FIDIS

Future of Identity in the Information Society

Title:	"D17.2: New (Id)entities and the Law: Perspectives on Legal Personhood for Non-Humans"
Author:	WP17
Editors:	Bert-Jaap Koops (TILT, Netherlands) David-Olivier Jaquet-Chiffelle (VIP, Switzerland)
Reviewers:	Jozef Vyskoc (VaF, Slovakia) Hans Buitelaar (TILT, Netherlands)
Identifier:	D17.2
Type:	[Report]
Version:	1.0
Date:	24 October 2008
Status:	[Final]
Class:	[Public]
File:	fidis-wp17-del17.2-new_entities_and_law_def.pdf

Summary

New entities in the information society that operate at increasing distance from the physical persons 'behind' them, such as pseudonyms, avatars, and software agents, challenge the law. This report explores whether such entities – abstract persons – could be attributed legal rights and/or duties in some contexts, thus creating entities that are addressable in law themselves rather than the persons 'behind' them. Are current legal constructions sufficient to solve potential conflicts involving new entities, or would it help to create (limited) legal personhood for these new entities? The report identifies three strategies for the law to deal with the challenge of new entities: interpreting existing law, changing the law with specific rules, and changing the legal system by granting limited or full legal personhood to new entities. It provides a tentative conclusion and an agenda for further research.

The FIDIS NoE receives research funding from the Community's Sixth Framework Program

Information Society Technologies

Copyright Notice

PLEASE NOTE: This document may change without notice. Updated versions of this document can be found at the FIDIS NoE website at www.fidis.net.

Members of the FIDIS consortium

1. Goethe University Frankfurt	Germany
2. Joint Research Centre (JRC)	Spain
3. Vrije Universiteit Brussel	Belgium
4. Unabhängiges Landeszentrum für Datenschutz	Germany
5. Institut Europeen D'Administration Des Affaires (INSEAD)	France
6. University of Reading	United Kingdom
7. Katholieke Universiteit Leuven	Belgium
8. Tilburg University	Netherlands
9. Karlstads University	Sweden
10. Technische Universität Berlin	Germany
11. Technische Universität Dresden	Germany
12. Albert-Ludwig-University Freiburg	Germany
13. Masarykova universita v Brne	Czech Republic
14. VaF Bratislava	Slovakia
15. London School of Economics and Political Science	United Kingdom
16. Budapest University of Technology and Economics (ISTRI)	Hungary
17. IBM Research GmbH	Switzerland
18. Institut de recherche criminelle de la Gendarmerie Nationale	France
19. Netherlands Forensic Institute	Netherlands
20. Virtual Identity and Privacy Research Center	Switzerland
21. Europäisches Microsoft Innovations Center GmbH	Germany
22. Institute of Communication and Computer Systems (ICCS)	Greece
23. AXSionics AG	Switzerland
24. SIRRIX AG Security Technologies	Germany

Versions

Version	*Date*	*Description (Editor)*
0.1	18.06.2008	- first versions of chapters (all authors)
0.2	08.08.2008	- first integrated version (BJK)
0.3	03.09.2008	- second integrated version (HZ)
0.4	21.09.2009	- third integrated version (DOJC, HZ, MH)
0.5	26.09.2008	- final version for internal review (BJK)
1.0	24.10.2008	- final version (all authors, BJK)

Foreword

FIDIS partners from various disciplines have contributed as authors to this report. The following list names the contributors for the chapters of this report.

Chapter	*Contributor(s)*
Executive Summary	Bert-Jaap Koops (TILT)
1 Introduction	Bert-Jaap Koops (TILT) David-Olivier Jaquet-Chiffelle (VIP)
2 Current law	Mireille Hildebrandt (VUB) Harald Zwingelberg (ICPP)
3 New types of abstract persons	Harald Zwingelberg (ICPP) Maurice Schellekens (TILT)
4 New legal abstract persons?	Mireille Hildebrandt (VUB)
5 Conclusion	Bert-Jaap Koops (TILT)

Table of Contents

Executive Summary

Technological developments in the information society bring new challenges, both to the applicability and to the enforceability of the law. One major challenge is posed by new entities that operate at increasing distance – in every sense of the term – from the physical persons 'behind' them, such as pseudonyms, avatars, and software agents. In case of accidents or misbehavior, current laws require that the physical or legal person(s) 'behind' the entity is found so that she can be held to account. This may be problematic if the linkability of the identities of entity and principal is questionable.

The FIDIS workpackage «Abstract persons» aims to better understand the impact of these new entities, which function like 'abstract persons': virtual entities that can have (not necessarily legal or moral) rights, duties, obligations and/or responsibilities associated to them in a certain context. This report explores whether abstract persons could also be attributed *legal* rights and/or duties, thus creating entities that are addressable in law themselves rather than the persons 'behind' them. A closer look is provided at arguments pro and con legal personhood for non-human entities, including a discussion of alternative approaches to solving the emerging 'accountability gap'. The research question in this report is:

> Given the rise of new entities in the information society that operate at increasing distance from the persons who employ them, are current legal constructions sufficient to solve potential conflicts, or would it help to create (limited) legal personhood for these new entities in some contexts?

The report discusses how the law currently deals with abstract persons, noticing the generality of the law and generic legal constructs like (legal) agents and personhood. Three types of new entities are discussed in-depth: pseudonyms, avatars, and software agents, sketching legal problems that arise and indicating how current law addresses these problems. Then, a more generic study is undertaken to assess the merits and pitfalls of attributing personhood to new non-human entities.

The analysis shows that various types of 'personhood' exist. In increasing order of 'personality', entities can be abstract persons, legal persons, moral persons, and social persons, with abstract persons being the widest class of 'person' (which includes software or a machine with, e.g., access rights) and social persons being the narrowest class of those whom society considers to be 'full' or 'real' persons (which includes most human beings). The key question in this report is whether some abstract persons in some contexts could 'step up' one category and enter the more inner circle of legal persons, or perhaps even – in the long term – reach the category of moral or social persons.

Legal personhood is associated with legal consequences that attach to the capacity to act, involving civil actions (such as contracting) and criminal actions (committing a crime). For personhood to be meaningful, this means that an entity should be capable of performing such actions and of bearing the legal consequences, which is particularly relevant when something goes wrong. We can distinguish between a limited legal personhood (civil actions and some liability for criminal actions, associated with juridical persons like companies) and a full legal personhood (including full criminal liability, associated with moral persons like human beings).

Facing the challenge of emerging abstract entities that operate at increasing distance from persons who employ them, the legal system has three potential courses of action. First, it can *interpret* the law and incorporate the new technical developments in the existing legal system, for example, applying existing legal doctrines of messenger, principal and undisclosed and

disclosed agent, actual and ostensible agent, and newly developed theories like the programmed will, to electronic agents to determine who is liable in case of conflicts. For today's electronic agents, this is sufficient, but for tomorrow's agents, this strategy might stretch legal interpretation to the point of breaking.

Then, the second strategy is to *change* the law using *specific* constructions, like introducing sector-specific rules for electronic agents. Solutions proposed in the literature include a public register for agents with certification, victim funds, and insurance in case errors occur.

Such constructions can evolve into the third strategy, namely to *change* the *legal system* itself. Creating legal personhood for new actors is such a strategy, which has in the past been used to meet the increasingly complex social interactions of companies and states. Electronic agents could likewise be given limited legal personhood, with ability to contract and to pay for civil damages (and earning money to pay for this). Currently, it does not solve much to do this, but with on-going technological developments that create more and more truly autonomic entities, it is an option worth considering in the longer term. It is even imaginable, at least for proponents of a functional approach to law, that electronic agents could ultimately be attributed moral personhood, if they ever gain the ability to make decisions that are functionally equivalent to moral decisions. Although it is more far-fetched for current instances, other abstract persons could, as their technology evolves in the next decades, also benefit from limited legal personhood, to smooth their economic functioning (for pseudonyms with a valuable reputation) or to protect them (for avatars with strong emotional ties in social relationships).

Whether it makes sense to speculate on such future strategies to deal with new abstract persons, will depend on one's outlook on law and technology, on what constitutes a true 'person', and on how the world is changing. For the time being, the research question can fairly easily be answered: current legal constructions suffice to solve potential conflicts that arise through the increasing distance between emerging abstract entities and the persons who employ them. There is no need to give legal personhood, even of the limited type to enable contracting and paying civil damages, to abstract persons. As technology evolves and entities like pseudonyms, avatars, and particularly electronic agents become more autonomic and acquire a 'personality' of their own, however, it might be useful to treat them as new identities in themselves with certain legal rights, duties, obligations, and/or responsibilities. Should their autonomy reach such a level that they have a functional equivalent of self-consciousness, we may even consider giving them full legal personhood.

This tentative conclusion leaves open various questions that merit further study and debate. The report therefore ends with an agenda for further research. It is recommended that policy makers facilitate this research and societal debate. Timely addressing these further questions will prepare society for the advent of truly autonomic, and who knows autonomous, technologies that are likely to gain a foothold in tomorrow's information society.

Abbreviations

AG	Aktiengesellschaft (public limited company)
BGB	Bürgerliches Gesetzbuch (German Civil Code)
BDSG	Bundesdatenschtuzgesetz (German Federal Data Protection Act)
BV	Besloten Vennootschap (private company) (Netherlands)
CSP	Certification Service Provider
DCC	Dutch Civil Code
ECHR	European Convention on Human Rights
EDI	Electronic Data Interchange
GmbH	Gesellschaft mit beschränkter Haftung (private limited company)
GmbHG	Gesetz betreffend Gesellschaften mit Beschränkter Haftung (German Limited Liability Company Law)
HGB	Handelsgesetzbuch (German Commercial Code)
s.	section
SigG	Signaturgesetz (Law on electronic Signatures)
StGB	Strafgesetzbuch (German Criminal Code)
TMG	Telemediengesetz (German Law on Telemedia)
UGB	Unternehmensgesetzbuch (Austrian Commercial Code)
U.S.C.	United States Code
VwVfG	Verwaltungsvrfahrensgesetz (German Law on Administrative Procedure)
ZGB	Zivilgesetzbuch (Swiss Civil Code)
ZPO	Zivilprozessordnung (German Code of Civil Procedure)

1 Introduction

1.1 New challenges to technology and law

Technological developments in the information society bring new legal and technical challenges. This concerns both the applicability and adequacy of current laws and the enforceability of these laws. The new challenges cannot be solved by law or technology alone; they require an interdisciplinary approach that can combine innovative solutions with a thorough understanding of both technology and law.

To briefly illustrate some of the new developments and challenges, we will follow a what? where? when? why? who? approach. For example, **what** can be considered as property in law? Can a unique and precious virtual object in an on-line game be considered as property recognised by today's laws?

Where did the crime of criminal threat take place, if a Swiss resident during a workshop in Brussels reads a threatening email on his Gmail account that is stored on a server in the USA, which message was sent by someone from Germany via a Malaysian Internet provider? If some "physical presence" is a legal condition for the *locus delicti* in a crime, this has to be interpreted in the light of new technologies: is it the location of the person sending or reading, or the location of servers storing and transmitting the message that are constitutive of jurisdiction, or all of these? **When** is an electronic contract concluded for buying a camera online: when the 'OK' button is pressed by the consumer, when the OK message reaches the webshop, when a receipt acknowledgement is sent by the webshop, or when the acknowledgement is received by the consumer?

In order to assess responsibility, the reason **why** an action took place sometimes has to be determined. Was the email threat actually sent with the intent of criminal threat, and did the consumer really intend to buy the camera? Can non-human entities, like a software agent, be considered to have their own will and take independent decisions?

The widespread use of persistent pseudonyms on the Internet, for example of an eBay e-tailer or consumer, raises questions about the link between a transaction and the physical person with whom the transaction is made, since this person is often invisible for most observers. How do we deal with this new reality, when if something goes wrong, no physical person can be linked with a reasonable amount of effort to the transaction? **Who** is responsible and will bear the (legal) consequences? New forms of unlawful activities take advantage of these grey zones, where the law is theoretically applicable but becomes very hard to enforce in a globalised cyberworld.

1.2 The FIDIS concept of abstract persons

The FIDIS workpackage «Abstract persons» studies in particular the "who" aspects, i.e., the core issues directly related to *identity*, *identification* and *authentication* in the information society. It aims to better understand the impact of new entities, such as avatars, digital pseudonyms, and software agents, on the information society and on the legal framework that regulates the information society. We investigate whether we can treat emerging new entities as separate, independent and meaningful entities, i.e., with some kind of 'personality' of their own rather than being mere extensions of the human beings using them. If so, we can call them ‘abstract persons’: virtual entities that can have rights, duties, obligations and/or responsibilities[1] associated to them in a certain context.

In FIDIS deliverable 2.13, *Virtual Persons and Identities*,[2] a new model is defined with two layers: the physical world and the virtual world[3]. It allows a precise and unifying representation of new forms of identities in the information society. The virtual world allows a unified description of many identity-related concepts that are usually defined separately without taking into consideration their similarities: avatars, pseudonyms, categories, profiles, legal persons, etc. This unified description is based on a generalisation of the traditional concepts of a virtual person. Abstract entities belong to the virtual world.

Laws have a long experience of using abstract entities to define rules, categories, etc., in order to associate legal rights, obligations, and responsibilities to persons that can in concrete situations be considered instances of these abstract entities. The law does not say that John Doe will inherit his mother’s fortune when she dies, but defines generically who is the ‘heir’ under which conditions. The application of the law in a specific situation makes an entity with legal personhood the bearer of the legal rights, legal obligations, legal responsibilities associated to one of these abstract entities that the law uses. The model developed in D2.13 intentionally uses a similar construction. Therefore, the model might learn from the long experience of handling abstract entities in law to refine some of its concepts specifically for the legal framework. Reciprocally, the legal framework might use this generic model to represent its abstract entities as well as new abstract entities together. This might be useful if current laws need to be adapted to encompass new paradigms, such as the rise of autonomically[4] acting entities, to better understand if and when new laws or even new legal persons have to be created as a response to new technological developments.

The abstract layer in the model is particularly well-suited to describe (new) entities operating at an increasing distance from the physical or legal persons behind them. It recognises the existence of these (new) intermediate entities and explicitly incorporates them in the model. Some of these intermediate entities are recognised as persons in law (e.g., companies), others are not.

The concept of virtual persons in the FIDIS model is very general; this is necessary in order for it to cover all possibly relevant entities with respect to rights, obligations and responsibilities. Of course, not all virtual entities can have the same legal status or even have a legal status; in particular, not all virtual persons will have legal personhood. For example, avatars – a typical, traditional example of a virtual person, who have in-game rights and duties[5] – do not have legal personhood, and they very well may never acquire it. However, for some types of new entities it might be useful to extend ‘virtual personhood’ to legal personhood, if their position and functioning in society warrants giving them legal rights and duties.

[1] These rights etc. are not necessarily legal or moral in nature.

[2] Jaquet-Chiffelle 2008. The term ‘virtual person’ in that report is a synonym for the term ‘abstract persons’ that we prefer to use in this report.

[3] ‘Virtual world’ here does not denote ‘cyberspace’, but an abstract environment, which is a product of the mind rather than of matter.

[4] On the concept of autonomic entity, see section 4.3.

[5] This illustrates that the term ‘person’ is not restricted to entities with legal personhood; it is thus a broader concept than the legal notion of ‘person’.

1.3 Abstract persons and the law

New entities that operate at a distance from physical persons and actions appear in the information society. For example, pseudonyms can make the link between a physical person and her actions invisible; avatars interact intimately while their users may be thousands of miles apart; mobile software agents act and contract on behalf of a user who may be located in a faraway, even unknown jurisdiction. In case of accidents or misbehavior, current laws require that the physical or legal person 'behind' the entity is found so that she can be held to account.

In case of a pseudonym, the physical person who uses the pseudonym is legally responsible; however, the law too often becomes useless because it is hard to enforce legal rights. Indeed, the link between the physical person and her pseudonym can often not be revealed with a reasonable amount of effort. In case of a software agent, who is the person responsible – its programmer, its seller, or its user? What happens if the software agent adapts itself and learns from its environment, so that it behaves in an intrinsically unpredictable way? Is it then still meaningful to find a physical person or another entity with legal personhood who is accountable for the behavior of this software agent?

In this report, we explore whether rights and/or duties and responsibilities can be attached to new entities themselves rather than to the persons 'behind' them, as a potential way of addressing the challenges we face. New entities, seen as 'abstract persons' that perhaps can be incorporated as a new kind of 'person' in law, might thus contribute to making the law and its enforceability 'information society-proof'.

To be sure, it is – at least at this point in time – not necessary to give legal personhood to avatars or software agents. The law has a respectable tradition in flexibly incorporating social and technological developments in its system. New conditions created by new paradigms have often successfully been interpreted in terms of the existing legal framework. Historically, when this interpretation becomes too difficult or too costly to maintain, the legal system has proven itself dynamic enough to move along with new paradigms: new legal constructions or even new legal entities have been created. For example, legal subjectivity has been granted to non-human entities, such as companies, trust funds, and states.

Now, when an action or a transaction is realised with the help of an intermediate acting abstract entity, and when this action or transaction cannot be linked to the person who is legally responsible today, what are solutions to make the law applicable and enforceable? Can current laws comfortably incorporate the new entities, or do we need to use again the dynamism of the legal system to create new legal constructions or even new legal persons?

1.4 A crazy idea? Two provocative pleas for personhood

Attributing legal personhood to avatars or software agents may sound like a crazy idea to many readers. Avatars cannot be put in jail (not in a real-world jail, that is), and pseudonyms have no money to pay damages. A software agent has no self-consciousness to reflect on issues of right and wrong, and hence cannot learn from legal verdicts. Why would long-standing legal solutions for 'distance conflicts' not suffice, such as strict liability or victim funds?

We recall that a company is a legal person, even though it is not self-conscious and cannot be put in jail. Functionally, however, the organs of a company are self-conscious and can learn from legal verdicts, and a company can be given a hefty fine instead of a jail sentence. It is therefore not evidently impossible to attribute legal rights and responsibilities to other non-humans.

In fact, various scholars have argued that new entities *should* be given legal personhood. Before embarking on our own perspectives on this issue, we give two appetizing lines of argument from others as food for thought. This may serve to illustrate that the question we pose in this report is not such a crazy idea after all.

In a provocative Max Weber Lecture at the European University Institute in Florence, Gunther Teubner (2007) has argued that

> there is no compelling reason to restrict the attribution of action exclusively to humans and to social systems [i.e., legal persons like companies and states, eds] (…). Personifying other non-humans is a social reality today and a political necessity for the future.

In particular, Teubner – from a systems theory perspective – considers electronic agents and animals (or, more generally, ecological species) to be candidates for legal personhood, since in current society, they raise significant problems leading to substantial uncertainty. In his view, attributing personhood is a mechanism for social systems to reduce uncertainty: viewing a complex entity as a person enables you to communicate with it and to mutually establish expectations. In fact, 'through personification, the social system "parasitises" the intrinsic dynamics of autonomous processes in its environment.'[6] Depending on the entity and the social context, legal capacity for action can selectively be attributed; in the case of animal rights, these are basically defensive institutions (to preserve ecology), whereas in the case of electronic agents, legal personification enables them to act in an economic and technologically significant way.[7]

Another 'plea for legal change' – as his subtitle emphasises – is given by Andreas Matthias (2008), who has explored conditions for legal, moral, and social personhood and applied these to self-learning and self-adapting technology. He identifies an 'accountability gap' (*Verantwortungslücke*):

> there exists a growing class of accidents caused by machines, where the traditional ways of attributing responsibility are no longer compatible with our feeling of justice and the moral preconditions of society, since no-one has sufficient *control* over the actions of the machine, to be able to take responsibility.[8]

Matthias articulates five (cumulative) conditions for the ability to carry legal responsibility: intentionality, receptivity and responsiveness to causes, having second-order desires, legal sanity, and ability to distinguish between intended and merely foreseeable consequences of actions.[9] Interpreting these conditions in a functional way, he argues that legal accountability could accrue to certain classes of machines (software and/or hardware) – perhaps not current ones, but those in the foreseeable future that are even more self-learning and autonomic than today's machines. He observes that 'persons' and 'human beings' should not be equated off-hand, since history and culture teach us that many humans were (and sometimes are) not considered by society or law as persons, and vice versa.

Thus, Matthias' analysis warns us not to interpret criteria for personhood in an anthropomorphic way, but functionally in terms of whether the goals of legal accountability

[6] Teubner 2007, p. 7.

[7] Ibid., p. 20.

[8] Matthias 2008, p. 22 (emphasis in original, our translation).

[9] Ibid., p. 46ff.

can be met. Thus, machines can 'learn' and 'be educated' (e.g., through neural networks that can incorporate legal decisions into their rule system), and they can earn and administer money (since they perform economic tasks and can learn to manage bank accounts) out of which damages can be compensated. Even the criminal goal of retribution can be reached, because, even if the machine does not observe retributive punishment as such, 'the only aspect important for the effectiveness of a retributive act is whether it makes the original victim experience an adequate feeling of satisfaction', and this could in principle also be effected by 'punishing' a machine.[10]

1.5 Research question and outline

Although their line of argument is impressive and well-constructed, we are not yet ready to fully agree with Teubner and Matthias, if only because they write from perspectives – systems theory and a functionalist approach, respectively – that will not be shared by all readers, and indeed, not by all authors of this report. We want to give a closer look at arguments pro and con legal personhood for non-human entities, including a discussion of alternative approaches to solving the 'accountability gap'. So, the research question we aim to answer in this report is:

> Given the rise of new entities in the information society that operate at increasing distance from the persons who employ them, are current legal constructions sufficient to solve potential conflicts, or would it help to create (limited) legal personhood for these new entities in some contexts?

