avatar is, the defamation can also take effect in the non-virtual world and is, therefore, extravirtual.

Finally, computer-simulated human acts or human acts made possible by computer simulation can intrude upon public interests. It seems implausible that they can intrude upon the interest in a clean environment, but computer-simulated human acts or human acts made possible by computer simulation can definitely intrude upon the interest in economic stability. Counterfeiting, for example, can be made possible by computer simulation, for people can use graphics software to create false bank notes. And computer simulation can also play a role in intrusions upon political stability, since terrorists sometimes make use of the virtual worlds of computer games to plot attacks. For example, Anders Behring Breivik, the Norwegain accused perpetrator of the 2011 bomb attack and mass shooting in Norway, told the court that he "trained" for the shooting attacks he carried out by playing the computer game *Call of Duty: Modern Warfare* (http://www.guardian.co.uk/world/2012/apr/19/anders-breivik-call-of-duty).

3.2 Can computer-simulated human acts or human acts, made possible by computer-simulation result in 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). The offense principle cannot 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).

According to Feinberg examples of penal provisions that are 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 aforementioned 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.[7] The second category concerns the ridiculing or criticizing of beliefs and

[7]It actually also includes the sale and distribution of pornography, but Weckert has excluded pornography from his discussion, because it raises issues of its own (Weckert 2000, p. 108). He probably refers to the fact that feminist authors argue that pornography does not produce offense, but harm. See pp. 153-155 of my essay on virtual child pornography: Litska Strikwerda (2011). Virtual Child Pornography Why Images Do Harm from a

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 was mentioned above, Feinberg thinks that we have to balance the seriousness of the offense caused against the independent reasonableness (avoidability) of the offender's conduct when we invoke the offense principle. As Weckert points out, 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 chose not to visit that website. This would be different if one was 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 was confronted with the offensive material on the road one has 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, where offenses from the first 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, pp. 116-117).

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 themselves shape the virtual world, such as *SecondLife*, 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 also only offenses from the third category are serious enough to tip the scales and invoke the offense principle. 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 chat function. But they can also consist of computer simulated images (Weckert 2000, p. 106). In the United Kingdom, 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 (http://www.independent.co.uk/news /uk/crime/internet-ban-for-offensive-image-7575915.html). The aforementioned acts are all human acts made possible by computer simulation. Computer-simulated human acts can produce offenses from

---

Moral Perspective. In Charles Ess & May Thorseth (Eds.), *Trust and Virtual Worlds Contemporary Perspectives* (pp. 139-161). New York: Peter Lang Publishing. The discussion on pornography goes beyond the scope of this paper, however.

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 the person behind the avatar is black him- or herself, he or she can take offense.

It becomes clear here that offense in the virtual realm differs in one important aspect from harm in the virtual realm: contrary to harm, we cannot distinguish between intra- and extravirtual offense. In section 2.2.1 harm was defined as a wrongful setback to an interest. As was established in section 3.1, a wrongful setback to an interest can be either intra- or extravirtual. Sometimes, an intravirtual wrongful setback to one interest counts as an extravirtual wrongful setback to another interest. As was 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).

3.3 Can computer-simulated human acts or human acts, made possible by computer-simulation result in extravirtual harm to the self ?

As was established in the last section, the 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 3.1 we 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 reduces his or her own liberty of movement through abduction or false imprisonment or that a person violates 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, Gerald Dworkin lists the following eleven examples of paternalistic interferences by law:

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."

(Dworkin 1972, pp. 65-66)

Not all of these examples concern the criminal law. The fourth, eighth and tenth example concern laws that are generally not part of the criminal law. With regard to the fifth example, it should be added that most countries have repealed their laws against homosexuality. 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 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 choose (Ibid.). So we could say that, in the case of professional licensing, the practitioner is coerced so that the would-be patient or client cannot choose to be treated be 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 self-harming prohibited human activities above. One can, for example, make an avatar drive a motorcycle without a safety helmet or swim at an unguarded beach. And as was mentioned in section 2.1.1 people can use a drug called "Seclimine" through their avatars within the virtual world of *SecondLife*. Also, many multiplayer computer games, e.g. *World of Warcraft*, 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. The only computer-simulated human act that can actually cause extravirtual harm to the self is the act of gambling on a virtual slot machine. As was already discussed in section 2.1.1 that is because the computer-simulated human act of gambling on a virtual slot machine involves real, non-virtual money and can thus cause financial losses in the non-virtual world.