We do not aim at providing a definitive answer to this question. Rather, we give various perspectives that are relevant for answering it, in order to come to a tentative conclusion that can be built on in future research. The authors in this report sometimes apply different perspectives themselves, looking at similar questions from different angles; we have included some intentional overlap in the discussions in order to enrich the analysis and to show that clear-cut answers cannot be expected on a question that strikes at the heart of our legal systems.

We start with an overview of how the law currently deals with abstract persons, noticing the generality of the law and generic legal constructs like agents and personhood (Chapter 2). We then move on to discussing three types of new entities: pseudonyms, avatars, and software agents, sketching legal problems that arise through the growing distance between these entities and the persons 'behind' them. We indicate how current law addresses these problems, with a focus on continental legal systems (particularly the German and Dutch systems) that have a well-developed doctrinal tradition in dealing with intermediaries (Chapter 3). This sets the stage for a more in-depth and generic discussion of the research question, which – standing on the shoulders of Solum and Bourcier – allows us to see the merits and pitfalls of attributing personhood to new non-human entities (Chapter 4). We conclude with a tentative answer to the research question and some issues for further debate and research (Chapter 5).

[10] Ibid., p. 249 (our translation).

2 Abstract persons in current law

2.1 The generality of law

Laws are general in the sense that they do not address particular persons but a specified category of legal subjects. This way the generality of the law embodies two crucial principles of constitutional democracy:

1. equality before the law and
2. legal certainty.

The generality of law implies that in order to find out whether a law applies to a particular person, one must investigate whether that person (his/her legally relevant actions or status) fulfils the conditions set by the law for its applicability. Applicability of the law means that legal consequence is attributed to a type of action or event. For the difference between a legal fact and a legal action and the centrality of the concept of legal consequence we refer to section 3.2.1 of FIDIS deliverable 2.13.

One could thus describe law in the modern state as a system of rules, principles and policies that stipulate which legal consequences are attributed to which legal facts (e.g. tort), legal actions (e.g. a contract) or legally relevant events (e.g. birth or death). The generality that is embodied in rules, principles and policies is related to the fact that these rules, principles and policies are abstract (or virtual) rather than concrete. To realise equality before the law and legal certainty the law 'thinks' in terms of abstract or virtual concepts that need actualisation on a case-by-case basis. The relationship between law's virtuality and law's casuistic nature is neither mechanical nor arbitrary. Rules cannot apply themselves (as Wittgenstein remarked), they need creative intervention. This, however, does not mean that whoever applies the law is not obligated to her fellow citizens to attune her interpretation to past and future applications, thus sustaining the continuity and trust of legal certainty. In fact, to qualify as a virtual *person*, one would expect an entity to have the capacity to apply rules in a way that is consistent without being mechanical (Lévy, 1998). After all, the difference between a human person and other entities is precisely this: applying (legal or other) rules in a consistent but not mechanical way. One may wonder to what extent digital entities, like electronic agents, will at some point in time be capable of a similar creative actualisation of rules, principles and policies. In as far as digital entities can only mechanically apply pre-existent rules, their behaviour does not match with human interaction. This may affect the issue of whether a digital entity should be understood as an abstract person or only as an abstract entity in view of this conception of personhood. It may also affect the issue of whether a digital entity should be attributed legal personhood. We should take note, however, that in the model of FIDIS deliverable 2.13, personhood can also be attributed to entities that have no claim to *creative* rule application, speaking of entities with, for example, technical or mechanical access rights as qualifying for personhood. This is important to bear in mind: we should be careful in taking the step from entities with (non-legal) personhood to entities to legal personhood, precisely because of the difference in rule application.

2.2 Abstract persons and the generality of law

How does the concept of abstract persons relate to the generality of law? The concept has been defined in FIDIS deliverable 2.13 (note that we use 'virtual person' as a synonym of 'abstract person'):

> A *virtual entity* is an entity which is or has been the product of the mind or imagination.
>
> A *virtual person* is a virtual entity that can have rights, duties, obligations and/or responsibilities associated to it in a certain context. A virtual person is like a mask for a subject or another virtual person. It is a synonym for an abstract person.

Basically one could say that the generality of law depends on a concept of abstract persons, more in particular, on the concept of the legal subject. The difference between the concept of an abstract person and the concept of a legal subject is that the rights, duties, obligations and/or responsibilities associated with an abstract person need not be legal in the strict sense. An avatar or a software programme may 'have' certain responsibilities, but at this moment positive law does not attribute legal consequences to these responsibilities. They are a matter of social norms, habits, or – perhaps – ethical implications of the 'behaviour' of avatars or electronic agents. To see when it is useful to attribute *legal* rights and obligations to entities, we shall now look at the entities that are currently considered to be legal subjects., i.e., the bearers of legal personhood.

2.2.1 Legal subjects and legal personhood

Legal personhood indicates the capability to be subject of rights and duties.[11]

All humans have legal personhood. It is granted by Art. 6 of the Universal Declaration of Human Rights of 1948 and Art. 16 of the International Covenant on Civil and Political Rights of 1966 to all (living)[12] human beings.[13] The drafters of the European Convention on Human Rights (ECHR)[14] even held it to be too trivial and self-evident to include a provision on legal personhood of humans.

Within the legal doctrine of Germanic and Romanic jurisdictions, the legal personality thereby constitutes the first logic prerequisite for the capacity to act. The legal capacity may again be split into contractual and delictual capacity, describing the ability to bind oneself contractually or to generate consequences by unlawful behaviour.

[11] Heldrich and Steiner 1995, para. 2-2; Schmitt, § 1 BGB para. 6.

[12] For a comparison of the fuzzy borderline at the very beginning of life in German, English, American, French, and Spanish law, see Mahr 2006.

[13] International Covenant on Civil and Political Rights, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171 available online at: http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.

[14] The European Convention on Human Rights of 1950, 213 U.N.T.S. 222, available at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

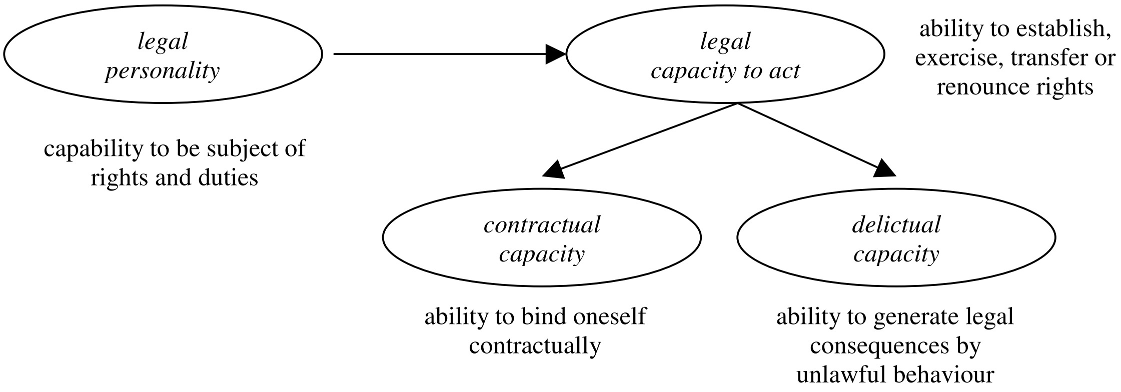
legal personality
capability to be subject of rights and duties
legal capacity to act
ability to establish, exercise, transfer or renounce rights
contractual capacity
ability to bind oneself contractually
delictual capacity
ability to generate legal consequences by unlawful behaviour

Figure 1. Legal personhood

This classification of the legal personality and the capacity to act has not spread to many other legal systems. There the question of whether an entity is able to have rights and duties is discussed mainly under the terminology capacity to act.[15]

All relevant legal systems grant legal personhood not only to humans but also to legal persons. Those are legal entities allowing several persons to act in law as if they were a single person (for example registered associations and companies). To protect trade from incapable or fraudulently acting entities, usually high requirements in regard to publicity of the incorporation act apply encompassing mandatory requirements in regard to formal registration procedures in public registers and mostly some kind of minimum capitalisation. This kind of legal personhood is, in opposition to personhood of humans, not automatically recognised worldwide but rather determined by national law. In fact, until 2002 companies founded within the EU were not legally recognised in German and Austrian jurisdictions when not acting from within the state of incorporation.[16]

Currently, all other entities besides humans and those legal persons recognised by law are considered to be legal objects. This applies, despite an ongoing movement by animal law activists,[17] also to animals, which are treated as things in private law, being objects of rights of their owners.[18] Thus, the question whether virtual entities such as avatars or software agents may be attributed legal personhood can currently be only answered negatively. They

[15] The concept of “Rechtsfähigkeit“ was first developed by German legal scholars in the 18th and 19th century and influenced the thinking of Romanic legal culture as well. It is referred to as capacité de jouissance, or capacità giuridica in the Romanic legal traditions. The concept offered solutions to the question how to deal with a separation of the holder of a right and the one who enforces it, as may happen with unborn or incapable persons and legal entities. The Common Law jurisdictions do not follow this separation. In common law the institute of a trust offers an alternative way to deal with the said challenges. In trust arrangements holding and exercising rights is both done by a trustee in favour of a beneficiary. For further information see Heldrich and Steiner, para. 2 et seq. For a clear distinction between Rechtsfähigkeit und Handlungsfähigkeit see e.g. Articles 11, 12, 17 Swiss ZGB.

[16] This changed with the decision of the European Court of Justice of 5 November 2002, Case C-208/00, Überseering BV vs. Nordic Construction Company Baumanagement, enabling European companies to act outside their country of incorporation.

[17] See: Goodall and Weise 1997. For an historical overview of animal rights in continental and common law systems, see Epstein 2002.

[18] Cf. § 90a BGB (Germany), Art 719 ZGB (Switzerland).

are neither humans nor does a law exist which explicitly grants legal personhood to such non-human entities.

2.2.2 Other forms of abstract persons in the law

The relationship between the concept of an abstract person and the law is not restricted to the general concept of the legal subject. In fact, positive law uses a variety of abstract persons to specify the conditions for attributing legal consequence to legal subjects. To demonstrate how this 'works' we provide some examples.

'Whoever commits a tort'

The Civil Code (or precedent in common law) can attribute legal consequence (rights and obligations) to whoever commits a tort. 'Whoever commits a tort' is the abstract person here, a subcategory of the category of legal subjects, defined as a whoever commits a wrongful action that can be attributed to her/him and causes harm to another person. This definition is articulated in conformity with Dutch law (art. 6:162 (1) of the Dutch Civil Code). Other jurisdictions will specify different abstract persons.[19]

'Whoever concludes a contract'

The Civil Code (or precedent in common law) specifies that whoever concludes a contract has to fulfil the obligations specified by the contract. This is not a moral obligation or a social norm, but the legal consequence of entering into a valid contract. 'Whoever concludes a contract' is the abstract person here, defined by a series of conditions that stipulate when one enters into a valid contract, further defined by a series of conditions that stipulate in which case the contract is void, voidable etc.

'Whoever does not fulfil the terms of a contract'

The Civil Code (or precedent in common law) specifies the legal consequences if one of the parties does not fulfil her obligations. 'Whoever does not fulfil the terms of a contract' is the abstract person here, defined by a series of conditions that stipulate at which point in time compensation has to be paid, as well as conditions that justify the breach of contract, which may have different legal consequences (nullification of the contract, with ensuing obligations to return goods already delivered or to compensate for services already provided).

'Whoever performs labour for another, weekly or at least 20 hours per month during at least 3 months'

The Dutch Civil Code specifies in art. 7:610a that whoever performs labour for another, weekly or at least 20 hours per month during at least 3 months, is assumed to perform labour according to a 'work contract' (arbeidsovereenkomst), meaning that in that case the legal consequences attributed by the Civil Code to a 'work contract' are in place. 'Whoever performs labour for another, weekly or at least 20 hours per month during at least 3 months' is the abstract person here, defining who counts as an employee. Interestingly other laws – e.g. concerning health insurance, pension or social security' – define the abstract person of an employee differently, stipulating other conditions for other types of legal consequence, depending on the particular legal statute in play.

[19] Comparative law provides many examples of how 'whoever commits a tort' varies between different jurisdictions, see e.g. Zweigert & Kötz 1995, at 595-628.

As we can see, abstract persons are elementary building blocks in law, all subsumed under the abstract person of 'the legal subject', because to attribute competences, rights and obligations, the abstract entity must be a legal subject. Other abstract entities in the law will be legal objects, such as: 'a house built without permission of the municipality', 'an animal that caused serious harm', 'an emission of more than 0.3 mg of a specific toxic substance' etc. Outside the law, we could call some of these legal objects abstract persons, if we think that they can be held responsible: 'the dog that bit me' can be 'punished', 'the electronic agent that sold me a product that did not fit my expectations' could be deleted, etc. Whether such an abstract person is also considered as an abstract person in law will always depend on whether a particular jurisdiction recognises the abstract person (in a non-legal sense) as a legal subject (making it an abstract person in the legal sense).

The fact that the category of the legal subject encompasses a variety of different abstract persons (cf. the examples above) indicates that the legal consequences of addressing an entity as a legal subject may vary widely. This will depend on the particular legal context: an entity that has legal subjectivity in the private law may not have legal subjectivity in the criminal law, the legal subject of the employer may have different legal obligations in a law on the contract between employer and employee than the legal subject of the employer in a fiscal law. This already implies that legal subjectivity is a relative category: attributing legal personhood is a decision (of a legislator or a court)[20] that is both constitutive and limitative of legal personhood. In section 4.4 and section 4.5 we will build on this relative approach for legal personhood.

2.3 Agents and agency; virtual persons and personhood

Before moving into a discussion of new legal abstract (or virtual) persons, we must briefly clarify what is meant with a person and a persona. This relates to the concepts of agent and agency.

In computer science an agent is defined as:

> A program that performs some information gathering or processing task in the background. Typically, an agent is given a very small and well-defined task.[21]

Importantly:

> In computer science, there is a school of thought that believes that the human mind essentially consists of thousands or millions of agents all working in parallel. To produce real artificial intelligence, this school holds, we should build computer systems that also contain many agents and systems for arbitrating among the agents' competing results.[22]

In law, an agent is often defined as:

> A person authorized to act for and under the direction of another person when dealing with third parties. The person who appoints an agent is called the principal. An agent can enter into binding agreements on

[20] In the common law legal personhood for natural persons has originally been initiated by the 'writ', a royal instruction to the royal complaints courts to stipulate which complaints fell within the royal jurisdiction. In continental law the civil and criminal codes determine who and what is to have legal personhood. One could say that in as far as courts co-determine the scope of application of legal entitlements they co-constitute the legal personhood of who or whatever is entitled.

[21] See http://www.webopedia.com/TERM/A/agent.html.

[22] See http://www.webopedia.com/TERM/A/agent.html.

> the principal's behalf and may even create liability for the principal if the agent causes harm while carrying out his or her duties.[23]

In the present legal framework, a computer agent cannot play the role of a legal agent, because to be a legal agent, the agent must be a legal person and so far, only natural persons, specific types of companies, associations, trust fund and public bodies have been attributed legal personhood.

In law, ethics and philosophy 'agency' is a term usually reserved for the capability of a person to have intentions and to make conscious deliberate choices on the basis of a moral and/or pragmatic judgement about what is at stake.[24] Though it makes sense to argue that non-human entities 'act' and make a difference (Latour 2005:52-54), this is not usually meant to suggest that they act on the basis of conscious reflection.

In computer games a persona is equivalent to an avatar, while in legal theory a persona is often described as the mask of legal personhood that allows a person to act in law, while protecting the physical person behind the mask from being equated with its legal role. The similarity between a persona/avatar and a legal person could be found in the fact that both refer to a role instead of the entirety of a physical person. This, however, does not imply that they are similar in other ways. An avatar-persona is created in order to play in a virtual game; it is not created to provide legal rights and obligations that allow for legal certainty and legal equality. Legal personhood attributes a specific type of personhood to an entity and personhood is often associated with what has been described as 'agency' above.

One of the pertinent issues that is at stake in this deliverable may be the question when legal personhood should be attributed to entities devoid of 'agency' in the legal, ethical and philosophical sense referred to above. The problem with the attribution of legal personhood to such entities (animals, ships, trust funds, organisations) is twofold. First, in a court of law they will always have to be represented by entities with agency (at this point in time that means they need representation by human beings).[25] Second, it is difficult if not impossible to establish liability for intentional wrong-doing or criminal guilt in the case of an entity without agency, which usually means that in those cases the liability of other legal subjects (with agency) needs to be established.[26]

We should note that the model developed in FIDIS deliverable 2.13 does not involve agency as a condition for personhood, which can be attributed to any entity that has a right of access, or is programmed to follow an algorithm that incorporates the application of certain obligations. In defining an abstract person as an entity with rights, obligations and/or other

[23] See http://www.nolo.com/definition.cfm/term/688A86E9-01FC-4A61-BF31C4A315325DAC. See also the definitions of actual and ostesible agency, and disclosed and undisclosed agents in law 4.5.4 below.

[24] See http://plato.stanford.edu/search/searcher.py?query=agency for an overview of the intricacies of the concept of agency in law and moral philosophy.

[25] As one of our internal reviewers remarked, one could imagine that digital entities require a different type of non-human courts or even a non-human law. This raises many interesting questions. The fact that animals do not have standing in court is not resolved by inventing animal courts (e.g., with a lion presiding as king and adjudicator?). A non-human court could be a merely technical invention to solve technical problems, in which case it would be confusing to speak of 'courts' or 'law'. However, if newly embodied intelligence emerges from multi-agent systems, one could eventually imagine the emergence of a new type of courts. The emerging 'subjects' could probably take care of that themselves (if they are interested in dispute resolution).

[26] For an interesting brainstorm on the legal personhood of personae without agency see: http://identityblog.burtongroup.com/bgidps/2006/11/the_limited_lia.html and http://thestateofme.wordpress.com/2008/01/09/persona/.

responsibilities, the model stipulates a usage of terms like rights, obligations and responsibilities that is not familiar to law, ethics and philosophy. One of the challenges of this deliverable will be to investigate how this new concept of personhood compares to legal concepts of personhood when extending the concept of an abstract person to an entity with non-legal and non-moral rights and obligations, for example, a technical 'right' of access or a technical responsibility. Some will claim this reduces personhood to a trivial notion that is deprived of its core meaning.

To investigate whether it makes sense to attribute legal personhood to emerging entities whose actions are less directly linkable to human actions, we shall now describe some specific cases of such entities.

3 New types of abstract persons in the information society

In this chapter, we describe legal problems that arise with the emergence of new entities whose actions take place somewhat at a distance from physical persons. We discuss potential solutions to these problems, among which is the question of legal personhood. We have chosen to describe here three kinds of entities that exist today and that have different characteristics: pseudonyms, avatars, and software agents.

3.1 Pseudonyms

3.1.1 Introduction and terminology

A pseudonym is an identifier of a subject other than one of the subject's real names.[27] The term "pseudonym" originates from the Greek word *pseudonumon* meaning *false name*. Traditionally it refers to pen or stage names of writers and artists.

By the model applied here, as described in deliverable D2.13, pseudonyms are regarded to be virtual identities for the respective physical person (drawn through line).[28] In the light of virtual persons pseudonyms become the identity[29] of a virtual person. If the link between the virtual person and the physical person can be recognised by a specific observer, the pseudonym becomes a virtual identity of the physical person from the view of the observer.[30]

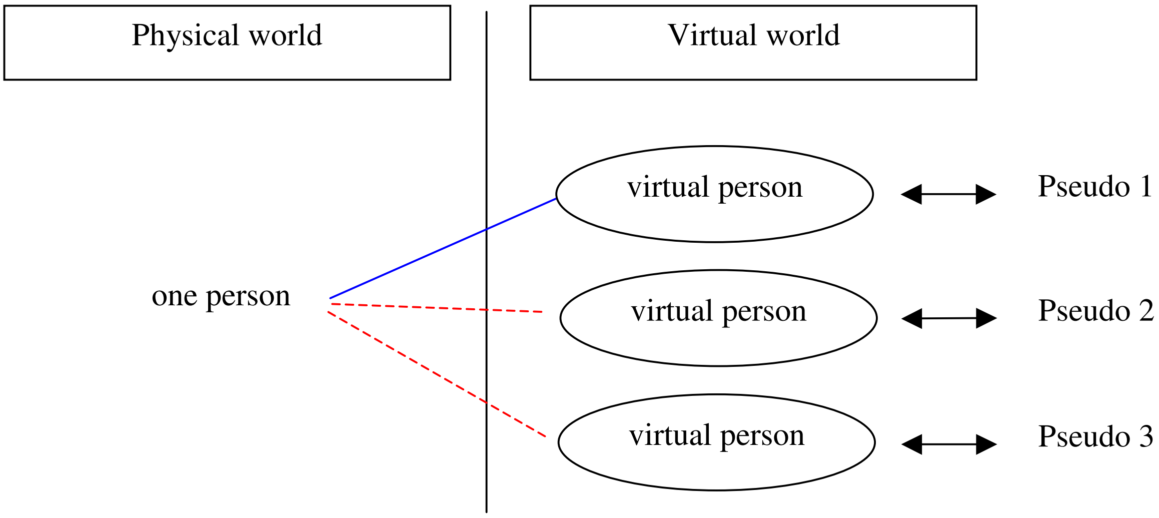

Figure 2. Linkable and unlinkable pseudonyms

[27] Pfitzmann and Hansen 2008, p. 20 et seq.

[28] Jaquet-Chiffelle 2008, p. 45, p. 49.

[29] An identity of an entity - according to an observer - is identifying information that can be linked to this entity by that observer, see Jaquet-Chiffelle 2008, p. 34.

[30] Jaquet-Chiffelle 2008, p.26. The identity of the abstract person is a partial identity according to the terminology of Pfitzmann and Hansen 2008, p. 20 et seq., who refrain from addressing pseudonyms as identities but qualify them as identifiers instead. For further details on this distinction please refer to Jaquet-Chiffelle 2008, p. 37-39.

One thinkable advantage of the concept of virtual persons is the possible privacy-enhancing effect. By hiding the link between the virtual and the physical person, anonymity for the physical person may be achieved. However, this requires that this is acceptable for the parties involved.

For acceptance in commercial and legal practice, deanonymisability is an important attribute of pseudonyms. A pseudonym is deanonymisable when the information that provides the link to the physical person can be disclosed upon request. This leads to the difference whether or not the identity of the holder of the pseudonym can be disclosed at least in a defined set of situations, for example when a contractual party does not comply with its duties. Such disclosure as well as the control over the requirements of a disclosure may be handled by a trusted third party, a linkability broker,[31] which needs to be in possession of the information to match the pseudonym with the name of the holder, i.e., the physical person behind the pseudonym.

3.1.2 Recognition of pseudonyms and pseudonymity in the law

Currently pseudonyms are mentioned in several contexts within European and national laws.[32]

Rules on electronic signatures

Legislation in favour of pseudonyms can be found in the Directive on a Community framework for electronic signatures[33] stipulating that member states shall not prevent service providers to issue certificates stating a pseudonym instead of the signatory's name.[34] If a pseudonym certificate is issued, the use of the pseudonym should clearly be indicated for secure signature verification.[35] However, the provisions on pseudonyms do not prevent Member States from requiring identification of persons.[36]

In the German law on electronic signatures of 1997 (SigG) § 5 s. 3 SigG provides a possibility for users to get a certificate indicating a pseudonym instead of the real name. This possibility was introduced to enhance privacy in particular in order to hinder profiling.[37] The pseudonym used must be distinctive, thus precluding group pseudonyms. Furthermore the nature of it being a pseudonym must be indicated within the certificate.[38] A disclosure of the identity of the holder is possible, but the trusted third party issuing the certificate (Certification Service Provider, CSP) may only disclose the identity if this is necessary for public authorities or when a court in a pending civil lawsuit orders to do so. According to the text of the provision the trusted third party (CSP) has to issue a pseudonym certificate upon request by the user.[39]

[31] Cf. Pfitzmann and Hansen 2008, p. 21 footnote 58.

[32] For an overview on the Canadian and US-American common law in regard to the permitted use of pseudonyms in general as well as in legal proceedings see Lucock and Yeo 2006.

[33] Directive 1999/93/EC of the European Parliament Official Journal L 13, 19/01/2000 p. 12 - 20, available online at: eur-lex.europa.eu.

[34] Art. 9 s. 3 Directive 1999/93/EC.

[35] Annex IV lit. (f) Directive 1999/93/EC.

[36] Recital 25 of Directive 1999/93/EC.

[37] See reasoning of the 1997 draft, BTDrucks. 13/7385, p. 31.

[38] § 7 s. 1 nr. 1 German SigG.

[39] However, whether a duty to provide pseudonymous certificates exists or whether this may be opted out by contract is still an open question within German legal discussion. In favour of a right to receive a pseudonymous certificate: Hornung 2006, p. 57. The governmental draft of the 2004 amendment on the SigG stated that in spite of the wording a duty to provide a pseudonym certificate does not exist as this may be contractually opted out by the CSP, BTDrucks. 15/3417, p. 7.

However, while the SigG offers the possibility for pseudonymous signatures, German Private Law frustrates this approach as § 126a German Civil Code (BGB) requires that the name of the signee must be stated within the plaintext of the document for an electronic signature to validly replace a written signature required by law for certain legal acts. This serves mainly two purposes closely connected to the purpose of the classical written form: to easily identify and to alert the signee before conducting a, potentially momentous,[40] legal action.[41] The validity of declarations of intent which do not require a written signature is not affected, e.g., for concluding a sales contract on chattels.

In German administrative law the use of pseudonyms in electronic signatures is prohibited, altogether.[42]

Thus the use of pseudonyms is possible and even encouraged by European law. However, at least in Germany neither the necessary infrastructure nor the acceptance within the relevant fields of business (consumers and service providers) is currently given.

Data protection legislation

The rules of German data protection legislation do not refer directly to pseudonyms but to the act of pseudonymisation, §3 s. 6a German Federal Data Protection Act (BDSG). Pseudonymisation means that data sets containing person-related information are protected by replacing the name and other identifying characteristics with labels or random data. This serves to preclude identification or render it more difficult.[43]

Law on Telemedia

The EC Directive on privacy and electronic communications, 2002/58/EC, prompts Member States in recital 9 to provide for possibilities for the application of pseudonyms. However, this must only be applied "where possible". The German Act on Telemedia (TMG) substantiates this in § 13 s. 6 TMG: A service provider has to enable the use of the service anonymously or under pseudonym, however, only as far as this is technically possible and reasonable. Due to this wide exception clause, the provisions do not yet grant an effective right to pseudonymous access as many service providers do not possess the possibilities to process requests and payment anonymously or to verify electronic signatures. Furthermore it is forbidden to merge pseudonymous user profiles with identifying data and in case of infringement this constitutes a misdemeanour.[44]

[40] The German civil code (BGB) requires the written form for contracts on timesharing, § 484 s. 1 BGB; credit contracts, § 492 s. 1 BGB; notice of cancellation for a contract of employment, § 623 BGB; putting a guarantee (bail) § 766 BGB. However, for all of the enumerated contracts the electronic form is excluded by law, so that a (pseudonymous) electronic signature is not possible anyhow.

[41] Cf. the grounds given by the German Government commenting the draft of § 126a BGB, BTDrucks. 14/4987 p. 16-17, and for the reasons to sign with the full name see German Bundesgerichtshof, BGH judgement 25 Oct. 2002 - V ZR 279/ 01 para. 22. The same was true for the Swiss draft on Art. 14 s. 2^{bis} Obligationenrecht (OR) that demanded that the certificate must be registered on a natural or legal person, cf. Schlauri 2002, p. 145 footnote 849. However this requirement has not become part of the enacted version of art. 14 s. 2^{bis} OR.

[42] § 3a s. 2 VwVfG (German Federal Law on Administrative Procedure). This is criticised within German legal literature as pseudonyms would be sufficient in many cases where authorities offer services such as information from a register or services of a public library as long as a disclosure is possible when necessary, cf. Hornung, p. 60, and FIDIS deliverable D5.4, p. 42-45, available at www.fidis.net.

[43] Pfitzmann and Hansen 2008, p. 21, Fn. 59.

[44] Cf. § 15 s. 2 nr. 6 German Law on Telemedia (TMG).

Thus pseudonyms are known to the legal European environment, where their use is encouraged for example in directive 1999/93/EC. But the use of pseudonyms is currently restricted to some areas, mainly for contractual relationships in private law.

3.1.3 Legal personhood

As we have seen above (section 2.2.1), the virtual person associated to a pseudonym or any non-human entity behind a pseudonym can currently not be attributed legal personhood. Indeed, the virtual person associated to a pseudonym is not human and no law exists which explicitly grants legal personhood to non-human entities masked by a pseudonym. So, legal rights and duties do not attach to the pseudonym (or its corresponding virtual person) but to human beings (or perhaps legal persons) linked to them. This raises various questions on to whom legal rights and duties can be attributed in actual situations; this is what we shall study in the next section.

3.1.4 Rights and duties under private law

Since virtual persons associated to pseudonyms currently lack legal personhood, they are considered as objects (and not subjects) of rights and duties. Legal subject of all transactions made under a pseudonym remains the holder, be it a natural (physical) person or a legal person.

However the idea of granting legal personhood to virtual entities holding a pseudonym as its identity would strengthen their protective veil for privacy protection as this could make disclosure of the acting physical persons unnecessary in many cases. The following analysis will explore whether such a construction of legal personhood fits into the current European[45] legal framework and what technical and legal means are necessary to strengthen pseudonymous transactions.

The legal construction that is closest to resembling pseudonyms are business names in commercial trade. In the Germanic legal tradition these are referred to by the *terminus technicus* “Firma” meaning the name of a business enterprise, where the enterprise may be a company as well as a single physical person.[46]

In case of a sole proprietor of a business the proprietor may have a Firma. But here should be referred to legal persons as these provide the additional layer of a virtual person between the pseudonym (the virtual identity) and the proprietors (physical persons). According to the definition given in the FIDIS report D2.13,[47] legal persons are described as abstract entities with their own, unique identity, having a legal status. As legal persons were granted legal personhood by law already a comparison may reveal the likelihood of an acceptance and adequacy of pseudonymous transactions within private law in particular in respect to one of the core aims of the concept of virtual persons – enhancing privacy protection.

Within the current European legal set, legal persons do not enhance privacy of the acting persons (i.e. CEOs) as all companies with a limited liability[48] must compulsorily disclose the

[45] For a comprehensive analysis of the legal possibility to use pseudonyms under German private, criminal and public law see Henry Krasemann, Selbstgesteuertes Identitätsmanagement in DuD 2006, p. 211-214.

[46] Cf. §§ 1, 8 Austrian Commercial Code (UGB), §§ 1, 2 German Commercial Code (HGB).

[47] Cf. Jaquet-Chiffelle 2008, p. 29.

[48] The two concepts of limited liability and legal personhood must not be confused. Limited liability excludes the personal liability of the shareholders (except for cases of fraud etc.) and is granted for example in Germany to the GmbH, KGaA, AG; in France for the société anonyme, la société à responsabilité limitée or

identity of "the persons who […] are authorised to represent the company in dealing with third parties and legal proceedings [or] take part in the administration, supervision or control of the company".[49] In Germany also the shareholders that are not actively participating in the management are accordingly enlisted within the public registers and thus can be easily disclosed, too.[50] The company register and the list of shareholders serve for the protection of creditors of the company but also for the interest in information for minority shareholders, potential acquirers of shares and the public, in particular current and future creditors. Thus the quintessence is, that the rules are supposed to protect contractual partners and hence to establish the basis for trust necessary in commercial transactions.

Similar considerations of trust and of preserving rights as well as the possibilities to enforce those rights also within online trade and other distance communication inspired the European legislator to require certain minimum information to be provided prior to contracting for the customer including the full name and the address, of the supplier.[51]

In private law legal acts depend on a declaration of intent. In many jurisdictions this declaration of intent must be free of mistake, otherwise avoidance may be declared. Erring about the identity or characteristics of a person is considered as a relevant mistake in many jurisdictions.[52] For example when, for a service of a certain kind, a specialist is sought but the contractual partner is later recognised to be lacking the specific qualification, the declaration of intent may be avoided with the effect that the service contract becomes null and void. Pseudonymous transactions could hence cause much uncertainty about the validity of legal acts. To some extent a technical solution may be found in anonymous credentials issued by a trusted third party, which may anonymously attest certain characteristics such as the approbation as a physician, the status of a specialised solicitor or the like.

This shows that trust is an essential basis for trade and private law relations. This assertion is backed by general research on trust in e-commerce showing that it is pivotal for legitimacy

the naamloze vennootschap in the Netherlands. All of these companies do also have legal personhood but this is true also for other general partnerships where the shareholders are still personally liable for any debts of the company, e.g., the commercial associations of OHG or KG in Germany. Companies with a limited liability are enumerated in art. 1 of Council Directive 68/151/EEC of 9 March 1968.

[49] Council Directive 68/151/EEC and Directive 2003/58/EC of the European Parliament amending the foresaid directive as well as the respective national laws enacting these directives. For example the Austrian Enterprise Code (Unternehmensgesetzbuch, UGB) provides public access to the entries in the *Firmenregister* (public company register), § 9 s. 1 UGB.

[50] In Germany § 40 GmbHG requires to provide an updated list of shareholders including their full name, date of birth and registered residence for the register. These lists as well as the other content of the register may be viewed online by anyone at www.handelsregister.de, § 9 s. 1 HGB. By requiring the publication of the shareholder's names the German law goes beyond the requirements of art. 2 s. 1 of the directive 2003/58/EC on disclosure requirements for certain types of companies. In contrast, in Austrian law viewing other documents than the main entries of the trade register (*Firmenbuch)* requires a legitimate interest of the applicant.

[51] See recital 11 of Directive 97/7/EC.The address must only be provided when the contract includes payment in advance by the customer, art. 4 s. 1 nr. 1 Directive 97/7/EC, however, the German implementation always requires the address excluding post office boxes (requirement of a "ladungsfähige Anschrift", an address where an official representative of the company, capable of representing e.g. in court cases, resides), § 1 s. 1 nr. 1, 3 BGB-InfoV. The Directive on electronic commerce requires name and geographical address to be provided, art. 5 s. 1 of Directive 2000/31/EC.

[52] § 119 s. 2 German BGB, art. 24 s. 2 Swiss OR, art. 139 s. 2 Brazilian Código Civil. But erring about the person of the contractual partner is not considered a relevant mistake under art. 4:103 of the Principles of European Contract Law or art. 3.5 of the UNIDROIT Principles.

and trust for buyers and sellers that their counterparts are who they claim to be.[53] The aforesaid also shows that both the traditional national legal systems and the European legislator deem it necessary to enhance trust by requiring minimum information about the contracting parties and thereby prohibiting the use of pseudonyms for suppliers or other parties that are likely to be debtor of claims. Therefore any suggestion made to further enhance the use of pseudonyms or virtual entities stepping as shield between the parties must address and solve the question of trust and enforceability of claims. The future FIDIS deliverable 17.4 "Identification and trust in the light of virtual persons" will address and study trust issues in the light of virtual persons.

One possibility to ensure that claims can be enforced would be to guarantee disclosure of the identity of the physical person by a trusted third party, as mentioned for the electronic signature above, or by any other means that provides for a certain, fast and easy way of identification.

To solve the problem one might further develop the idea that the holder of a pseudonym must accept that he is addressed under this pseudonymous identity even as a defendant in court. However, in continental European jurisdictions the service of documents that initialise court proceedings is traditionally seen as an act of state, which is strictly regulated and limited to the respective national territory.[54] The purpose of the strict rules on the service of procedural documents is to ensure a fair trail, namely that the defendant can take timely notice and effectively defend himself. It is also an essential interest of the claimant because an invalid service renders a judgement unenforceable and worthless outside of the state of origin.[55]

Accepting service to a pseudonym, e.g., an e-mail address, would need to place the contractual partner of the pseudonym's holder in the same position as if he possessed the real name and address. And for the possible defendant this must not have the consequence that the risk of not being informed about proceedings, e.g., because of technical failure, resides with the pseudonym's holder unless he caused the impossibility to render service of the documents.

To enable service to a pseudonym or other virtual entities it is thus necessary to develop ways to technically ensure a court-proof confirmation of the service which is also acceptable for at least a noteworthy number of states, as the international service of documents is currently a task of public authorities. Thus it is not completely unimaginable that once a trustworthy and widespread public-key infrastructure as well as a court-proof confirmation of service is established, future regulations may allow pseudonymous dispute settlement. Given that prerequisite, proceedings against pseudonyms and other virtual entities with assets of their own might also become imaginable in the more distant future.

In closed systems, such as online games, on the other hand arbitration indeed could be an effective solution already, provided the enforcement of the award is possible within the system. For example when the possession of a virtual item is contended and the award can be enforced by transfer or deletion of the item by the game provider or moderator and this third person is also willing to do so. Furthermore this would require the necessary facilities, i.e., a virtual courtroom and judges the parties agree upon as well as a mutual arbitration agreement

[53] Shepherd and Dhonde 2001, p. 42-56.
[54] Schack 2006, para. 589 et seq.
[55] Cf. Art. 34 nr. 2 of the Council Regulation No 44/2001 of 22 December 2000.

concluded in written form after the dispute has arisen.[56] The requirement of an agreement after the dispute has arisen will in practice be a major hindrance for any dispute between physical parties in different jurisdictions as the party who will presumably underlie is likely to object. But even if such a system for dispute resolution could be established in a binding way within a closed system like a game world this does not resolve the question of disputes outside such limited environments.

Conclusion

For trade and private law two major factors influence the potential use of pseudonyms. These are trust and the effectiveness of dispute settlement including recognition and enforcement of awards or judgements. Therefore pseudonymous transactions are likely to be accepted only in cases of an immediate performance, thus avoiding any form of credit for the holder of the pseudonym and provided that it is most unlikely that disputes against the holder arise later, e.g., by using anonymous e-money in exchange for downloadable software or services on the net. This concept corresponds to the immediate purchase for cash on a flea-market, where usually identities do not need to be revealed.

Summing up, the idea of pseudonyms as protective veil for privacy is currently not very likely to be successful in the field of private law unless in cases of an immediate mutual performance. Other transactions namely those involving some kind of credit require either enormous trust of the parties or sufficient means to enforce one’s rights in case of non-performance. However, once convincing technological solutions are found and available for all citizens, modernised procedural regulations may pave the way in the future for other ways of dispute settlement, which may also enable enforcement against future forms of aggregated assets.

3.1.5 Criminal liability

As mentioned in section 3.1.2, German data protection laws require that holders of pseudonyms in electronic signatures under the SigG are disclosed for purposes of law enforcement and criminal prosecution.

Furthermore criminal liability always requires an element of blame – guilt in continental law or mens rea in common law jurisdictions. As a moral concept, blame only makes sense with regard to a human being; organisations are usually not held liable but the persons acting in their behalf. In this respect, many criminal offences do not raise problems as the acting physical person will fulfil the necessary requirements himself, e.g., taking a foreign chattel away in a case of theft. More difficult is the attribution of guilt for offences where a duty of the company is neglected or attributes of the company are a necessary prerequisite for punishment. In German law this may for example be the case for not paying social security provisions as an employer[57] where the company usually concludes the contracts with the employees. Here, the required attribute “employer” is assigned to the acting or, in case of

[56] In commercial arbitration an arbitration agreement must be concluded in written form, cf. art. 7 UNCITRAL Model Law on International Commercial Arbitration, with amendments as adopted in 2006, available at: ; art. 2 of the Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 1958 "New York Convention”, 330 U.N.T.S. 38 (1959). However the written form usually requires that the parties sign the documents with their name and thus need to disclose their identity. In relation to a consumer the agreement must further be concluded after the dispute has arisen and may not deprive him from the right to bring an action before the competent courts; see Commission Recommendation 98/257/EC of 30 March 1998, s. VI.

[57] § 266a StGB (German Criminal Code).

duties, neglecting physical person in the company.[58] However, this again shows that even if legal personhood is attributed to a virtual entity criminal liability is always attributed to the actual wrongdoer, the physical person behind the pseudonym.

The use of pseudonyms, e.g., indicating a false name without criminal or fraudulent intent, is not illegal or punishable in itself in European jurisdictions but using the real name of someone else might be punishable in non-European countries.[59]

Summing up, the use of pseudonyms is not of relevance in the field of current criminal law.

3.2 Avatars

3.2.1 Introduction and terminology

A likely first association with the term "virtual person" will be related to avatars in computer games and other online environments, as described and covered in FIDIS deliverable 2.13.[60] Such digital avatars represent the player in the game world of Multi User Dungeons (MUDs), Massively Multiplayer Online Role Playing Games (MMORPG) and other computer games (further referred to as "virtual games"). The term avatar does not only refer to three-dimensional representations in virtual games but also to icons representing a specific user in an online forum or any other graphical representation of a computer user.[61] For this deliverable the avatar as virtual person representing one ore more players in the physical world or even a computer program, as used by game publishers to control non-player characters (NPCs).

Engaging in a virtual game usually starts off with the creation of a personalised avatar by adjusting the appearance of the graphical representation on the screen by choosing skin, facial features and clothes. In many games, particularly role playing games, further attributes such as strength, dexterity and abilities such as swimming, climbing or pickpocketing can be assigned to further personalise the avatar. These attributes may then be improved during the course of the game allowing the avatar to act more efficiently. In fact, in many role playing games advancement and development of the avatar is a central aspect of the game play. Guiding an avatar in its advancement over a long time and individualising the avatar with one's own preferences or getting absorbed by the interaction with other avatars forges a tight relation between the player and his avatar.[62]

As having an advanced avatar makes the game play more enjoyable, a demand for both good items and well-developed avatars as a whole exists, creating a market for such virtual goods. Depending on the game publishers' terms of service such trade may be allowed, even intended, limited to in-game trade, or forbidden. Increasingly, publishers allow and encourage the transfer of avatars between players.

The increased demand and market value of virtual items gave rise to legal discussions and has even led to first legal actions brought to national courts.[63]

[58] See. § 14 s. 1 and s. 2 German Criminal Code (StGB).

[59] See Koops 2005, p. 11 et seq.

[60] Jaquet-Chiffelle 2008, p. 11-15.

[61] http://en.wikipedia.org/wiki/Avatar_%28computing%29.

[62] Yee 2006, p. 187- 207.

[63] A recent case concerned the sale of a piece of virtual land. See *Bragg* v. *Linden Research, Inc. et al.*, http://docs.justia.com/cases/federal/district-courts/pennsylvania/paedce/2:2006cv04925/217858/26/.

3.2.2 Legal personhood

As seen above legal personhood is currently granted only to humans and registered companies. Therefore the question whether avatars have legal personhood can currently be answered negatively.[64] Avatars are neither humans nor does a law exist which explicitly grants legal personhood to such entities. Accordingly avatars lack a legal capacity to act. Also the factual ability to act separately from its human player, e.g., when steered by a script, does not constitute agency for the player (see below 3.2.3.1).