I can think of two examples of human acts made possible by computer simulation that can cause extravirtual bodily harm to the self. First, suicide can be made possible by the Internet and, conceivably, also by computer simulation. In the Netherlands there exists a "suicide foundation". They have a website (<http://deeinder.nl>) through which people who want to commit suicide can contact a "suicide counselor". According to the website, suicide counselors offer "information and counseling" for those wanting to kill themselves (<http://deeinder.nl>). In 2005 one of these suicide counselors was convicted for the crime of

aiding and abetting a suicide. He had not only advised a "client" on fatal drug cocktails, but he had also provided her one. He had summoned people to send him all sorts of prescription drugs. Once he had collected enough of the right prescription drugs to mix a fatal drug cocktail, he sent it to the client. She committed suicide by taking the fatal drug cocktail that she obtained from him. The suicide counselor was sentenced to one year of imprisonment (Rechtbank Alkmaar, 7 December 2005, LJN: AU7519). A suicide foundation could also be set up in a metaverse, like *SecondLife*. People could then consult a suicide counselor through their avatars and maybe even trade prescription drugs among each other or through the suicide counselor so that they could save up for a fatal drug cocktail which they could use to commit suicide.

Second, unlicensed practice of medicine can be made possible by the Internet and, conceivably, 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). So far, one fatal case of do-it-yourself-healthcare by the use of health information on the Internet has been reported. 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 *SecondLife* one can find several virtual hospitals. In some of them one can also consult a virtual doctor. Here, the reliability problem arises as well. After all, it is difficult to establish whether or not the person behind the virtual doctor is a licensed doctor. Thus, taking a medical advice from a virtual doctor can be as dangerous for one's own health as relying on health information on the Internet.

3.4 Can computer-simulated human acts or human acts, made possible by computer-simulation result in extravirtual evils of other kinds?

As was established in the last section, (pure) legal moralism entails that it is legitimate to prohibit conduct on the ground that it is inherently immoral, although it causes neither harm nor offense to the actor or to others. Examples of penal provisions that are 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 that are 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 the metaverse of *SecondLife*. Some people sell sex through their avatars there. They usually work for a virtual escort service or a virtual bordello. Like in the non-virtual world, they charge their clients for their services and give the owner of the escort service or bordello a percentage of their earnings. 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 as were discussed in section 2.1.1 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). 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 (Ibid., p. 68). The offense principle, which generally offers ground to prohibit pornography, cannot be invoked either, however. As was established in section 3.2 , we have to balance the seriousness of the offense caused against the independent reasonableness (avoidability) of the offender's conduct when we invoke the offense principle. 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 3.2 it was explained that pornography is not a serious enough offense that is to do that.

Bigamy can also occur in *SecondLife*. 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 *SecondLife* unions (Ibid., p. 69). And, therefore, the underlying traditional concerns about morality that historically gave rise to the criminalization of bigamy do not apply either.

Prostitution or bigamy cannot be made possible by computer simulation, at least I cannot think of examples. Thus, neither of Feinberg's examples of penal provisions that are based upon legal moralism are applicable to the virtual realm. Nevertheless, there is one prohibition on a human act made possible by computer simulation that seems to be based on legal moralism and that is the prohibition on the production, distribution and possession of virtual child pornography, as was discussed in section 1.2.1. I have written extensively on this topic in my paper *Virtual Child Pornography Why Images Do Harm from a Moral Perspective* (2011). In this paper I argue, in short, that virtual child pornography does not do harm to others, because, contrary to non-virtual child pornography, no actual children are involved in the production (Strikwerda 2011, pp. 142-146).[8] It does not do harm to the self either, at least there is not enough evidence that it would encourage or seduce children into participating in sexual contacts with adults or that it would encourage or seduce peadophiles to commit child abuse (Strikwerda 2011, pp. 147-151). And virtual child pornography cannot be brought under the scope of the offense principle, because it is not traded in public, but secretly among peadophiles, and, therefore, there are no unwilling spectators who are deprived of the power to determine for themselves whether or not to see these images. Feinberg distinguishes a special class of cases where we are offended at the "bare thought" that the conduct occurs (Feinberg 1988, p. 15). I think that the production, distribution and possession of virtual child pornography belongs to this special class of cases. According to Feinberg, conduct that offends at bare thought is found offensive, because it is judged to be immoral. Therefore, it should be brought under the scope of legal moralism (Ibid.). In my paper I have claimed that virtual child pornographic images are generally judged to be immoral, because they flout our sexual mentality, which is based on the equality norm, for sex between adults and children is per definition unequal (Strikwerda 2011, pp. 157-159). The production, distribution and possession of virtual child pornography thus results in an evil of another kind than harm (to others or to the self) or offense.

[8]Note that child pornography differs essentially from adult pornography because children cannot consent to sex. Sex with children is, therefore, always considered abuse or rape. Child pornography is thus a recording of abuse and rape and is prohibited on the ground that it harms children and not on the ground that it is offensive.