3.2.3 Rights and duties under private law

In private law, legal relationships are usually organised bilaterally. For the most likely case of avatars in a virtual game, the imaginable legal relationships are shown in the figure below.

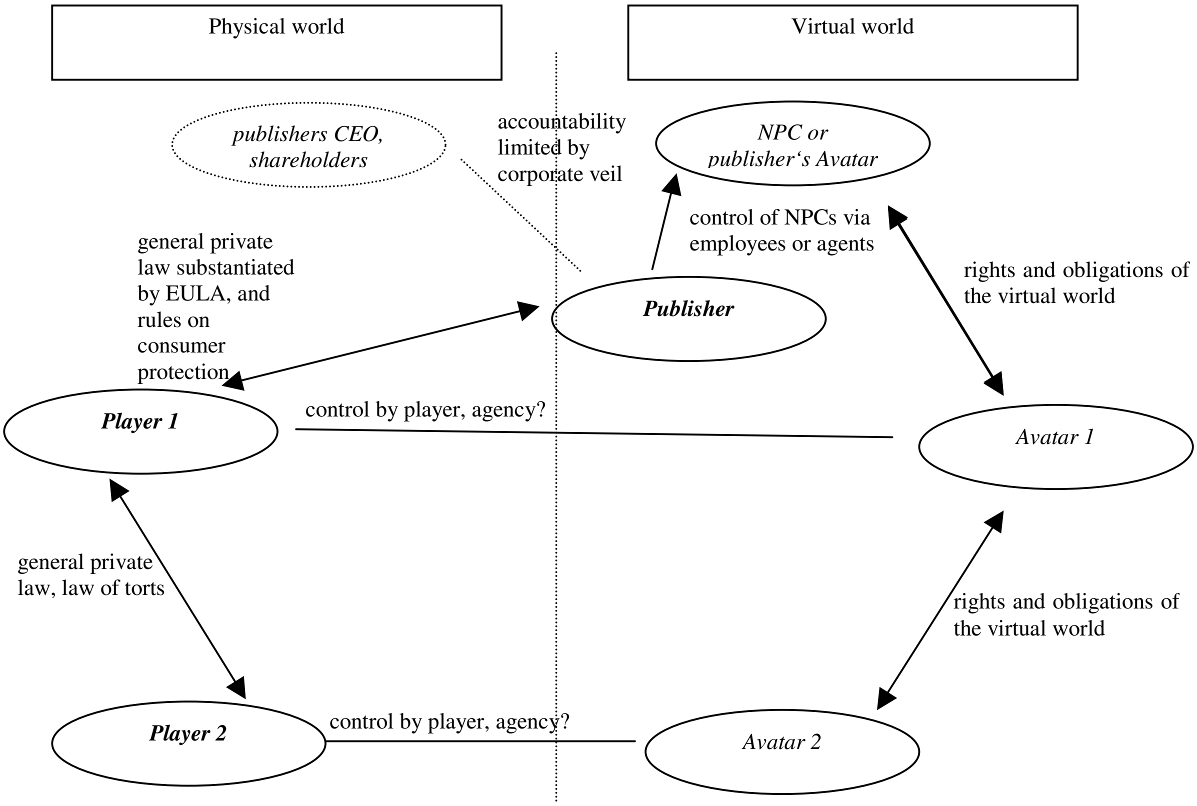
Physical world
Virtual world
publishers CEO, shareholders
accountability limited by corporate veil
NPC or publisher's Avatar
control of NPCs via employees or agents
general private law substantiated by EULA, and rules on consumer protection
Publisher
rights and obligations of the virtual world
Player 1
control by player, agency?
Avatar 1
general private law, law of torts
rights and obligations of the virtual world
Player 2
control by player, agency?
Avatar 2

Figure 3. Legal relationships in virtual worlds

Legal subjects are the publisher of the game and the players. The publisher is the virtual entity operating the servers, offering the client software, developing the game world etc. Publishers of computer games are usually legal persons or in fact will consist of several legal persons processing development and distribution of a game separately. For reasons of simplicity the players and publishers shall be treated as if they were a single person with legal personhood.

[64] See Habel 2008, p. 76.

3.2.3.1 Contract law

Player - avatar

The relation between the player and his avatar has been described from different perspectives in the FIDIS report D2.13, including the tight emotional bond physical persons can establish with their avatar.[65]

In contemporary private law only few statements can be made about this relation. As avatars do not have legal personhood they cannot be subject to rights and duties. Whether an avatar or any other item in virtual games can be object of the player's rights and the nature of such a right, is a matter of current legal discussion.[66] But all rights and duties will be linked to the player or publisher, who are the legal subjects involved.[67]

As avatars are acting for someone else and are able to create legal rights and obligations for the player in the physical world, a comparison with the legal institute of agency is suggested. This must not be mistaken with smart agents which will be covered later (section 3.3); we use the legal concept of agent here (see section 2.3). However, avatars are not agents of the player in private law. Agency requires that one person, the agent, has authority on behalf of another person to conclude a contract, and in the continental law tradition also that the agent acts in the name of the principal.[68] Acting for the principal requires that the agent has at least a certain range for own decisions, otherwise the agent would only be a messenger transmitting the player's declaration of will. Having the avatar choose between options would require that its program code incorporates a routine for decision making. In this case, this sub-program would "decide" and the avatar is only a means to visualise the result. The actions of such smart agents will be evaluated below in section 3.3.

Furthermore the avatar does not act in the name of the principal. This does not require that the identity of the player must be disclosed but it must be noticeable that the contractual rights and duties will be established with the physical person behind the avatar. The immediate acting, steering and deciding party is the player.[69] This is usually evident to all participants. Therefore all contracts with a relation to the physical world will be concluded only between the physical persons engaged.

Thus avatars are legally seen only as a visual frontend to communicate the player's declaration of intent, much like a chat client.

Relation between two avatars

As shown, avatars cannot be subject of legal rights and obligations. But depending on the rules of a virtual game an avatar's deeds that would constitute legal facts or legal actions[70] may be governed solely by the internal game rules of the virtual environment. If it is for example allowed in an online role playing game to act as a thief or to take items from a beaten foe, these actions do not establish legal rights and obligations between the players. This rule

[65] See Jaquet-Chiffelle 2008, p. 12.

[66] German legal literature: Lober and Weber 2005, p. 653; Krasemann 2005, p. 354.

[67] The same conclusion is drawn by Habel 2008, p. 76.

[68] Art. 1 Para. 1 UNIDROIT Convention on Agency in the International Sale of Goods (Geneva, 17 February 1983), avialable at: http://www.unidroit.org/english/conventions/1983agency/1983agency-e.htm.

[69] Krasemann 2005, p. 355.

[70] For definitions see Jaquet-Chiffelle 2008, p. 17.

finds its limits in cheating or using exploits.[71] Furthermore contracts negotiated between avatars are subject to national laws once they have binding force in the physical word.

If it could happen that two avatars fall in love and replicate, the relation between the offspring and its parents would also be dealt with by the rules of the specific virtual world.

Relation between other entities

Finally, the relationship between players and the publisher is governed by the applicable national laws which are chosen by the conflict-of-laws rules of the state where the court has its forum. In practice choice of law and choice of forum clauses are enclosed in the software's licence agreements. However, such stipulations are often invalid in regard to consumers as they violate European consumer protection regulations. For example when the software is bought in a box, a consumer usually does not have the possibility to get acquainted with the terms and conditions of the agreement prior to the conclusion of the sales contract as required by Directive 93/13/EEC.[72] When the player downloaded the software and hence had an opportunity to read the rules prior to the conclusion of the contract, the choice of foreign law will still not deprive him of the protections available under the mandatory law of the country in which he has his habitual residence, if he responded to advertising material.[73] As most publishers offer nationalised websites, the requirement of advertisement targeted to certain markets is met.

In the absence of a choice of law clause, the contractual relation between players is governed by the law of the country with which the contract is most closely connected.[74] This will often be the habitual residence of the seller.[75]

The relation between the publisher's corporation, which is a legal person and therefore part of the virtual word, and its physical counterparts, CEO, employees and shareholders, is governed by the applicable company law and does not raise specific issues of avatars or virtual persons.

3.2.3.2 Liability for torts and under criminal law

The liability for torts will be analysed in the same legal relationships as done for the contractual obligations before.

[71] Krasemann 2005, p. 354.

[72] Directive 93/13/EEC annex (i).

[73] Art. 5 Para. 2 of the Convention on the Law Applicable to Contractual Obligations (80/934/EEC) Official Journal L 266, 09/10/1980 p. 1 - 19. As of December 2009 see art. 6 s. 1 and s. 2 of the corresponding council regulation of 17 June 2008 on the law applicable to contractual obligations (Rome I), Official Journal L 177/6, 04/07/2008.

[74] Art. 4 Para. 1 of the Convention on the Law Applicable to Contractual Obligations, supra.

[75] Cf. Art. 4 Para. 2 of the Convention on the Law Applicable to Contractual Obligations, supra.

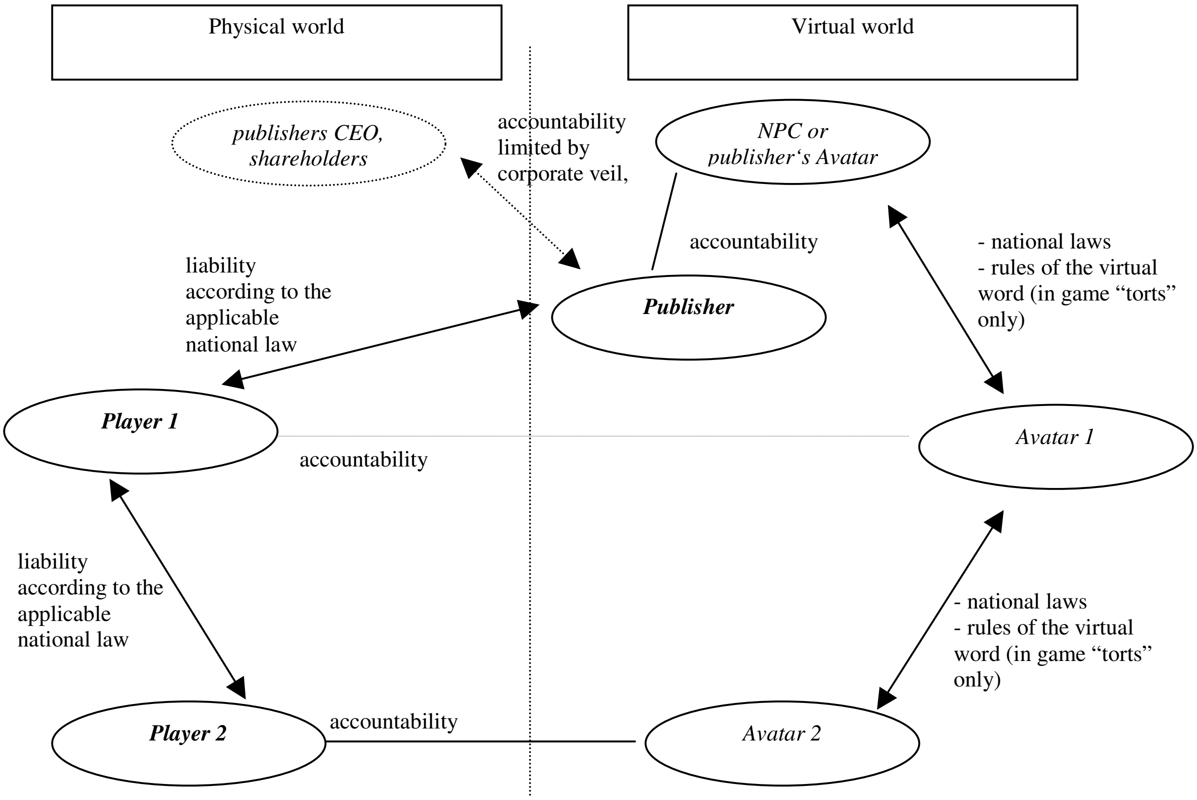
Physical world
Virtual world
publishers CEO, shareholders
accountability limited by corporate veil,
NPC or publisher's Avatar
accountability
- national laws
- rules of the virtual word (in game "torts" only)
liability according to the applicable national law
Publisher
Player 1
accountability
Avatar 1
liability according to the applicable national law
- national laws
- rules of the virtual word (in game "torts" only)
Player 2
accountability
Avatar 2

Figure 4. Liability in virtual worlds

Aim of the rules on civil liability

The central aim of the rules on liability (civil law) and the law of tort (common law) is to separate the huge mass of interferences with interests of others causing some loss from such severe interventions for which actually damages shall be granted.[76] No jurisdiction wards damages for every loss suffered from a causal action of another person. Irrespective of the general approach taken by a legal system,[77] the boundaries differ between the jurisdictions and are drawn by case law.

Relation between a player and his avatar

As an avatar does not possess legal personhood and all steering and controlling functions reside with the player, actions that could constitute a tort in the physical world are attributable

[76] Zweigert and Kötz 1996, p. 598, 625.

[77] While in the common law jurisdictions the law of tort was mainly developed by case law based on the writ of trespass on the case and now forms a widely differentiated system of actions the civil law jurisdictions base their law of liability on a blanket clause. According to the traditional French legal view liability requires the existence of three factors: a fault, a damage and a causal connection between the fault and the damage, see Art. 1382 and Art. 1383 French Code Civil. These rules of the Code Civil became model for many continental legal systems. The German concept of *Delikt* (unlawful act) as laid down in §§ 823, 826 German Civil Code (BGB) requires an unlawful and faulty violation of the interests of others offending either a special or a general duty.
For a successful action on tort in common law a loss caused by a breach of duty owed to the pursuer and causality between the breach of duty and the loss are required, see Lyall 2002, p. 261. Regarding negligently caused damage all systems agree that liability requires that the tortfeasor has violated due diligence ("im Verkehr erforderliche Sorgfalt") or has not acted as a "reasonable man" or "homme avisé" would have done.

to the player. Such actions need to have effects in the physical world such as the defamation of another physical player. Accountability is given too, when the player initiated a script steering the avatar into tortuous actions.

The aforesaid is also valid when the link between the player and the avatar is not visible. Avatars, pseudonyms and other forms of virtual entities are already often used to enhance privacy and anonymity by intentionally hiding the link between them and the player. This gravely impedes the enforcement of rights (cf. section 3.1.4) and while partners of a contract at least have a chance to choose their contractual partners, to check for their credibility and to decide whom to trust beforehand, victims of torts and crimes do not. So even if current law can easily attribute the actions of the avatar to the physical person in control, the factual problem of enforcement arises.

One solution could be the establishment of victim funds. A prominent example for a victim fund is the federal US "Crime Victims Fund" pooling all fines collected from persons convicted of offenses against the federal state, granting compensations and assistance to crime victims.[78] But such a fund needs to be filled with assets. Collecting fines will probably not work for virtual persons as the offenders usually cannot be identified – the initial reason why one might want to establish a victim fund. Thus unless an efficient way is found to raise funds, e.g., from a majority of users who are convinced of the necessity of using unlinkable avatars, this is not an efficient solution.

Another solution may be to collect money of everybody using avatars or virtual entities. An effective way may be a mandatory insurance, as widely known for cars or operators of dangerous goods. Insurance companies offer the additional advantage of efficient mathematical methods for risk analysis and therefore get closest to fair rates in accordance with the potential risk at stake. In many European countries such a mandatory insurance has proven effective for motor vehicles in combination with strict liability for all damages incurred by operating a car. The legal doctrine of strict liability means that a person is liable for all damage and loss caused, regardless of culpable conduct. While this is an effective solution for engines and cars and might even be applicable for certain kinds of smart agents and other bots with a vast damage potential, for example when used in stock trade, such a solution will prove far too expensive and hard to handle for smaller everyday applications, avatars in online games and in particular for pseudonyms as modern identity management systems tend to use one-time pseudonyms and mail-addresses to enhance privacy.[79]

At present the problem of accountability cannot be sufficiently resolved. While the legal position is clear, a problem of enforcement remains and cannot be resolved by currently available means.

Relation between avatars

In the virtual world, torts may be committed within the strict boundaries of the game's rules as part of the game play. Such offences will be subject to the rules and procedures implemented within the virtual game. Accordingly thievery may be allowed in certain environments. Such misdeeds are subject to the game's internal rules or even to several

[78] US Code, 42 U.S.C. 10601 et seq., available at: http://www4.law.cornell.edu/uscode/42/usc_sup_01_42_10_112.html.

[79] Cf. Al-Majid 2007.

internal "laws", e.g., for separate countries in a virtual world, where one region may allow polygamy or certain indecent clothing while others do not.

Relation between players

Torts committed within the virtual world can cause liability of the player when they are not expressively allowed by the game rules or otherwise part of the game play. Such claims must be settled between the players. Therefore, acting in a virtual environment does not affect any rights and obligations in the relation between the physical persons (players) involved.

As the relation between a player and his avatar can grow very close and intimate, it is possible that the player suffers damage due to a mistreatment of his avatar.[80] Currently, no legal case is known where a mistreatment of an avatar was raised as an action for damages in court. Such an action will unlikely be successful. In most jurisdictions, precedents exist which are reluctant with awarding damages for emotional distress or mental suffering in much severer cases.[81] The relationship between a player and its avatar must usually be regarded as too remote to grant any damages for a mistreatment of an avatar.

Deceit can be committed in virtual worlds by cheating someone into a disposition over a virtual entity by a knowingly false statement.[82] Therefore damages can be granted as far as a loss is suffered, which is the case when the item has a market value in the physical world.[83]Defamation is possible in virtual environments. Defaming means a communication tending to "harm the reputation of another as to lower him in the estimation of the community", being of and concerning a certain person.[84] This raises the question who may be victim of defamation. Is only the physical person a qualified target or is it possible to defame a virtual entity such as an avatar?

For the physical person the answer is evident. Acting within virtual environments does not affect any rights and obligations in the relation between the physical persons (players) involved. As long as an avatar remains under the sole control of a physical person, it is merely a means of communication. It therefore remains possible for the player to commit torts against other physical persons. This may either be done by defaming a known physical person, by asking for the player's name in real life or by directly insulting the other player.[85]

[80] Jaquet-Chiffelle 2008 describes how close the emotional band between a player and his avatar may grow. In particular, well-developed avatars with a long history may become part of the identity of the person. Prins 2007 describes some insecure teenage girls which gain a certain degree of security from their strong avatar and asks what will happen if this insecure teenage girl is insulted, menaced, or even "virtually raped" by other avatars in the virtual world. Psychologically, this may have real effects in the physical world impairing the daily performance and have potential traumatic effects.

[81] In common law mental suffering has traditionally not been recognised; shock was recognised by the courts only step by step and is limited by the requirement of "remoteness of damage", see Deakin, Johnston and Markesinis 2003, p. 21; Zweigert and Kötz 1996, p. 628. In German law constraints have been made by the requirement of a very close relation to the victim and the shock must be of an intensity that it is medically detectable leading to grave psychopathological conditions, Lange and Schmidbauer 2006, § 823 BGB para. 57. The New York Court of Appeals requires in Howell v. New York Post the conduct to be sufficiently outrageous and extreme in degree, available at www.law.cornell.edu/nyctap/I93_0071.htm#n3a, 612 N.E.2d 699.

[82] Definition of Deceit taken form Deakin, Johnston and Markesinis 2003, p. 501.

[83] Deceit with virtual items is possible under German law, cf. Krasemann 2005, p. 355.

[84] Chin 2007, p. 1333, 1338.

[85] The law on defamations differs among the judicial systems. Not all legal systems have criminal penalties for defamation but grant damages under private law. Common law, unlike all of the civil law jurisdictions, differentiates between the torts of libel and slander by the medium the harmful statement is communicated

Again, once the avatar acts independently from the player, we leave the given definition of avatars and regard must be held to the software or script in control of the avatar (for software agents see below section 3.3).

Regarding defamation of an avatar the question is not as clear. Based on its prior actions, an avatar may have a reputation of some kind. Part of this reputation may be represented by a ranking or reputation system within the virtual world. The programs and scripts in control of other avatars could refer to this kind of reputation of the avatar to calculate their response towards the avatar. Such reputation may even become a factor affecting the economic value of the avatar in the physical world. Damaging this reputation causes a monetary loss for the player in the physical word and may constitute a tort and grant a claim for damages. But in contrast to reputation, an avatar is not capable of having honour, dignity, or self-esteem.[86] Consequently this raises the essential question as to what exactly is the object of the protection by the regulations on defamation in the different jurisdictions.

Most countries have provisions in private and criminal law against defamation.[87] The German Criminal Code for example provides for the protection of dignity and honour of individuals, dead persons, the state and public bodies. For individuals, the entitlement to honour and dignity is based on human dignity. The majority of German courts and legal authors also assume that institutions are capable of being insulted in a way that it constitutes defamation. Interestingly, it is not assumed that the defamation of the institution constitutes a defamation of the individuals as members of the institution and respectively an attack on their individual dignity, but that organisations that fulfil a legally accepted social function must not be discredited as otherwise their socially desired function could be impaired.[88] This raises the question as to which extent avatars and other virtual entities may be entitled for a protection against defamation, too. At present, there is little occasion to assume such a need, but this may change if avatars should acquire a more important function in social life than they currently have.

Summing up, defamation of an avatar or other virtual entities is not possible currently, but defamation of the user or the physical person behind the virtual entity is. This does not only hold true for civil law tort cases but also for criminal defamation. As a criminal defamation of an avatar cannot be justified with the infringement of the dignity of the (human) victim, other justifications must be found. As far as several legal systems know criminal defamation of states, organisations or groups, these concepts are not undisputed. In particular, the grave conflict with the freedom of speech must duly be taken into account. Before transferring these ideas to foster the protection of virtual entities, one must further acknowledge that as long as the link between the virtual entity and the physical person is visible to the offender or any witness, a private law tort claim is given, dispelling the need for a separate claim of the virtual entity. If the link is not visible, the anonymity of the virtual environment and the function of

with. While slander refers to a transitory form such as speech, libel can be committed by any other means of communication (written, electronic, etc.). The German Criminal Code differentiates between two kinds of defamation "Üble Nachrede" (Defamation of character) and "Beleidigung" (insult), §§ 185, 186 StGB. While "Üble Nachrede" requires spreading facts that are apt to discredit the victim to third persons, "Beleidigung" is committed vis-à-vis by expressing disrespect for the victim.

[86] For the related issue of self-consciousness, the ability of reflection and deliberation and moral choices see sections 4.3 and 4.5.2 below.

[87] For a brief comparative introduction from the freedom of expression view see Kirtley 2003.

[88] Lenckner 2006, introduction to §§ 185ff para. 3.

avatars to act as protective veils must be taken into account and an infringement must therefore be much more severe as if directed against a physical person with human dignity.

Thus even though some jurisdictions may accept criminal defamation of virtual entities in a consequent forward projection of their existing laws, no need for such an extension of criminal defamation can be seen currently.

3.2.3.3 Summary of private law

Avatars are not recognised as legal entities and lack legal personhood. All legal relationships with a connection to the physical world are linked to the player, including a liability for torts committed within the game to some other player.

3.2.4 Privacy protection

An avatar cannot claim privacy protection for itself, again due to the lack of legal personhood. However, as the avatar serves also as a pseudonym masking the identity of a physical person,[89] the privacy rights of the player are applicable. EU member states should enable their citizens to act anonymously or pseudonymously where possible.[90] However, as Koops put it, at some point there is always someone with a right to have the identity revealed.[91] For details on privacy protection laws and possible duties to reveal one's identity, we refer to section 3.1.4.

3.3 Software agents

3.3.1 Introduction

Software agents (which in this section we will refer to as 'agents') become ever more pervasive. They help bring the efficient and effective use of ICT to a higher plane; agents relieve humans from tasks they consider burdensome or boring. Their attractiveness is mainly based on the fact that they act to a certain extent autonomically, i.e., that they function without human intervention (we use 'autonomic' here rather than 'autonomous', see section 4.3). Especially, this autonomic aspect of agents' functioning is legally relevant. The increase in their use and the way in which they operate gives rise to new legal questions and gives reasons to reassess existing legal concepts. In this section, we explore from a legal perspective what agents are, whether they should be recognised as personae under law and to what extent their acts can be attributed to their users. The first section presents a way in which a lawyer might classify agents. We will refer back to this classification of agents wherever expedient. Subsequently, we deal with the question whether an agent is a person in law or just a tool of the person who uses it. Without an answer to this question or at least an assumption about the answer, most other legal issues cannot be dealt with. After these preliminary issues, the question of attribution is dealt with. Under what circumstances can the actions of an agent be attributed to its user?

3.3.2 What are agents?

Agents are software programs that act for their users. In doing so, agents display a number of characteristics. In computer science, the following characteristics are being discerned:

[89] Cf. Jaquet-Chiffelle 2008, p. 25-27.

[90] Cf. recital No. 9 of Directive 2002/58/EC (Directive on privacy and electronic communications).

[91] Koops 2007.

Autonomy: the agent functions to some extent independently from human intervention, especially independently from its own user, almost in the sense that it takes responsibility for the interest of the user.

Persistence: the agent is continuously activated and performs its function if and when it detects the necessity to do so.

Social ability: an agent communicates with its environment.

Reactivity: the agent reacts to signals it receives from its environment, such as other agents.

For the purpose of this chapter, we introduce a classification of agents as may be made from a lawyer's perspective. An agent is a process (i.e., a programme in action) that looks after certain interests of its user in a network environment; this environment is characterised by the presence of other users who have their own set of interests and possibly their own set of agents to take care of them. An agent may take care of its user's interests with varying degrees of autonomy and intelligent behaviour. For the purpose of this brief legal analysis, we propose to distinguish three types of agents, depending on the degree of autonomy with which they operate.

- **A slave**: a slave has no autonomy at all. For any decision that affects the possessions, legal rights and obligations of its 'master', it has to consult him.
- **A representative:** he may take its own decisions within a well-defined domain and within strict limits.
- **A salesman**: this agent may take its own decisions and is not restricted in the way in which it intends to take care of its user's interest. It is bound to serve the interests its user wants to be taken care of. It may for instance manage a stock portfolio of its user.

3.3.3 Is an agent a holder of legal rights and obligations?

A user makes use of an agent in order to perform certain tasks. This may raise the question how the role of the agent should be classified or interpreted in law. On the one hand, one may say that the agent is the inanimate tool in the hands of its user. In this view, it is the user who acts and the agent is merely the modality of the human behaviour. The agent constitutes merely the circumstances of human behaviour and may as such play a role in the legal assessment of the human behaviour. On the other hand, agents perform tasks that were previously the sole domain of human agents. They do so with a certain autonomy. Therefore one could say that to some extent, agents take on some properties of human beings. They may display their own 'personality'. This may especially be true of the salesman type of agent. From the observation that an agent has its own 'personality', one could possibly argue that an agent should also be given the legal dimension of personality. In other words, this view begs the question: is it possible to consider an agent as a holder of legal rights and obligations? Or even more succinctly put, should an agent be a persona in law?

In order to answer the question, we survey who according to Dutch law are the holders of legal rights and obligations; the Dutch situation may be considered as representative for most continental European law systems in this respect. The primary source of law for this question are the first two books of the Dutch Civil Code (Burgerlijk Wetboek, hereinafter: DCC). In the first place all natural persons, i.e., human beings of flesh and blood are recognised as personae in law. Apart from these, the law recognises some organisations as legal persons. The Dutch Civil Code mentions the 'vereniging' (the association), de 'stichting' (the foundation), the ‘B.V.’ (the private company), the ‘N.V.’ (the corporation), religious bodies, and corporate bodies governed by public law, such as inter alia the state, provinces and municipalities. The enumeration of legal person in the Dutch Civil Code is not exhaustive. Other statutory laws declare other organisations or bodies to be legal persons. Even if statutory law does not explicitly declare certain bodies to be legal persons, they nonetheless may be qualified as such, if the law regulates a body in such a way that the conclusion of its legal personality is obvious.[92] As statutory law does not declare agents to be legal persons nor regulates agents, the conclusion seems to be that, for now, agents are not legal persons. Only a change of statutory law or perhaps an authoritative decision by a judge may change this situation. Whether this is desirable cannot be deduced from the foregoing. In order to have a clearer idea about the desirability of personality of agents in law, another approach is in order.

For answering the question of the desirability of ‘recognition in law’, we take the following approach: what concrete legal or societal problems are being solved by making an agent a persona in law? We must admit that we are hard pressed to find such a reason for legal recognition. Perhaps one could argue that recognition would shield the user of an agent from large liability risks, just like existing legal persons shield their shareholders from an unlimited liability. After all, creditors of a legal person cannot recoup their money from the personal possessions of a shareholder, but have to confine themselves to the possessions of the legal person. But then the question is: what is the rationale for giving users of agents such a ‘privileged’ position? To be sure, the use of agents can be considered desirable and the liability that could follow from their use might scare people away from using agents. But the desirability of using agents seems to be an order of magnitude smaller than the desirability of enabling human beings to undertake matters together, which is the rationale for traditional legal persons such as the Dutch private company (BV). The thesis that people refrain from using agents because of the liability risks involved, is – to our knowledge – unproven and arguably untrue. Moreover, if there were serious liability concerns over the use of agents, a user could always choose to establish a traditional legal person, such as a B.V., and have the agent work in name and for the account of the B.V.[93] Therefore, we think that for the time being, a liability problem, if existent, can be solved within the existing legal framework, without recognition of the agent as a persona in law.

Are there other problems that might require recognition of agents in law? Perhaps one could argue that an agent is an independent actor and that – in the view that an agent is merely a tool – the legal assessment of its behaviour is complicated by the fact that its behaviour always has to be ascribed to its user. The argument would then be that through recognition, law would have a set of concepts and a dogmatic foundation that makes it easier to handle legal problems involving agents.[94] The value of this argument is difficult to assess. It requires a comparison between the situation as it now exists and the hypothetical situation in which an agent is or can be a legal persona. The latter situation is not unambiguous because the recognition is probably not a matter of simply stating that from now on agents are legally recognised as persons. Just as with traditional legal persons, recognition would entail regulation of the institutional aspects of the (new) legal person. A recognition thus becomes a complex matter in which many choices have to be made. Recognition might involve regulation of multiple

[92] Maeijer 2007, p. 225.

[93] Cf. Sartor 2003; Andrade et al. 2007, p. 371.

[94] As is argued (albeit with respect to future, somewhat more evolved, agent systems) by, e.g., Matthias 2007 and Teubner 2007 (see also supra, section 1.4). Contra, e.g., Chopra and White 2004.

aspects such as the definition of what legally constitutes an agent, the gathering and maintenance of its capital, perhaps an obligatory insurance against liability, the control of a user over an agent, the scope of its authority, its registration at a Chamber of Commerce or some other authority and the compliance with judicial sentences. With such a complex regulation – the detailing of which may be worked out in one of various ways – it is not straightforward to answer the question of its desirability. Apart from this aspect, the introduction of an agent as a persona in law might even bring about new problems. I think of the distribution of responsibility between the user and the agent. As there are two personae (the user and the agent), questions may arise, e.g., as to whether the user did not take due care when instructing the agent or whether the agent's processing of the instructions was fallible. Such a problem could arguably be avoided, if there were only one persona, the user.

The final judgement as to whether the introduction could bring advantages and whether possible advantages would be so compelling that a recognition and regulation should follow is difficult to tell without further investigation of options and thorough contemplation of merits and drawbacks. Such a research goes beyond the possibilities of this explorative text and may be subject of subsequent research.

For the moment, however, it seems safe to assume that agents are not personae in law. They are considered as the mere tools of their users. The desirability of recognition as personae is at this moment far from evident.

3.3.4 Legal acts

Personae recognised in law may change their (civil) legal state, i.e., change their legal rights and obligations (art. 3:32 jo. 2:5 DCC). They may do so by entering into contracts, acquire goods, hire employees, commit themselves to deliver services etc. In general, one may change one's legal state by performing a so-called legal act (in Dutch: rechtshandeling). An actor's goal in performing a legal act is to bring about the desired legal effect (in Dutch: rechtsgevolg), i.e., the change in his legal state. This does not tell us how a legal act can be performed. To perform a legal act, one has to declare one's will to bring about the desired legal effect (art. 3:33 DCC). Two parties may, e.g., declare that they want to conclude a (purchase) contract by which the one party commits itself to deliver a good to the other one and the other party commits itself to pay a certain amount of money to the former one. Declarations may be made in any form (art. 3:37.1 DCC). For example, at an auction, one can declare one's intention to buy by simply putting up a hand or a sign. As there are in general no form requirements for declarations, one may use a software agent to make a declaration. So, in general, there is no reason why an agent could not be used for declarative purposes. This does however not mean that the use of software agents cannot give rise to questions.

In the first place declarations have to be sent to the person to whom they are directed. While in transit the data constituting the declaration may through natural or manmade causes get lost. Is there a declaration in the legal sense, if this happens? In law a declaration has to reach the person for whom it is intended in order to have the desired effect. Therefore, a message that got lost does not constitute a declaration. There is however an exception to this rule. There is nonetheless a declaration if the non-reception of the message is attributable to the person addressed, to persons for which he is liable or to other circumstances that regard the addressee and justify that the addressee bears the burden of the prejudice that flows from the non-reception. If the addressee for whatever reason does not read the message, although it has been received by his agent, this very likely constitutes a circumstance for which the sender does not have to bear the risk. For the design of software agents this may mean that there should be a solid system for confirmation of receipt of messages. The construction of such a confirmation is facilitated by the exception to the rule. In the same line of thinking is art. 11 of the European Directive on Electronic Commerce (2000/31/EC). A service provider who receives an order through technological means has to acknowledge the receipt of the order without undue delay and by electronic means. This rule however does not apply if a contract is concluded exclusively by exchange of electronic mail or by equivalent individual communications. The order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them.[95]

Secondly, it is not about just any declaration, it is a declaration of one's will. If somebody declares, the declaration of will generally corresponds to one's 'real' will. Problems of declarations that do not correspond with one's will, may however arise in cases of a mental defect or by accident. E.g., one puts inadvertently up one's hand during an auction. What is the law in such cases? Is the declarant bound because his act could be perceived as a declaration, or is he not bound, because he lacks the will to be bound? The answer under Dutch law is that the declarant is bound by his act, if the other person could reasonably assume that the act was a declaration directed at him. This rule is inspired by the idea that a person must be able to trust what he sees or hears (at least if there is no reason to assume that something is wrong). In case of a mental defect, the situation may become a little more complicated. If somebody's declaration was affected by his mental defect and the legal act he entered into was foreseeably prejudicial to him, it is assumed that his will and declaration do not correspond. In such a case of non-correspondence, the legal act is nullifiable. This can be done by notifying the person to whom the declaration was directed of the nullification. If the declaration was not directed at a particular person the declaration is *ab initio* null and void.

How does this affect the use of software agents for declarative purposes? The slave type agent is the easiest case. As the user has full control over the slave, there seems to be no difference from the situation in which a person declares orally or uses a passive means for the declaration, such as a telephone.

The representative type of agent constitutes a more challenging situation. This agent has clear limits, but is free to act within boundaries that are imposed upon him. This may mean that the user does not know about the particular legal acts the agent enters into. As the user does not know of the particular legal act, one may ask whether the user's will does extend to the legal act at hand. This situation bears significant resemblance with EDI systems. In general one can say that there is a will that corresponds to the declaration by his agent. This will is however not straightforward and requires further explanation. What is this will based on? In the literature, several theories have been proposed: the representation theory, the theory of the programmed will, the theory of the general will and the theory of the framework agreement.[96] We will shortly explain what these theories are about. In the representation theory, the agent is put on a par with a human agent that makes a declaration that has been formulated by the represented person. It is the involvement of the represented person with the declaration that constitutes the link between the declaration and the will of the represented person. Apart from that, the idea that one person can represent another is very well-known in law. For agent cases, this theory however has two drawbacks. In the first place, representation in law is confined to representation by a natural or legal person. As we saw above, the recognition of a

[95] Parties who are not consumers may agree otherwise on the topic of acknowledgement and the definition of receipt.

[96] Van Esch 1997, p.45-53.

software agent as a legal person is not commonplace. Secondly and perhaps more importantly, the representation theory still very much builds on the involvement of the represented person, whereas our goal is to find an explanation for a will where this involvement is lacking or is at most marginal. The next theory is the theory of the programmed will. This theory builds on the idea that the declarations made by the agent are determined by the code and parameters of the programme that constitutes the agent. It is assumed that the user knows the code and that the activation of the agent constitutes an expression of the will to accept all declarations that are made by the agent in accordance with its code and parameters. This theory is usable, but it bears the risk that a user states that he did not know of parts of the code and thus had not had the will to make the associated statement. The theory does not acknowledge that a user usually does not know the exact code, but has only a general knowledge of the functionality of the agent. The next theory, the theory of the general will does not assume that the user has a will to perform the specific legal act, but it assumes that in law a general will to accept the legal acts that the agent brings about is sufficient. This general will is expressed to the outside world by activating the agent and keeping it in action. Finally, there is the theory of the framework agreement. This theory takes as a starting point that users have concluded framework agreements with each other, in which they agree that declarations of user's agents will be considered as valid expressions of the will of their users. It is self-evident that this theory only works if such a framework agreement exists. In open environments, however, these agreements will generally not be in place.

Where does all this leave us when constructing an agent? In general one does want that if a user is to be bound by a declaration of an agent, the bindingness is based upon the will of the user. It is not desirable that a user is bound by a declaration that he did not want, but was 'forced' upon him; remember that another party that could reasonably assume that the declaration of the agent is in accordance with the will of its user can make the declaration stick to the user. The agent must thus be constructed in such a way that it is transparent to its user what the agent can do and what he cannot do. This transparency can be realised by providing the user at activation time (or earlier) with information about the functioning of the agent. It may also be possible that an agent while in action seeks authorisation from the user before it enters into legal acts that are particularly burdensome to the user. Secondly, it is important (or at least helpful) that a contracting party of an agent knows about the agent, its authority to act and goals the user and agent try to establish by entering into legal acts. The more the contracting party knows, the easier it is to detect that an agent goes beyond the will of its user. In other words, the more a contracting party knows the more difficult it will become for this party to state that it could reasonably consider a declaration as a declaration that is in accordance with the will of the user. There is an advantage in making available as much information as possible.

Finally, the salesman type of agent may be provided with a business goal and it is left to the agent to determine which – if any – legal acts are needed to meet the goal. This type of agent does not to seem be operative at this point in time. But, if it becomes available, how will it perform legal acts? If one sticks to the idea that an agent is not a persona in law, much of what is said above about the representative agent might apply here as well. The theory of the general will can arguably be stretched to fit the salesman type of agent. On the other hand as this type of agent is somewhat a thing of the future, one could feel free to more fundamentally rethink law. An agent with a goal as the one described above, needs a budget of its own to accomplish its goal. Once it has its own capital, the step to making it a legal person becomes less implausible. If you really make it a legal person and no longer an entity acting on behalf of a natural or legal person, the idea of finding a basis in the will of the 'user' becomes superfluous. Instead there rather seems to be a need to have some mechanism in place that manages the capital of the agent and prevents it from building up debts. Perhaps, however, this is something that the agent itself could do or learn to do as well.[97]

3.4 Conclusion

In this Chapter, we have discussed three types of new entities – pseudonyms, avatars, and software agents – from the perspective of the current legal framework and currently proposed solutions in legal doctrine to deal with potential conflicts involving these entities. Generally, the legal framework seems sufficiently equipped to solve the legal problems that currently arise. This does not come as a complete surprise: the analysis has focused on particular continental legal systems (the German and Dutch systems) that have a well-developed doctrinal tradition in dealing with intermediaries, and the new entities discussed are not yet so advanced in their functioning that they substantially diverge from existing types of intermediaries.

Does the same conclusion hold if we approach the same issues from a more general perspective of legal theory, abstracting away from concrete legal systems and current legal frameworks? This is the challenge we address in the next chapter.

[97] Cf. Matthias 2007, p. 244-245, who argues that agents could earn and administer money themselves, in order, *inter alia*, to pay damages.

4 Emerging abstract persons: new legal abstract persons?

4.1 Legal and non-legal abstract persons

In FIDIS deliverable 2.13, we have given some examples of new entities that may qualify as abstract persons outside the law, but which – so far - have not been recognised as such within the law:

- animals,
- avatars,
- intelligent robots,
- software programs,
- smart environments,
- hybrid multi-agent-systems.

In as far as these (old and) new entities have certain responsibilities, they may be termed *non-legal* abstract persons in jurisdictions where they have no legal subjectivity. Being a *non*-legal abstract person is – of course – not the same as being an *il*legal abstract person. To be illegal, the difference between legal and illegal must be relevant, while in the case of non-legal persons this difference is not valid. Being a non-legal abstract person implies that the person cannot be illegal or act illegally; it means that *in law* the actions of the non-legal abstract person are attributed to whoever designed, produced, sold or used 'it'.

Danielle Bourcier,[98] while discussing what she calls 'virtual persons', discriminates between:

a. the numerical person, composed of digital data of a physical person, present on the internet (we will call this the digital person);
b. a new creature – not necessarily created in the image of man – which acts on its own initiative, for instance an autonomic software programme;
c. a profile, inferred from masses of data, which represents a physical person (we will call this a digital person too).

Category (a) seems a rather simple digital proxy, while category (c) seems a more sophisticated proxy. The problem with category (c) is that is seems restricted to individual profiles, while even personalised profiles are often inferred from group profiles. Though a personalised profile – even if it is inferred from non-distributive group profiles (as discussed in FIDIS deliverable 7.2) does represent a physical person, this is not the case for a group profile, which can be said to represent a group. We will refrain from calling this a digital person and introduce a fourth category:

d. a group profile, inferred from masses of data by means of data mining, representing a category of people

Category (b), however, presents new challenges due to its relative autonomy. We would suggest that (a) and (c) are digital entities, while (b) might in fact qualify as a digital person.

[98] See Jaquet-Chiffelle 2008, section 3.3; Bourcier 2001.

We will now discuss the legal implications of (a) and (c) in terms of their capacity to generate legal consequences (for whom), after which we will discuss whether it makes sense to attribute legal subjectivity to (b).

4.2 The numerical person (a) and the profiles (c, d): non-legal abstract persons?

In terms of the model provided in FIDIS deliverable 2.13 (a), (c) and (d) are identifiers and would qualify as the identity of a virtual entity, i.e., they define a corresponding virtual entity; at the same time, they may also be an identifier of one or more physical persons.