3.5 Some short comments on what the future holds

In the sections 1.2.1 and 3.1 it was noted that virtual reality technologies will probably allow for new possibilities to do harm to others when they become multi-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 to give offense, do harm to the self or to act inherently immoral.

Philip Zhai (1998) 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 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 that are in accordance with one's changing video and audio sensations. Moreover 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. This way one is fully immersed in a virtual world, 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 world 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 world one can also meet other human beings. They may be virtual human beings whose behavior is totally programmed by the computer (Zhai 1998, p. 49). But they may also be the virtual representations of persons who are wired to the same computer as one is oneself. When one interacts with them, one does not only get the sensory feedback belonging to the act oneself, but they also get the sensory feedback 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 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, for example, describes how two persons wired to the same computer could have sex through "a seamless combination of digital simulation, sensory immersion, and functional teleoperation" (1998, p. 169).

Zhai does not think that human interactions mediated by virtual reality technologies can be harmful. He states: "(...) in the virtual world, 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 what if a user hacks the program of another user and changes the settings? Then one could hit, kick or otherwise physically hurt the virtual representation of the other person wired to the same computer 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 oneself: one could hack into the program of a user of a

virtual reality technology and add to it a virtual human being that hits, kicks or does another kind of bodily harm. 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 inherently immoral.

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 3.2 that offense in the virtual realm differs in one important aspect from harm in the virtual realm, because, contrary to harm, we cannot distinguish between intra- and extravirtual offense. 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. 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.

Virtual reality technologies could allow for new possibilities to do harm to the self though. 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 other types of harm to the self. 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 the criminal law.

Virtual reality technologies could also allow for new possibilities for inherently immoral behavior. In section 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 was mentioned above, Zhai claims that people might be able to have sex in the virtual world in the future. If so, they can also sell sex and thus prostitute themselves in the virtual world. 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, body suit 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 sense like they are kissed. Once the law would recognize marriage by proxy through virtual reality technology, bigamy through virtual reality technology would also be possible.

Finally, it might be worth to point 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 messed 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). That way (un)intended harm to the self can cause harm to others. One could also confuse a virtual human being with the virtual representation of another person wired to the same computer. 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 the criminal law, however. As was established in section 2.1.1 one of the basic elements that is required by each crime is a *mens rea* (a blameworthy mental state, usually it is required 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. When 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 the criminal law.

4 Conclusion

In this paper I have studied the question when virtual cybercrime should be brought under the scope of the criminal law. The paper consists of three parts. The first part of the paper is an empirical exploration; in this part I have examined what virtual cybercrime is and how, if at all, it is treated within existing legal systems. The second part of the paper is a philosophical analysis; in this part I have established, drawing from ontology and legal philosophy, what the necessary and sufficient conditions are for virtual cybercrime to obtain in order to count as crime under existing law. The third part of the paper is a moral evaluation; in this part I have studied when virtual cybercrime meets the aforementioned criteria.

In the first part of the paper I have 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 have 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, offences related to child pornography, offences 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 offence 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 offence categories concern traditional crimes where computers or computer networks are used as a tool to commit the crime in a different way.

Subsequently, I have 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. Contrary to ordinary cybercrime, virtual cybercrime does not concern new human activities; only different human activities. Therefore, it requires legislators to extend existing laws, but 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. Currently, the production, possession and distribution of virtual child pornography is the only virtual cybercrime that is commonly prohibited, although not as commonly as non-virtual child pornography. Putative virtual cybercrimes are, for example, virtual rape, virtual killing and theft of virtual items.

In the second part of the paper I have explained that an empirical study of the law 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 to obtain in order to be prohibited under existing law, since the production, distribution and possession of virtual child pornography is the only virtual cybercrime that is 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 have studied virtual cybercrime from a different point of view. As was stated in the introduction, the study of virtual cybercrime belongs to the field of legal ontology. Applied forms of ontology often put to use the tools of philosophical ontology in order to categorize things within a specific domain. I made use of this method and put to use the tools of the philosophical ontology of the American philosopher Searle 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. 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 have 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 it is required 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 have 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 have 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) also 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 have 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, its virtual environment or the non-virtual world, determines whether the act can be included in the scope of an existing penal provision. I have explained that lawyers commonly agree that penal 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 the 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 have 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 penal 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 penal 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. 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 have 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 the penal law should deal with virtual cybercrime.

In the third part of the paper I have 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 have 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 have claimed that computer-simulated human acts or human acts made possible by computer simulation can result in a couple of forms of extravirtual harm to the self and that they can, therefore, be brought under the scope of legal paternalism. Subsequently I have 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. Last I have 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 inherently immoral, 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.

In conclusion, those computer-simulated human acts or human acts made possible by computer simulation that result in extravirtual harm to others, offense, harm to the self or evils of other kinds should be brought under the scope of the criminal law, provided that they also satisfy the (other) elements of a crime.