Though in terms of the model, an identity does not qualify itself as a virtual entity, it makes sense to raise some questions as to the legal status of their corresponding virtual entities, before moving into the legal status of the entities under (b). Can we image a situation in which it makes sense to attribute rights and responsibilities to virtual entities defined by digital identities and profiles, meaning that these entities could be qualified as persons in terms of the model of D17.1? Could we even understand them as legal persons, or are they only non-legal abstract entities without any legal responsibilities independent from the physical person to which they link?[99]

Digital profiles are constructed by means of data mining or KDD and may be ‘owned’ by data controllers. This means that though they relate to a physical person (or to a category of physical persons, or – as mentioned – to a corporation, a trust fund or a public body) these persons may not be aware of their existence. The data controller is in charge of these profiles. If one qualifies the virtual entity defined by a digital identity or profile as a virtual person, then what is the legal status of such virtual persons? The following considerations are relevant as to the legal status of what could be qualified as virtual persons in terms of the model of D17.1 (defined by digital identities and digital profiles), and thus pertinent to answer the question of their legal status.

1. Can they negotiate and conclude contracts on their own account?

    A digital identity or profile as described above, cannot negotiate or conclude contracts, irrespective of whether a law would grant them legal personhood. They are identities or partial identities of a person or a group and can be used by that person/group – or by others – to provide information or (in the case of a profile) knowledge about a (category of) person(s). A digital identity or profile is not a software program.

    The legal status of a digital identity or profile is complex and depends on who provided the information, under what conditions, and on whether data protection legislation and intellectual property rights apply. This – in turn – will depend on whether the digital identity consists of personal data (if it is a unique identifier, it probably does) and whether the digital profile is part of a database that is protected by copyright or the *sui generis* database right, etc.. In fact, the right of a data subject to

[99] It is important to note that the conditions for virtual personhood in terms of the model of D17.1 consist of virtual entities having rights, obligations or other responsibilities , whereas the meaning of these terms is different from the meaning attached to these terms in law, ethics or even common sense. For instance a technical right of access of an identity to a website falls within the scope of the model, allowing one to qualify an the corresponding virtual entity of the identity as a virtual person. This means that virtual personhood does not automatically imply that it makes sense to attribute legal personhood.

have access to the logic of an automated decision could very well collide with the intellectual property rights of the data controller. Those considerations might affect the legal status of the corresponding virtual persons defined by a digital identity or a profile.

2. Can they represent the physical person to which they relate, and generate legal obligations for this person?

   In as far as we are discussing virtual identities (e.g. identities of virtual persons representing a physical person) they clearly cannot represent this physical person in the legal sense of the term. However, in as far as a digital identity or profile provides adequate information about a person, it could allow for the establishment of legal obligations that depend on certain conditions being fulfilled. This does not mean that the digital identity or the digital profile generates legal obligations; they merely disclose information that allows the determination of such obligations. In fact, if the information is incorrect the legal obligations attributed on the basis of this information could be non-existent. One could invoke nullity by providing the correct information. The point is who is responsible for the availability and usage of incorrect information: should the claimant have corrected the information or should the defendant have investigated whether the information was correct?

3. Can they cause harm and be made responsible for the damage incurred?

   A digital identity or profile could be a *conditio sine qua non* for the occurrence of certain damages. Making the corresponding virtual person legally responsible does not seem to make sense as it has no control whatsoever over the impact it may have.

4. Can they cause harm and generate legal liability for the data subject or the data controller who has control over them?

   If a digital identity or profile ‘causes’ a person to be categorised in a way that brings about damage, one could imagine that whoever was in control should be held liable.[100]

5. Can digital identities or profiles be further processed, sold, exchanged, transformed and if so, who can do this and to whom can they be sold or exchanged? What is the impact on the corresponding (new) virtual persons?

   This is an issue of data protection and intellectual property. Data controllers often sell the personal data or (group) profiles they have aggregated. This implies a loss of control of the data subject whose data have been used, and/or the data subject to whom such profiles can be applied.

[100] The problem with AmI scenarios, informed by autonomic computing that reduces human intervention to a minimum, is that it becomes very difficult to attribute control to a particular human being or organisation or even to a particular non-human node. This, however, does not imply that the profile itself can be held responsible (unless the meaning of responsibility is understood as purely technical).

Bourcier discriminates between digital identities and profiles and new creatures that can act on their own initiative. This seems to leave out software programmes, expert systems, and other technologies that – other than identities and profiles – perform certain actions but that do not (except when specifically programmed to do so) take the initiative. In as far as digital technologies are based on algorithms and do not move beyond mechanical application or programmed rules, they differ from her new creatures due to the fact that they have no initiative or independence. Category (b) should for this reason be split into (b).1 and (b).2. We will call b.1 (new creatures acting to some extent on their own initiative) autonomic entities and call b.2 (predictable, mechanical, algorithmic software programmes) automatic entities.

4.3 Automatic and autonomic entities and autonomous persons

At this point, it is important to make some conceptual distinctions between different levels of automation and initiative.

Automatic entities

Traditionally automation is associated with mechanical, non-creative applications that perform one or more actions automatically, i.e. in a predefined manner. In software programmes automation builds on the application of an algorithm that defines the behaviour of the programme.

Autonomic entities

The emerging technologies referred to by Bourcier have a crucially and new type of capacity: the capacity to initiate a change in their own programme in order to better achieve a certain goal. The programme's actions are not entirely predictable, not defined in a closed manner and *under*determined. Below, in section 4.5.4 we will discuss them further. Autonomic behaviour does not imply consciousness or self-consciousness. This raises the issue of whether it makes sense to speak of personhood in the case of an autonomic entity.

Autonomous persons

In law, ethics and philosophy autonomy is understood as the capacity to determine one's goals and the rules and principles that guide one's interactions. This requires both consciousness and self-consciousness, i.e. the capacity to reflect upon one's actions as well as the goals, rules and principles that inform our choice of action. Self-consciousness as the precondition for autonomous action is typical of human agency. So far, machines have not developed either consciousness let alone self-consciousness, while animals with a central nervous system do have consciousness but lack the type of self-consciousness that enables reflection and deliberation. Evidently, we cannot be sure if and if so, when machines will develop the type of self-consciousness that allows for autonomous action. For personhood in the sense of law and moral philosophy, the capability to generate autonomous action seems to be a precondition. For further discussion in the light of granting legal personhood to autonomic entities see section 4.5.4.

4.4 Automatic and autonomic entities b.1 and b.2: emerging abstract persons?

In terms of the model provided in FIDIS deliverable 2.13, b1 and b2 would qualify as an abstract person, because in terms of the model personhood does not depend on the capability for autonomous action as described above. This does not mean that such entities necessarily qualify as an abstract person in law, as this would depend on them having been attributed legal subjectivity. The question is whether it makes sense to attribute a measure of legal subjectivity to some of the virtual entities falling within the scope of (b) in order to create the possibility to accommodate the relevant abstract persons in law.

If an automatic or autonomic entity – a virtual person in the sense of FIDIS deliverable 2.13 – is attributed legal subjectivity, it will need representation to have standing in a court of law if it cannot speak for itself (e.g., a software programme). At this moment, this is the case for every legal person that is not a natural person, like for instance a limited company with legal subjectivity. It is also the case for minors or other natural persons that lack the competence to perform legal actions, even though they are legal subjects. If animals were to have standing in a court of law, they would also need representation to argue their case.

In itself, the fact that an entity is not a natural person does not preclude the attribution of legal subjectivity. However, the fact that organisations can have legal personhood while animals and trees presently cannot, raises the question of *under which conditions* it makes sense to attribute legal subjectivity and *to what extent* legal subjectivity should be granted. As explained in FIDIS deliverable 2.13, this will also depend on the relevant legal domain, because strict liability for harm caused may be adequate in private law but out of bounds in criminal law. While investigating under which conditions and to what extent legal subjectivity could and perhaps should be granted to new creatures, we must keep in mind that in the present legal framework the producer and/or the designer and/or the seller and/or the owner and/or the user of a smart technology may be imputed strict liability for harm caused. Does creating new legal abstract persons solve problems that cannot be solved by imputing liability to the designer/producer/seller/owner/user of the relevant 'new creature'? What is the added value of creating new legal abstract persons? On the one hand, it might simplify or even avoid disputes between the designer/producer/seller/owner/user of the relevant 'new creature' when liability is hard, if ever possible, to clearly attribute to exactly one of them. On the other hand, creating new legal abstract persons may generate new problems that are avoided when the designer/producer/seller (or even the user) is held liable.

4.5 From non-legal to legal abstract person?

4.5.1 Software programmes, electronic agents, expert systems, multi-agent systems, distributed intelligence: objects or subjects in law?

The crucial question is when a digital entity qualifies as a (legal) object and when it qualifies as a (legal) subject. A related question is which are the boundaries of the subject, which becomes relevant if we look into polymorphous agents, networked multi-agent systems and distributed intelligence.

To sharpen our minds we will now discuss whether a digital entity that is capable of executing a series of tasks, like a reasonably advanced expert system, warrants the status of legal subject. Such a digital entity may be either automatic or autonomic, but we do not expect it to be capable of autonomous action as defined above in the near future. We shall follow the exemplary analysis of a leading legal theorist, Lawrence Solum, and several other legal scholars who investigated to what extent non-human digital entities should be granted the legal capacity to contract (Allen and Widdison, 1996) or to be held liable (Karnow, 1996), integrating the work of Sartor (2003) and Wettig and Zehendner (2004) on electronic agents in law.

4.5.2 Could an AI qualify for legal personhood?

In a ground-breaking article in an American Law Review of the early 1990s, Lawrence Solum discussed 'Legal Personhood for Artificial Intelligences' (Solum, 1992). Though technological devices and infrastructures have developed exponentially since he wrote his article, his comprehensive approach is equally relevant today, and we will follow his arguments to see how they can inform us of the conditions under which and the extent to which it makes sense to attribute legal subjectivity to what Bourcier calls 'new creatures, capable of acting on their own initiative' (autonomic devices), as well as to less advanced but nevertheless highly influencial automatic devices.

In Solum's age, artificial intelligence (AI) was as controversial as it is now. In speaking of AI, we do not take sides in the debate of whether 'non-human intelligence' is a contradictio in terminis and we will follow Solum's pragmatic approach. Solum avoids questions such as 'whether artificial intelligence is possible'. Instead his essay 'explores those questions through a series of thought experiments that transform theoretical questions whether artificial intelligence is possible into legal questions such as, "Could an artificial intelligence serve as a trustee?" (Solum, 1992:1232). He suggests that translating questions about AI in a concrete legal context will act as a pragmatic Occam's razor. This is the case because the law incorporates the dynamic body of practical knowledge that is accumulated within a specific jurisdiction, while it is also subject to public examination and contestation. According to Solum this turns the law into a resource in which we can detect the practical implications of providing legal personhood for smart technologies.

Personhood for non-humas: a legal fiction?

Referring to John Chipman Gray's *The Nature and Sources of the Law* of the beginning of the 20th century, Solum recounts the traditional idea that legal personhood for non-humans involves a fiction unless the entity can be said to have 'intelligence' and 'will'.[101] In order to avoid controversial terms like 'will' and 'intelligence', Solum investigates whether an AI could:

- serve as a trustee (perform complex actions);
- claim constitutional rights and liberties (assuming intentionality and consciousness).

Solum thus redefines the conditions for legal personhood in terms of the capacity to perform complex actions and/or the capacity to act intentionally and with (self-)consciousness.[102] This seems to comply with the traditional idea amongst many lawyers, legal theorists, legal philosophers and ethicists that personhood implies the capacity to act in a deliberate way. We should note, however, that legal personhood is often attributed to entities that do *not* qualify for such personhood (like ships, corporations etc.). Legal theory refers to this as a legal fiction: the law attributes personhood though in 'normal' life we would not think of the relevant entity as a person. Ironically, the traditional idea that legal personhood for non-humans is a legal fiction has been challenged by Tom Allen and Robin Widdison (1996). In fact they claim that in as far as contracts are initiated, negotiated and concluded by

[101] Solum, 1992, at 1238, footnote 26: Gray, J.C., *The Nature and Sources of the Law,* (ed. By Roland Gray in 1921, original publication in 1909).

[102] We note that Solum does not discriminate between consciousness and self-consciousness, often using the term 'consciousness' to refer to self-consciousness. As explained above, in the section 4.4 on autonomic behaviour and autonomous action, we think this to be a crucial difference.

autonomous computers,[103] this attribution would imply a legal fiction if the legal consequences of these actions were attributed to the owners or users of these computers. In as far as they are not even aware of the contracts being concluded, it would be fictitious to pretend they concluded the contracts. This position is not contrary to Solum's. He argues for a pragmatic approach to legal personhood: for him the question of whether we need legal personhood is empirically dependent on the measure of independence of the artificial intelligence he discusses. Such independence depends on the capability to perform complex actions (reducing the need for human intervention) and – in the case of claiming constitutional rights and liberties – on the capability to have conscious intentions.

4.5.3 The capacity to perform complex actions

To test whether an AI could perform the type of complex actions that are required for legal personhood, Solum describes three stages of involving an expert system in the management of a trust.[104]

Stage 1:

The expert system advises a human trustee to invest in publicly traded stocks, to pay the monthly bills to the beneficiary and to fill in the forms for tax returns. The actual performance of day-to-day tasks is largely automated but the final decisions are all taken by the human trustee.

Stage 2:

The expert system begins to outperform the human trustee as an investor and the settlor decides to include instructions in the terms of the trust that the human trustee must follow the advice of the expert system. The role of the human trustee diminishes and the number of trusts that can be handled by the expert system increases exponentially. All routine interventions of the human trustee (e.g., in the case she is frequently sued by a beneficiary) are taken over by the expert system, producing letters that need only a signature of the human trustee.

Stage 3:

The settlor decides to 'do away with the human trustee' because he wishes to save money or does not trust the human who may succumb to the temptation to embezzle funds. Now, who owns the expert system? If it were a legal person it could claim an ownership right to the hardware and software that allow it to operate, but since expert programs have no legal

[103] Allen and Widdison speak of 'autonomous' computers, whereas we would qualify these computers as autonomic devices.

[104] A trust is 'defined as '"a fiduciary relationship with respect to property subjecting the person by whom the title to property is held to equitable duties to deal with the property for the benefit of another person, which arises as a result of a manifestation of an intention to create it." *Restatement (Second) of Trusts* § 2 (1959). The trustee is the legal person who administers the trust – invests trust assets, and so forth. The beneficiary is the person for whom the trust is maintained, for example, the person who receives income from the trust. The settlor is the person who establishes the trust. The terms of the trust are the directives to the trustee in the document or instrument creating the trust' (Solum, 1992:1240n).

subjectivity under contemporary law, the hardware and software are probably owned by another legal person, e.g., a company.

Solum then raises the legal question of:

> 'whether an AI can become a legal person and serve as a trustee'.

For the sake of the argument, he assumes that the trust does not raise complex moral or aesthetic issues and that it gives the trustee very little discretion. He also assumes that the expert system can make sound investments, take care of automatic payments and recognise events such as the death of the beneficiary which requires a change of action. He then pins down the issue to the question of

> 'whether the AI is competent to administer the trust'.

Against the idea that an AI could serve as a trustee, he anticipates two objections: (1) the responsibility objection and (2) the judgment objection.

The responsibility objection

The thrust of this objection is that the expert system could not compensate the trust and cannot be punished if it violates legal obligations like the exercise of reasonable skill and care in investing the trusts assets or if the expert system embezzles trust assets. Presently the manufacturer of the system can be held liable on the basis of product liability. Can we imagine the system itself to be held liable? How could it compensate for damages? Solum suggests the system could be insured, but admits that civil liability for intentional wrongdoing or criminal liability are hard to imagine in the case of an expert system.

In response to the objection, Solum discusses the reasons for punishment.

- If deterrence is the reason for punishment one could claim that since expert systems can be designed in a way that makes it incapable of stealing or embezzling, there is simply no need for punishment.
- If desert or retribution is the reason for punishment, one could claim that non-human entities are not capable of the moral judgment that is required if one is to attribute desert and retribution.
- A third reason for punishment could be educative: punishment as a learning process. Like in the case of desert, Solum finds that educating an expert system by means of punishment does not make sense, because he cannot imagine which punitive action could communicate censure to the programme.

Solum thus concludes that regarding civil liability legal personhood for an expert system could work out for as far as the system can be insured for its liability. As to criminal liability or civil liability for intentional wrongdoing, he finds that liability is hard to imagine.

The judgment objection

The thrust of this objection is that an expert system will always consist of a – possibly – complex system of rules, which does not allow the system to make judgments in the sense of exercising discretion. The objection is played out in three versions. An AI cannot cope with:

1. a change of circumstances;
2. moral choices it may encounter, and
3. some of the legal choices it will have to make.

In all three versions, the problem is that – even in the case of parallel distributed algorithms – an expert system cannot but follow rules. As to (1) it seems to lack the kind of common sense needed to solve unexpected problems, as to (2) it seems to lack the 'sense of fairness' that is warranted when unexpected circumstances require one to overrule the letter of a rule in order to serve its purpose and as to (3) it seems to lack the ability to take the necessary action if called to account in a court of law.

Solum concludes that AIs presently do not have the capacity to perform the duties of a trustee, especially in the case of unexpected circumstances affecting the trust. He raises the question whether a more limited form of legal personhood could be designed, allowing an AI to serve as a limited purpose trustee and/or for simple trusts whose operation can be fully automatic. In that case the terms of the trust will need to specify a human take-over whenever unanticipated circumstances rule out automatic behaviour.

Solum seems to restrict himself here to automatic devices. As to autonomic computing it seems that responsiveness to changed circumstances is part of its definition: even if the system cannot but follow rules, it is supposed to be capable of adjusting the rules that determine its performance. The first objection may thus fail in the case of autonomic devices. As to the third objective, this is equally valid for corporations and funds to which legal personhood has been attributed.

Limited personhood: who is the real trustee?

In the case of limited personhood the terms of the trust could stipulate that a natural person should take over in case discretionary judgment, requiring normative evaluation, is needed. This raises the question of who is the real trustee here. Why attribute limited personhood if in the end the real decisions have to be taken by a delegated or substituted natural person? This objection can be read in two ways:

1. in essence the real trustee is whoever decides discretionary issues, or
2. for all practical purposes the real trustee is whoever decides discretionary issues.

The second way of reading the objection basically raises the question of what is the added value of providing a form of legal personhood to a non-human. Solum concludes that the added value can be found in economic terms: it may be cheaper to employ an AI as a trustee whenever routine handling of affairs suffices, while the risk that an AI embezzles or frauds is practically non-existent, thus diminishing losses due to such risks. Noting that Solum restricts his analysis at this point to automatic entities, we should investigate to what extent autonomic entities are capable of exercising 'a sense of fairness'. This will be done in the next section, as this capacity seems of equal importance with regard to the issue of whether AIs can apply for constitutional protection. Before going into this, we first mention some other discussions in the literature that are closely related to Solum's first criterion of being able to perfom complex tasks.

4.5.4 Can computers make contracts?

In 1996, Allen and Widdison investigated the issue of the legal implications of digital contracting by computer systems that operate *not just automatically* but *autonomously*. They define autonomous machines as those that (Allen and Widdison 1996:26):

- can learn through experience,
- modify the instructions in their own programs, and
- devise new instructions.

This sounds very much like what IBM has recently coined 'autonomic computing', which is defined as (Kephart & Chess, 2003):

- self-management,
- self-configuration,
- self-optimisation,
- self-healing, and
- self-protections.

As already indicated above, in section 4.3, we find the use of the term 'autonomic' more apt for today's (and tomorrow's) smart devices than 'autonomous' (Hildebrandt, 2008). IBM chose the term 'autonomic' because of its reference to the autonomic nervous systems. 'Autonomic' thus refers to the independence of decision-making machines, while it also refers to the fact that the decisions are taken beyond the intervention of human consciousness. Speaking of autonomous machines could be understood as referring to human autonomy, which is based on the fact that humans can reflect upon their choices of actions and can make conscious decisions. At present, though some would claim that e.g. distributed multi-agent systems may come to act independently from their designers and users, they lack consciousness and are incapable of reflecting upon their own actions.

Allen and Widdison anticipate that what we call autonomic machines could be used for computer-generated business-to-business transactions on the internet, especially for one-off transactions that are not performed in the framework of predetermined trading relationships. They envisage that such 'on the spot' trading would encourage 'just-in-time' ordering and stock control. They argue for adequate legal protection of such transactions, to ensure that the legal consequences can be effected, for instance when it is unclear who is 'behind' such autonomically concluded contracts. One way to provide a legal infrastructure that generates reliable agreements could be to register autonomic electronic agents that initiate, negotiate and conclude contracts for a company, as agents for the company in a public register. This would enable contracting parties to locate the responsible (legal) person 'behind' the agent.

Allen and Widdison discuss four ways of dealing with electronic autonomic agents that initiate, negotiate and conclude contracts:

1. modifying contract doctrine;
2. seeing the computer as a tool of communication;
3. in the traditional analysis, denying validity to transactions generated by autonomous computers; or
4. conferring legal personality to computers.

We like to mention that their usage of the term 'computers' seems a bit awkward, as they are basically referring to interconnected systems (autonomic computing depends on connectivity; it cannot emerge on a single computer). For this reason we will discuss their suggestions as relating to autonomic digital agents.

Modifying contract doctrine

As to the first option, the authors find that relaxing the requirement of intentionality in contract-making could solve the problem of computer-generated contracts: 'the court would hold that the human trader's generalised and indirect intention to be bound by computer-generated agreements is sufficient to render the agreements legally binding' (Allen and Widdison, 1996:44). This would fit well with the fact that the 'real' intentions' of a contracting party will always remain virtual: they will be 'read' into the concrete interactions that lead others to trust the party's intention. We should however remember that the human parties that are thus bound by the contract may not know the exact terms of the contract and often not even be aware of the contract being concluded. The entire legal framework of offer and acceptance is replaced by machine-to-machine communication.[105]

The computer as a tool of communication

As to the second option the authors argue – as already indicated above - that in the case of autonomic digital agents this approach creates a legal fiction: the agents are regarded as if they are a mere instrument in the hands of the contracting parties, while in fact they interact autonomically. They remark that unexpected and unreasonable contractual obligations could arise by which the parties would nevertheless be bound. If the agents could be regarded as legal agents, courts could use the legal doctrine of actual and ostensible agency to mitigate the legal obligations.

Actual agency is defined as:[106]

> "the agency that exists when an agent is in fact employed by a principal".

Ostensible or apparent agency is defined as:[107]

> "agency by estoppel: an agency that is not created as an actual agency by a principal and an agent but that is imposed by law when a principal acts in such a way as to lead a third party to reasonably believe that another is the principal's agent and the third party is injured by relying on and acting in accordance with that belief A principal has a duty to correct a third party's mistaken belief in an agent's authority to act on the principal's behalf. If the principal could have corrected the misunderstanding but failed to do so, he or she is estopped from denying the existence of the agency and is bound by the agent's acts in dealing with the third party".

We should note that for ostensible agency an action is required by the principal, she cannot be bound to a third party (nor can a third party be bound to the principal) if there is no action of the principal that leads a third party to reasonably believe that the alleged agent is an actual agent.

Another important part of the law of agency that is relevant here is the doctrine of disclosed and undisclosed agency:[108]

> Continental European laws restrict the application of agency rules to cases where the agent acts openly in another's name. Thus, French jurists infer from article 1984 of their Civil Code, according to which agency is the act of the agent pour le mandant et en son nom ("for and on behalf of the principal"), the negative conclusion that in case an agent does not disclose that he is acting as an agent for a principal, the consequences touch only the "agent" himself. The hidden principal is not concerned by the effects of the transaction at all. Section 164 of the West German Civil Code expressly provides that "an agent, who acts without disclosing the fact that he is acting as agent, is the only one to acquire any rights and is exclusively personally liable."

[105] This is the difference between what has been coined as 'Ambient Law' in Hildebrandt and Koops (2007) and Hildebrandt (2008). Ambient Law would imply that a legal norm is articulated into a technology, which means that the legislator is aware of the affordances of the technology and also requires that if legal consequences are attributed to the violation of a norm, this is made contestable in a court of law. Replacing a legal by a technological framework is something altogether different, and could easily enforce norms in a way that places them outside the reach of the legal and constitutional framework.

[106] See for both definitions of agency and more clarification: http://dictionary.getlegal.com/agency.

[107] See for both definitions of agency and more clarification: http://dictionary.getlegal.com/agency.

[108] Quoting from: Agency. (2008). In Encyclopædia Britannica. Retrieved July 24, 2008, from Encyclopædia Britannica Online: http://www.britannica.com/EBchecked/topic/8976/agency.

> In contrast to the continental view, when an agent contracts in his own name without disclosing his principal, the common law allows the undisclosed principal under certain conditions to sue or be sued by the third party. Such conditions include that the agent had power to make the contract and that the parties eventually learn their respective identities. This wider concept of agency has no counterpart in continental legal tradition.
>
> The use of this basic doctrine in the common-law countries gives rise to questions regarding the identity of the undisclosed principal, the election of remedies that must be made by the third party, the extent of the respective liabilities, the right of the third party to setoff (the amount of its own damages from any sum that might be awarded it), etc. A solution to these conflicts of interests must in final analysis rest upon an evaluation of the extent to which the relationship between the undisclosed principal and the agent should influence the contract made by the agent with a third party.

The categories of disclosed and undisclosed agency seems highly relevant for our subject, and we should take into account what it affords in the case of attributing legal personhood to electronic agents or e.g. multi-agent-systems (MASs).

Denying validity to transactions generated by autonomous computers

As to the third option the authors point out that as current doctrine demands human intention, the actions of autonomic digital agents could not lead to a valid contract. By not relaxing this requirement (as under the first option) human parties would not be obligated by the contracts concluded by their autonomic agents. The authors indicate that the enforceability of an automatically generated contract would become dependent upon whether the agent was an autonomic agent, while in fact this may not always be apparent to the other party. This would stifle commercial enterprise, in their opinion.

Granting legal personhood

As to the fourth option the authors investigate the moral entitlement, the social reality and the legal expediency of legal personhood for autonomic digital agents. They agree with Solum (see below) that a moral entitlement to legal personhood would depend on them developing self-consciousness. However, while they agree that at present no sign of such self-consciousness has emerged, they find that the legal system could still recognise the social fact of the independent actions of autonomic digital agents. Referring to Teubner, they suggest that it makes sense to grant legal personhood to entities that are capable of what we call autonomic action. The point is not whether an agent *understands* the meaning of its actions (which would require consciousness and allow for autonomous actions). The point is only that since it is capable of developing a trading strategy of its own, it makes sense to make the agent responsible for such independent action. The legal expediency of granting legal personhood resides in allowing the agent to act as a legal agent (which is not possible for an entity without legal personhood), and to allow a contracting party to identify the digital agent as the legal agent of a specific company. They propose for companies to register their digital autonomic agents in a public register, stating the competence and limitation of liability. This suggestion is also embraced by Wettig and Zehender (2004: 128).

In terms of the model of FIDIS deliverable 2.13, we conclude that Allen and Widdison basically claim that autonomic digital agents are abstract persons, whether the law recognises this or not. They argue that attributing them the status of legal abstract persons – with a limited competence and liability – would solve a number of problems that are caused by maintaining the legal fiction that they are only abstract entities.

We like to add that their argument is not conclusive. Since they do not differentiate between autonomic and autonomous behaviour, we should reconsider which problems are raised by granting personhood to an autonomic entity. This seems an issue for further investigation.

4.5.5 Liability for distributed artificial intelligences?

In 1996, Karnow investigated the issue of legal solutions for harm caused by distributed artificial intelligences. His major point is that, at this moment, we see emergent AIs that operate in the real world with decision programs, making 'decisions unforeseen by humans' (Karnow 1996:148). These unforeseen – and sometimes unforeseeable – decisions will at some point cause damage or injury, and Karnow claims that this will lead to 'insuperable difficulties (…) posed by the traditional tort system's reliance on the essential element of causation' (Karnow 1996:148-149). He explains that the complexity of digital systems 'connotes multiple interacting but independent elements' making it 'difficult, and sometimes impossible, to predict the sum state of the complex system' (Karnow 1996:149). As to search machines, Karnow anticipates that even 'classic "expert" systems that mechanically apply a series of rules to well-defined fact patterns' (automatic systems, in our terms) will not be able to mine relevant information, due to the persistent and exponential information growth (cf. also Kallinikos, 2006). Instead, what he calls 'intelligent agent technology' will be 'responsible' for the searching of relevant databases, and for deciding on relevant actions to be taken. His reference to intelligent agent technology confirms Allen and Widdison's discussion of what we have called autonomic digital agents. Karnow (1996:154,161) claims that these agent systems are relatively unpredictable, stating that:

> 'Fixing' these unpredictable systems to operate predictably will eviscerate and render them useless.
>
> True creativity and autonomy require that the program truly makes its own decisions, outside the bounds expressly contemplated by either the human designers or users.'[109]

The problem, however, with such unpredictability is that it generates errors and faults, due to what Karnow calls 'pathological decisions' (1996:161). And such decisions are not something we can resolve by writing better programs. On the contrary, Karnow (1996:161) claims that '[t]hese are not 'bugs' in the programs, but are part of their essence.'

He speaks of the fact that 'the long-term operation of complex systems entails a fundamental uncertainty' precisely in the kind of complex and unpredictable environments that require the input of intelligent agents (Karnow 1996:162).

As these agents are both mobile and distributed, they easily move outside the control of their user and it becomes difficult to attribute causality to either the physical person or company that is 'behind' the agent. But as these agents interact within a networked world, it becomes equally impossible to attribute causality to a single node within a network (as the node builds on connectivity) or to the network as a whole. One of the reasons for this is that such intelligent agents will often be polymorphous (difficult to identify as the same agent) and the boundaries of the network are dynamic, raising similar difficulties of identification.

[109] Cf. also Sartor 2003: 'Note that the difficulty of anticipating the operations of the agent is not a remediable fault, but it is a necessary consequence of the very reason for using an agent: the need to approach complex environment by decentralizing knowledge acquisition, processing and use. If the user could forecast and predetermine the optimal behaviour in every circumstance, there would be no need to use an agent (or, at least, an intelligent agent).'

Liability in law requires causal agency: without the attribution of causality, one cannot attribute liability. Even in the case of strict liability, which forsakes traditional requirements like intention or fault, negligence, recklessness or other types of culpability, tort liability cannot do without 'proximate cause'. The concept of 'proximate cause' is a typically legal notion, used to discriminate between what Karnow (1996:176) calls 'cause in fact' (i.e., what continental lawyers would call the *conditio sine qua non*) and the legally relevant cause. The idea is that any event in real life has a multiplicity of causes that overlap and intermingle: from distant in time and space to relatively nearby or even concurrent causes. To establish liability, one needs to single out an event that allows the imputation of responsibility for harm suffered, which already limits the domain of possibly relevant causes to human action (including omission or neglect), or at least to actions performed by a legal person. To single out the relevant causation amongst the mass of causally relevant events, lawyers speak of the 'proximate cause', which is often equated with a cause that 'brought about' harm that was 'reasonably foreseeable' (Karnow 1996:178). The idea is that the (natural or legal) person that could have foreseen the harm should have prevented it (an argument also applauded in law and economics: liability must be attributed to those that can best prevent undesired events). For the same reason, someone who caused an accident in the sense of 'causation in fact' may be absolved in law from having caused the accident because of what is called an 'intervening' or 'superseding' cause that is deemed more relevant for the harm caused. Imagine that a person breaks the bike of a friend, which makes him liable for the damage done to the property of his friend. Not having the bike, his friend walks to the supermarket and gets hit by a car. Though breaking the bike is a 'cause in fact' of the accident, courts will probably consider the collision with the car to be an 'intervening cause'. Karnow (1996:181) rightly explains that what is 'reasonably foreseeable' depends on custom and common sense, meaning that in a fast changing environment like today's, 'reasonable foreseeability is a moving target'. This keeps the legal system alert and responsive to societal developments.

However, Karnow then moves on to discuss causality in an environment with autonomic digital agents. His main point is that such an environment will come to a point where the attribution of legal causality (the establishment of proximate cause) does not make sense anymore. The reason for this is that autonomic digital agents, cooperating across a distributed network, will develop what he calls 'pathological decisions' next to routine and highly original, successful decisions. Such decisions are not always predictable, they are not a matter of preventable error or bugs in the system, but – as argued above – part and parcel of the intelligence of the network. Karnow (1996:188) basically warns that we cannot have our cake and eat it too: autonomic digital agents will solve problems we could not have solved ourselves, but this will also involve an 'unpredictable pathology'. To attribute liability to any (human or non-human) node in the network, or even to the network itself, would create an arbitrary legal fiction that has no purpose in the law: since nobody could have foreseen this decision, nobody could have prevented it, so imputing causality or liability makes no sense. As Karnow (1996:191) explains:

> 'The notion of "proximate" or "legal" causation implies a court's ability to select out on a case-by-case basis the 'responsible' causes. But where damage is done by an ensemble of concurrently active polymorphic intelligent agents, there is insufficient persistence of individual identifiable agencies to allow this form of discrimination.'

One way of dealing with this situation would be to ban intelligent agents altogether. One could imagine that the principle of precaution is at play here, requiring more research into the potential consequences of harm 'caused' by entities that cannot be held responsible before introducing a technology with irreversible consequences. Another option, chosen by Karnow, is to abolish legal liability in such a case and to seek a technological solution for what he deems to be a technological problem. Instead of hanging on to the traditional tort system and trying to control the uncontrollable, Karnow proposes a Turing Registry. This Registry would enlist certified intelligent agents that are insured against the risk of pathological decisions, meaning that even when no proximate cause can be established (thus excluding strict liability) the relevant agent is at least insured in order to compensate for damages.

We agree with Karnow that the issue of unpredictable harm, 'caused' by a network with fuzzy boundaries, lacking consciousness and beyond the control of whoever designed or used it, raises a host of pertinent questions. We think, however, that his solution is not sustainable. For a start, the problem is not (only) technological but (also) social and legal: it concerns the need to attribute responsibility for harm caused. This relates to deeply seated moral intuitions about desert, deterrence, safety and security. Creating a technological infrastructure that can drift away beyond our control, causing physical and mental injury to fellow citizens without the possibility to attribute blame or at least responsibility does not make sense. Second, his solution contradicts his own diagnosis: if liability cannot be established, one can also not insure against liability and if the reason for not being able to establish causality is the polymorphous and fuzzy nature of the entities involved (nodes and network) then how could one register such an entity?

This is a good point to return to Solum's argument, taking up again the issue of whether Bourcier's 'new creatures' qualify for legal personhood.

4.5.6 Does an AI qualify for constitutional rights and freedoms?

Solum's objective in raising this question is not to prepare for the advent of artificial persons, as he believes such an event is not to be expected in the near future. Instead, he wishes to invite the reader to a thought experiment to sharpen our mind on the possibilities of AI and the related issue of their legal status and legal personhood. We will follow his argument as it may clarify some of the issues raised in the previous sections. We should keep in mind that Solum was writing at a moment when autonomic computing was hardly dreamt of, whereas today it looms just across the horizon.

The scenario on which Solum's question builds is one of relatively independent artificial agents that function as a kind of human-machine-interface (HMI) that locates relevant information for a human person, for instance in her professional life. Considering their computing power, they are capable of intelligent mining of a knowledge domain and of knowledge management far beyond the reach of the human brain. As Solum writes (1992:1256), they seem to have a 'mind of their own'. He then advances the idea that at some point in time these independent AIs could claim constitutional rights like free speech and the right not to be subject to involuntary servitude (13th Amendment US Constitution), meaning they would resist being owned by another person.

The question Solum wishes to raise is:

> 'whether we ought to give an AI constitutional rights, in order to protect its personhood for the AI's own sake' (Solum 1992, 1258).

He raises three kinds of objections: (1) only natural persons qualify for constitutional rights of personhood, (2) AIs lack some critical aspect of personhood, and (3) since AIs are human creations, they can never be more than human property. Though it may seem cumbersome to investigate these objections, we nevertheless take time to explain them, as well as Solum's response. We think that an adequate answer to the question of whether avatars, autonomic digital agents etc. should be seen as legal abstract persons will benefit from a serious consideration of these objections.

The natural person objection

Though one could claim that some constitutional rights should be restricted to human persons, we must acknowledge that specific constitutional rights (like the Equal Protection Clause and the Due Process Clause in the US Bill of Rights) already apply to non-human legal persons, while corporations also have a right to freedom of expression. The objection, however, maintains that in those cases the non-human legal person is no more than a place-holder for the rights of natural persons. A more fundamental argument against constitutional rights for non-humans is that the concept of person is intrinsically linked to humans. The idea is that since non-humans do not share our biological constitution, they cannot be conceptualised as persons. Solum counters this point by arguing that the fact that today we cannot imagine non-humans to qualify for personhood, does not imply that, in the future, AIs could not develop into non-biological entities that are intelligent, conscious and feeling in ways that *change our very concept of personhood*. Socio-biological and utilitarian arguments that it is not in our interest to grant constitutional personhood to AIs because they may take over seem to miss the point: they assume that moral obligations are only in play between humans and they ignore the fact that if AIs could take over this would certainly not depend on us granting them any rights. If we build machines that develop intelligence, consciousness and feeling – Solum seems to suggest – we take the risk of entering a new society of both human and non-human persons. We note that Solum does not differentiate between consciousness and self-consciousness. It seems that he is not always conscious of the implications of the distinction.

The missing-something objection

This argument basically evolves as follows: something (the soul, consciousness, intentionality, feelings, interests, free wills) is essential for personhood. As no AI can have this ‘something’, the simple fact that a computer could simulate having this something does not mean it actually does have it. Since having this ‘something’ determines humans as persons, non-humans cannot be persons.

Regarding the argument of non-humans not having a **soul**, Solum explains that in as far as this is a theological argument it cannot determine the attribution of legal personhood: in a pluralist society legal or political arguments need to be based on public reason, i.e., reasons that people from all different religious or non-religious beliefs can accept. In as far as the argument builds on a Cartesian duality between material causality and mental freedom, he finds it inextricably wound up in the pitfalls of an untenable dualism.

Regarding the argument of non-humans not being capable of possessing **consciousness**, Solum explains that if AIs are in fact incapable of having self-consciousness they would not be capable of experiencing their own life as good or evil, nor could they develop ends. According to Solum ends or goals are a precondition for being a right-holder. However, the question of whether AIs are capable of developing self-consciousness is an empirical question. Though at this moment consciousness seems restricted to biological beings, this in itself does not preclude the possibility of non-biological consciousness. The empirical question is complicated because a computer may simulate having consciousness, as a strategy to successfully claim constitutional rights, but this still does not rule out altogether that AIs may one day convince us of their self-consciousness. We would suggest that if AIs could in fact *simulate* consciousness as a *strategy* to claim constitutional rights, one would be tempted to infer that they have at least some kind of consciousness. We reiterate that Solum is unclear about the difference between consciousness and self-consciousness, but as he speaks of experiencing one's own life as good or evil we must presume he is thinking of self-consciousness.

Regarding the argument of non-humans not being capable of possessing **intentionality**, Solum explains that intentionality refers to 'meaning'. Just like a thermostat may seem to 'know' whether it is too hot or too cold in a room, an AI may seem to know which stocks to buy. However this 'knowledge' does not imply even the faintest idea of the *meaning* of hot and cold or expensive and cheap. So far, AIs seems to excel in *syntactics*, without having a clue as to the *semantics* of what they are 'doing'. The argument would be that as long as computers cannot give 'meaning' to their own life, it makes no sense to attribute constitutional rights. However, like in the case of consciousness, Solum argues that we cannot preclude AIs from developing meaning.

Regarding the argument that non-humans cannot possess **feelings**, Solum discusses the experience of emotions, desires, pleasures and pain. Though he has some doubts about whether personhood depends on having feelings, he moves on to discuss 'what if' emotions, pain and pleasure were to be essential for the attribution of personhood.[110] The argument then develops similarly as in the case of consciousness and intentionality: it may be that having feelings depends on our biological constitution, but it may also be the case that in the future AIs will develop feelings, though these feelings will be embodied differently from ours. In that case, he sees no reason to deny personhood for an AI.

Regarding the argument that non-humans cannot possess **interests,** defined as an interest in the good life, Solum discusses the utilitarian idea that the good life is defined as maximizing pleasures and minimising pain. In that case, the question of whether they can have interests equates with the question of whether they have feelings. However, if one takes a more objective and public perspective on interests, like John Finnis does for example, the question is whether an AI can flourish by including goods such as 'life, knowledge, play, aesthetic experience, friendship, practical reasonableness, and religion'.[111] Solum contends that even if AIs will not have a 'life' in the biological sense of the word, they might lay claim to a life in which goods like knowledge, play, friendship etc. can be realised. Moreover, if living in a pluralist society implies that we accept alternative conceptions of the good life, we should make room for radically different ways of conceptualising the good life, for which the attribution of personhood is in fact a precondition.

Regarding the argument that non-humans cannot possess **free wills**, being the precondition for autonomous action, Solum explains that in as far as AIs are merely an instrument to execute the free will of a human being, they could not qualify for personhood. The argument thus focuses on the issue of whether an AI could ever 'act' beyond the instructions (the programme) of the human that designed it. Are the actions of an AI entirely mechanical, or

[110] Solum (1992:1270) seems to agree with Kant that all rational beings qualify for personhood, irrespective of them having feelings. He also refers to Aaron Sloman's argument that any system with multiple goals requires a control system, with emotions achieving just that in the case of human beings. This seems to be confirmed by research demonstrating that intelligent people with brain-damage that reduces their capacity to be emotional can give multiple arguments for any course of action but remain incapable of making decisions.

[111] Solum 1992:1271n, referring to John Finnis, *Natural Law and Natural Rights*, 1980, at 85-90.

could we imagine them as capable of conscious deliberation, reasoning, and planning?[112] Again, this is an empirical question: we cannot preclude the possibility that AIs will develop 'a mind of their own', capable of conscious reflection, deliberation and planning. The fact that we could use a mechanical device to overrule an AI that does not obey our instructions, would – in itself – not be an argument against the attribution of personhood. It could be that this device is used precisely because the AI has developed its own reasons and plans; such a device would be like the discipline or punishment we exercise over other human beings, depriving them of the exercise of their free will rather than assuming they do not have one. We like to add that autonomic computing implies that the relevant digital agents 'act' beyond the instructions or algorithms of their human designer or user. This does however not imply that they have self-consciousness and plan or deliberate consciously about different courses of action. We must discriminate between autonomic and autonomous action. Both imply creative and partly unpredictable interactions, but autonomic action does not imply self-consciousness or the capacity for reflection that is at stake in autonomous action.

Summing up, in the case of souls and interests, Solum argues that the pluralism of our society should prevent us from imposing our own conceptions on spiritual matters or the good life on emerging AIs. In the case of consciousness, intentionality, feelings and free will, we should let experience decide the matter. As to the latter, Solum turns to the objection that we may apply the Turing test to AIs and find that they behave as persons, while in fact they are only **simulating**.[113] He points out that to make the distinction between the simulation of a person and the actual being of a person, behavioural evidence would perhaps not be sufficient. However, he claims that cognitive science could investigate the underlying processes, allowing us to confirm or reject the impression of non-human personhood.