Bibliography

Allen, Colin (2010). Artificial life, artificial agents, virtual realities: technologies of autonomous agency. In Luciano Floridi (ed.), *The Cambridge Handbook of Information and Computer Ethics* (pp. 219-233). Cambridge: Cambridge UP.

Beauchamp, Tom 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.

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

Brey, Philip (2008). Virtual Reality and Computer Simulation. In Kenneth Einar Himma and Herman T. Tavani (eds.), *The Handbook of Information and Computer Ethics* (pp. 361-384). Hoboken (NJ): John Wiley and Sons Inc.

Brey, Philip (forthcoming). The Physical and Social Reality of Virtual Worlds.

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

Clough, Jonathan (2010). *Principles of Cybercrime*, Cambridge: Cambridge UP.

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

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

Devlin, Patrick (1965). *The Enforcement of Morals*. Oxford: Oxford UP.

Dibbell, Julian (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.

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

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

Feinberg, Joel (1984). *The Moral Limits of the Criminal Law, Volume One, Harm to Others*. Oxford: Oxford UP.

Feinberg, Joel (1985). *The Moral Limits of the Criminal Law, Volume Two, Offense to Others*. Oxford: Oxford UP.

Feinberg, Joel (1986). *The Moral Limits of the Criminal Law, Volume Three, Harm to Self*. Oxford: Oxford UP.

Feinberg, Joel (1988). *The Moral Limits of the Criminal Law, Volume Four, Harmless Wrongdoing*. Oxford: Oxford UP.

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

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

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

Chuck Huff, Deborah G. Johnson and Keith Miller (2003). Virtual Harms and Real Responsibility. *IEEE Technology and Society Magazine*, 12-19.

Johnson, Deborah G. (2001). *Computer Ethics*, New Jersey: Prentice-Hall Inc.

Kerr, Orin 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

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

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

Moor, James H. (1985). What is Computer Ethics?. *Metaphilosophy, Vol. 16:4*, 266-275.

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

Powers, Thomas M. (2003). Real wrongs in virtual communities. *Ethics and Information Technology, 5*, 191-198.

Searle, John R. (1995). *The Construction of Social Reality*. New York: The Free Press.

Searle, John R. (2001). *Rationality in Action*. Cambridge (Massachusetts): The MIT Press.

Searle, John R. (2010). *Making the Social World. The Structure of Human Civilization*. New York: Oxford University Press Inc.

Strikwerda, Litska (2011). 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.

Strikwerda, Litska (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.

Søraker, J.H. (2010). *The value of virtual worlds / A philosophical analysis of virtual worlds and their potential impact on well-being* (doctoral dissertation). Enschede: Ipskamp.

Tavani, Herman T. (2007-2). *Ethics & Technology. Ethical Issues in an Age of Information and Communication Technology*. Hoboken (NJ): John Wiley & Sons Inc.

Van der Burg, Wibren (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.

Weckert, John (2000). Offence on the Internet. In Göran Collste (ed.), *Ethics in the Age of Information Technology* (pp. 104-118). Linköping: Centre for Applied Ethics.

Wolfendale, Jessica (2007). My avatar, my self: Virtual harm and attachment. *Ethics and Information Technology, 9,* 111-119.

Zaibert, Leo & Smith, Barry (2007). The varieties of normativity: an essay on social ontology. In Savas L. Tsohatzidis (ed.), *Intentional Acts and Institutional Facts / Essays on John Searle's Social Ontology* (pp. 157-173). Dordrecht: Springer.

Zhai, Philip (1998). *Get Real. A Philosophical Adventure in Virtual Reality*. Lanham (USA): Rowman & Littlefield Publishers.

Table of legal documents

Council of Europe, Convention on Cybercrime and Explanatory Report, Budapest, 23 November 2001 (CETS No.185). Accessible via <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). Accessible via <http://conventions.coe.int>.

Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and Explanatory Report, Lanzarote, 25 October 2007 (CETS No. 201). Accessible via <http://conventions.coe.int>.

Table of cases

Hoge Raad, 31 January 2012, LJN: BQ9251. Accessible via <http://www.rechtspraak.nl>.

Gerechtshof 's-Gravenhage, 16 November 2010, LJN: BO4035. Accessible via <http://www.rechtspraak.nl>.

Gerechtshof Leeuwarden, 10 November 2009, LJN: BK2773, BK2764. Accessible via <http://www.rechtspraak.nl>.

Rechtbank Amsterdam, 2 April 2009, LJN: BH9789, BH9790, BH9791. Accessible via <http://www.rechtspraak.nl>.

Rechtbank Alkmaar, 7 December 2005, LJN: AU7519. Accessible via <http://www.rechtspraak.nl>.