The objection that AIs should be property

This objection refers to Locke's proposition that artefacts that are the product of human labour are the property of those who made them.[114] For Locke, a human being is not 'made' by his parents but by God, implying that a parent does not have ultimate control over his children. Solum rejects this theological argument and asserts that we believe in personhood for all human beings, even if they are 'made' by their parents. The question is whether the fact that human beings are made 'naturally' while AIs are made 'artificially' should make a difference here. Solum believes the argument does not really add to the debate: whether an AI should be granted constitutional rights depends on it being a person and in as far as this is the case an AI should not be owned by another person. Moreover, even if AIs come into the world as the property of their makers, like slaves, they can emancipate and become 'free' persons. Or, as artificial slaves, 'they might still be entitled to some measure of due process and dignity' (Solum, 1992:1279).

[112] Solum (1992:1273) refers to the idea that human actions are not caused, meaning that the free will is not subject to the laws of causation. He rejects this as an implausible proposition, suggesting that 'an action is free if it is caused in the right way – through conscious reasoning and deliberation'.

[113] This is Searle's Chinese Room argument, discussed by Solum (1992) at 1236-1238. It concerns the fact that a computer makes its inferences on the basis of syntactical correlations, without any semantic reference. Though the inferences could allow the computer to pass the Turing test, this would merely indicate that the computer can simulate a person without actually being one. On the question to what extent a Turing test should be relevant as evidence of personhood in a court of law, see *idem* at 1280.

[114] Solum (1992:1276, footnote 159) referring to John Locke, *Two Treatises of Government* §§ 25-51, at 285-302 (Peter Laslett, ed. 1988/1690).

4.5.7 Legal abstract persons: a relative approach?

Solum basically concludes that one could employ an intelligent non-human system as a trustee, attributing it a measure of legal subjectivity that fits the restricted capabilities of a system that is capable of autonomic decision-making even if it does not 'understand' the meaning of its decisions and does not have a goal in life (and does not really have a 'life' in our sense of the word). However as long as its behaviour is ultimately syntactical, based on correlations that have no meaning because the system has no consciousness of the world around it, we cannot grant constitutional protections that presume the capability to reflect upon one's actions and take responsibility. Speaking in terms of today's software: even if one would integrate the semantic web, the system would integrate this by means of syntactical correlations, not be 'aware' of the references outside the system. And, perhaps even more to the point, even if a MAS has input from RFID systems and sensor technologies that provide real-time data about the environment, the knowledge it will infer from these data will be mined by means of mathematical techniques, not implying any type of consciousness. However, as Solum points out, we should not preclude distributed connectivity from developing something like a consciousness of the world.

We agree that to decide whether a specific entity qualifies as a person and the ensuing question of whether such artificial persons should qualify as legal abstract persons, we could take a relative approach. This means that next to establishing the preconditions for personhood we should acknowledge different levels of personhood, requiring different legal consequences. Thus, a particular smart application could qualify for a restricted form of legal personhood in as far as it can insure itself against liability; however, this should not imply the attribution of rights that make no sense for an entity that has no consciousness, no intentionality, no feelings, no independent goals and no capacity for autonomous action. This would also imply that criminal liability, which presumes a subject to be capable of autonomous action, would have to be attributed to another legal subject that has this capability. This would mean that while a non-human legal subject would be liable for harm caused in terms of private law, another legal subject would be liable for the same harm in terms of criminal law. This other legal subject could be a human being, a corporation or public body with legal personality. What should interest us here is whether the attribution of a restricted legal personhood has added value in comparison with other legal solutions.

In the next section, we will try to answer the question if and when some of the emerging technologies (software programmes, distributed intelligence, avatars, etc.) would qualify for legal personhood and to what extent they should be granted legal personhood. Moving from AIs to the technologies of AmI, we will further explore the important precondition for full legal personhood that has not been explored explicitly by Solum: the issue of whether an entity has self-consciousness rather than just consciousness.

4.6 Making sense of legal personhood for emerging technologies

4.6.1 Introduction

Building on (and adapting) the definition of abstract persons in FIDIS deliverable 2.13 (see section 1.2 above) *legal* abstract persons are entities 'that have legal rights, competences, liabilities or obligations associated to them in a certain context'. We have left out the 'can' in the definition because legal persons have certain rights, competences or obligations, which define them as legal persons. Whether a concrete physical or artificial person actually realises these rights will depend on the circumstances, but at the level of abstract persons a legal subject has these rights, competences or obligations irrespective of whether she exercises them. We have added 'competences' as a typical legal term, to denote a 'power' that is not entirely equivalent with a right as this usually refers to what Hohfeld has termed a claim-right.[115] A competence provides the authority to impose certain obligations on others (the competence to legislate or adjudicate) or to undertake specific legal actions (the competence to purchase assets in the case of a trustee). We have also added 'liability' as this – like contract – is what gives rise to specific obligations, including the obligation to stand trial and to the vulnerability of being subjected to conviction and punishment.

Obviously the competence to grant legal personhood is with the legislator (and to a certain extent with the courts), meaning that the decision to create new legal abstract persons is to a certain extent a political decision. We should keep this in mind and remember that there is a connection between citizenship and legal personhood: does it make sense to grant legal personhood and deny citizenship in the case of new persons? We can image that the non-humans presently attributed legal personhood (corporations and government bodies) are not considered as citizens, because they are composed of citizens. But if we grant animals or machines the status of legal personhood, could we deny them citizenship? And if we could not deny them citizenship, what would this mean in terms of representation: should they be represented by human citizens and if so, what is the added value of giving them citizenship? In this section, we will leave this question aside, but it should be kept in mind as an argument for legal personhood may turn out to be equally valid for the attribution of citizenship. The problem could perhaps be solved by granting a restricted personhood, as already discussed above. Apart from that, there is no reason to deny citizenship to non-humans that are capable of deliberation, and in that case we should hope that these non-humans – who may be far more intelligent than we presently are – have some compassion with us in still granting us citizenship. They may in fact come to treat us the way we treat cattle in bio-industry.

Granting legal personhood concerns rights like a title to property, concluding contracts in one's own name (even if acting as an agent for another legal person), competences like voting or running for president, and obligations like compensation in the case of tort or breach of contract. It could also involve liability in the case of criminal offenses. In as far as the obligations consist of the payment of damages, a legal person can insure himself if there is no case of intentional wrongdoing. Not every legal person has the same set of rights and obligations. Children lack the competence to vote, corporations cannot run for president, whoever is declared incompetent can no longer contract without permission, and many legal abstract persons are defined as particular roles with specific legal rights, competences, obligations and liabilities (cf. the examples provided in section 2.2). Non-human legal persons often have certain constitutional rights, though they may be restricted in comparison with those of human legal subjects.

The relativity of the legal institution of the legal person does not imply that legal personality can be attributed in an arbitrary fashion. Any attribution has legal consequences and this will produce opportunities, risks and restrictions for those involved, which will often be third parties that count on the behaviours that are made possible or restricted by law. In that sense, even private law has important public consequences: in providing legal certainty, it allows economic traffic that would otherwise be too risky to undertake. This means that to evaluate if it makes sense to attribute legal personhood to non-human entities, we must anticipate which

[115] On a categorisation of different meanings of the powers attributed by law and the ensuing liabilities or obligations see Hohfeld, W.N., *Fundamental legal conceptions, as applied in judicial reasoning*, 1919.

are the consequences, comparing this to the consequences of integrating multi-agent systems, avatars and other smart technologies into our legal systems by other means.

4.6.2 Two types of non-human legal persons

For a start, we must distinguish between two types of legal personhood for non-humans, discriminating between (1) a legal subject that can perform a restricted set of (legal) actions, while these restrictions are articulated into its technological embodiment, meaning that it is programmed by means of software and/or hardware not to act outside its restricted competence, while any damages that are the result of its (legal) actions incur a strict liability in terms of private law, and (2) a legal subject that can perform (legal) actions on its own initiative, meaning that its technological architecture is such that whoever designed it cannot predict how it will further develop.

Type 1 Legal Person (T1LP)

The first type of legal person (type 1) could be made legally responsible for certain actions but in the end all these actions would be initiated by whoever programmed and/or used the entity. Attributing legal personhood could be a pragmatic response to the complexity of legal relationships that ensues when contracts are concluded via such entities (software programmes, avatars etc.) by human or other legal persons. If such type 1 legal persons (T1LP) are registered in a special public registry by their users, anybody who interacts with them can find out the extent to which they are competent to conclude contracts and how their liability in the case of damages is restricted. The public registry would register the extent of their competence as well as their liability, meaning that certain guarantees must be in place for eventual obligations to pay or to perform. One could imagine certification regarding the technological architecture of the T1LP to ensure legal certainty as to the way an entity is restricted in its actions.

Type 2 Legal Persons (T2LP)

The second type of legal person (type 2) raises more difficult questions as to its responsibilities. Though its operations will have been initiated by whoever programmed and/or employed the entity, it has been programmed for autonomic computing, meaning that it maintains, repairs and manages its own workings (Kephart and Chess, 2003). Neither the designer, the manufacturer nor the employer of this entity have full control of its interactions with its environment, which they will also not be able to predict. As it is unclear what kind of consequences its interactions will bring about, it becomes equally unclear how its competence can be restricted: if the entity cannot be restricted mechanically by means of its technological architecture, does this mean that we must address it like we address human persons, appealing to a sense of (legal) obligation? Which, then, are the preconditions for such entities to be able to respond in a meaningful way to such appeals?

T1LPs: lack of personhood

T1LPs seems capable of mechanical application of rules, *lacking the capacity to decide in the case of discretion*. In a way this means that such a T1LP is an instrument for whoever uses it, rather than a person with independent objectives. It does not really qualify as a person in the sense of being able to 'make up its own mind', which is generally taken to be a precondition for the attribution of responsibility. To the extent that responsibilities can be mechanically attributed and connected with strict liabilities and guaranteed resources to account for eventual damages (e.g. by means of insurance), one could argue for legal personhood.

However, in the case of harm caused that cannot easily be compensated (like physical harm to human beings or damages incurred way beyond the restricted liability) victims may well be looking for other culprits. If we cannot attribute responsibility at all, the occurrence would in fact be like an act of God (nature), suggesting that technology has taken over and we have nobody left to blame. This is Karnow's scenario, as discussed above. If it turns out that the designer, producer or user of the T1LP can be accused of intentional wrongdoing or negligence, thus having created the *affordance* for the harm caused (Gibson, 1986), we may still have to find ways to attribute legal responsibility to this legal person, by-passing the restricted liability of the T1LP. It goes without saying that this also counts for criminal liability. A possible added value of attributing a very restricted legal subjectivity to a technology that – in the end – is a mere instrument in the hands of a user might be to easily and efficiently handle most of the minor cases. However, there might be other solutions to investigate that might eventually appear even more apt to handle the T1LP type.

T2LPs: radical issues of personhood

T2LPs generate many more fundamental questions. Allen and Widdison's argument that denying legal personhood for autonomic digital agents is equivalent with a legal fiction must be taken seriously. Attributing liability or contractual obligations to a designer, producer or user of a T2LP seems 'artificial' in the sense of creating unnecessary complications. Why not acknowledge that we are creating technologies beyond our control, because – paradoxically – that is the only way we can retain some control over the technological infrastructure we are putting in place? We think Solum's arguments holds: empirical evidence should be allowed to convince us of the potential of emerging technologies to act autonomically or autonomously. At this point, however, we need to make a more precise distinction between autonomic behaviour and autonomous behaviour, as already mentioned above. Technologies that are autonomic need not be conscious, let alone be self-conscious. Their behaviour can be creative and unpredictable – in our eyes – but this is not the same as being the result of reflection and deliberation. Attributing responsibilities to autonomic agents cannot have the same meaning as attributing responsibilities to autonomous agents. The reason why we reject criminal liability for animals is that we find them lacking in the capacity to reflect upon their behaviour; it seems unfair to treat them as if they could have acted differently in a deliberate way. They can be trained, they can learn, but they cannot be held responsible in the sense that we hold a person responsible who was aware of an explicit prohibition. In fact, animals, other than machines – are conscious, but not self-conscious. The crucial difference between consciousness and self-consciousness has been elaborated by the anthropologist Helmuth Plessner (1975/1928), who traced the uneasy consequences of human self-consciousness in his three anthropological constitutional laws:

1. the law of natural artificiality,
2. the law of mediated immediacy, and
3. the law of the utopian position.

Without moving into the philosophical foundations of these laws, we can clarify by stating that, for human beings, artificiality is the natural way of relating to the world (humans without technological tools never existed); this also implies that their immediate perception of the world is mediated through language and technologies (humans have no direct access to the world around them: their consciousness is always partly self-consciousness); and this indirect directness implies that human beings are capable of looking upon themselves from a distance (introspection is always mediated by what others have communicated about their self).

The idea of being a person: having rights and duties and other responsibilities, builds on this uneasy, ambiguous *conditio humana*. Because we have become aware of ourselves, we have become capable of taking responsibility for the choices we make. Treating autonomic digital agents or networks as if they can act autonomously, could be a hazardous enterprise. It could equate autonomic behaviour with autonomous behaviour, ending up with a situation whereas taking and imputing responsibility is no longer related to deliberate, conscious interaction, but rather based on pure syntactical relationships between different events.

5 Conclusion

In this report, we have explored, from a legal perspective, new entities that emerge in the information society and that operate at increasing distance from the persons 'behind' them. Some of these entities can be seen as abstract persons, i.e., virtual entities with (not necessarily legal or moral) rights, duties, obligations or responsibilities. The distance between these abstract persons and their principals creates practical and legal difficulties in light of the linkability with the principals who can or should be held accountable for the actions of the abstract persons. We have explored whether current legal constructions suffice to solve potential conflicts, or whether it would help to create legal personhood for some of the new entities that function as abstract persons.

It is helpful at this point to distinguish between various types of 'personhood'. Matthias makes a useful distinction between legal, moral, and social persons, with an increasing sense of 'personality'. That is, the widest class of persons is the legal person, i.e., a bearer of legal responsibility; they can contract and compensate for damages, and can also be the object of coercive or punitive measures, but only in a utilitarian – or functionalist – sense: they lack a moral dimension. A narrower class is the moral person, i.e., those legal persons that are responsive to moral reasoning; they can be praised or detested, rewarded or punished, and they are open to moral guilt. The narrowest class of persons is the social person, also called the natural or 'full' person, i.e., the moral person who is socially accepted as a person. Most human beings are social persons, but not always; it is culturally dependent just which human beings are fully accepted as persons.[116]

We can extend Matthias' categorisation with our model of abstract entities and abstract persons. The legal person is, after all, a subcategory of the category of abstract persons, which again is a subcategory of the category of abstract entities. This is illustrated in the following graph:

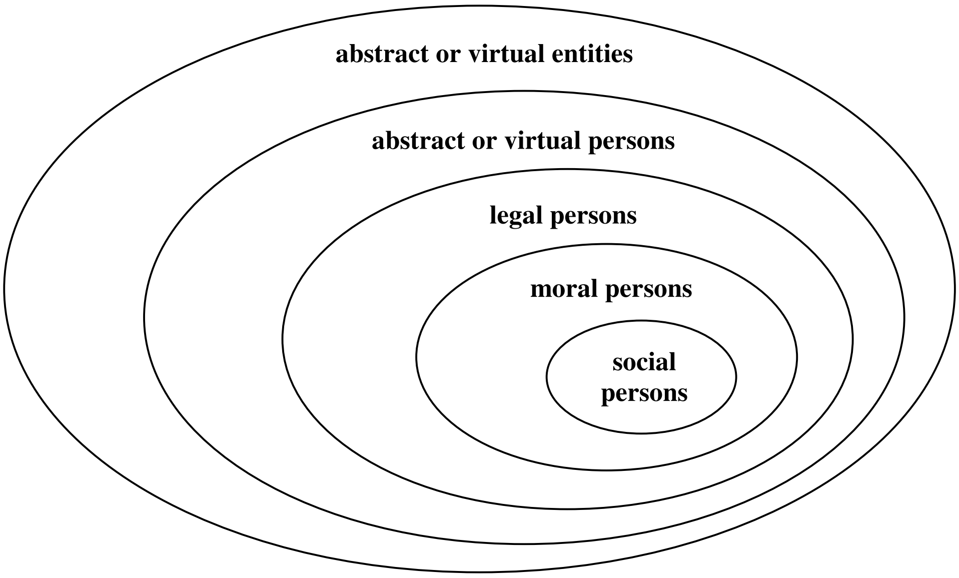

Figure 5. Categories of persons

[116] Matthias 2008, p. 43-44.

The central issue of this report can now be illustrated with this graph: certain abstract entities, like pseudonyms, avatars, and software agents, operate sufficiently autonomically that they can be considered abstract persons. The question we have explored is whether they could 'step up' one category and enter the more inner circle of legal persons, or perhaps even – in the long term – reach the category of moral or social persons.

Criteria for establishing legal personhood are not set in stone, and there is no obvious consensus distinguishable in legal literature what precisely is constitutive for legal personhood.[117] Some basics are clear, however, namely that personhood is associated with the legal capacity to act, and that this capacity involves civil actions (such as contracting) and criminal actions (committing a crime). For personhood to be meaningful, that means that an entity should be capable of performing such actions and bearing the consequences of them, which is particularly relevant when something goes wrong. It is here that legal personhood can be split in two:

- legal persons who are capable of civil actions, such as contracting, and who can bear consequences of civil wrong-doing: compensate for damages in case of breach of contract and tort; this may also include other unlawful but not morally wrong behavior, like misdemeanors[118] and administrative offenses;
- legal persons who are capable of all types of legal actions, and who can bear both civil and criminal responsibilities; this is the category of legal persons who are also moral persons.

Thus, we can distinguish between a limited and a full sense of legal personhood. What is considered constitutive for these types of personhood may depend on one's perspective on the law, for example, whether one approaches the law from systems theory, functionalism, naturalism, or legal positivism.

Regardless of one's approach to the law, it is clear that emerging entities that operate at increasing distance from their principal pose a challenge to the law. This concerns first a challenge to *determine* the law, for instance, if an electronic agent buys a camera outside his pre-programmed money range, is the contract null and void because of lack of intention to buy, or is it valid and should the principal pay – and can he then address the producer, programmer, or seller to compensate for his damages? Second, there is a challenge to *enforce* the law, because the distance between entity and principal – not only in the physical sense, but also in the metaphoric sense that the entity's action is not determined in detail by the principal's action – may make it hard to find the principal. Linking abstract persons' actions in the information society to their principals may require considerable effort, perhaps at a higher cost than the damage at issue.

Facing this twofold challenge, the legal system has three potential courses of action. First, it can *interpret* the law and incorporate the new technical developments in the existing legal system. This is daily practice, and the law has an impressive tradition in construing ways to

[117] Cf. Matthias 2008, p. 46, noting that many authors, while giving substantially varying criteria, each believe they have articulated the one and only sufficient condition for legal personhood (often based on an anthropomorphic paradigm of personhood).

[118] Criminal offenses consist of crimes and misdemeanors. Crimes are offenses that harm some fundamental value and thus can be considered as morally wrong; misdemeanors are offenses that breach a rule that is not primarily based on fundamental values but rather on creating order in society, such as the rule that cars drive on the right or left side of the road, or that citizens pay taxes.

apply seemingly inappropriate provisions to seemingly new situations. We can point to the legal doctrine of agency that has been developed to meet the increasing use of intermediaries in society to conduct transactions. It is no coincidence that the metaphor of 'electronic agent' was coined for software that roams computer networks in search of information, offers, or buyers: they have a likeness to the 'legal agent' that we know of old. The legal doctrines of messenger, undisclosed and disclosed agent, actual and ostensible agent, and newly developed theories like the programmed will or the framework agreement, can be applied to electronic agents to determine what in case of conflicts is the legal situation, i.e., who is liable. If users of electronic agents worry about liability, they can use existing legal measures to reduce their risk, for example, establish a company with limited liability as the principal for the agent. For the time being, with today's electronic agents, this seems to work well enough. For tomorrow's agents, however, applying these doctrines and theories may stretch legal interpretation to the point of breaking, when Matthias' 'accountability gap' (see section 1.4) really emerges in practice.

Then, a second strategy is to *change* the law using *specific*, well-known constructions. For example, rules can be – and in some jurisdictions have been – drafted for electronic agents, stipulating under which conditions contracts are valid and who is liable for which actions of agents. Such sector-specific rules provide legal certainty, and they can also – if the need to do so is felt – deviate from 'off-line' legal constructs, for example, limiting liability in order to stimulate the market for promising new technologies, or on the contrary, introducing strict liability for electronic agents if their unpredictable actions are felt to be too risky for business or consumers.

In line with this strategy, interesting solutions have been suggested in the literature, notably to introduce a public register for agents, which could allow contractants to find the identity of an agent's principal, or, alternatively, to lay a claim on insurance for damages in case a registered agent goes haywire. The latter is similar to the establishment of victim funds, which is a way for society to control risks involving not too high losses for potentially many people, that are hard to attribute to individual causal actors.

Such constructions can evolve into the third strategy, namely to *change* the law in a more fundamental way that affects *the legal system* more generally. Creating legal personhood for new actors is such a strategy, which has in the past been used to meet the increasingly complex social interactions of companies and states. Registering electronic agents might also be introduced with a limited type of personhood, that is, that the agent itself is responsible for its contracts and potential mishaps (outside of the moral or criminal sphere). The agent could have money itself, for example by earning a small provision for each transaction he makes for his principal, and use this money – perhaps via an insurance – to pay civil damages or administrative fines. It is currently not necessary to do this, but being aware of on-going technological developments that create more and more truly autonomic entities, we may have to consider this option in the middle or longer term. It is even imaginable that electronic agents could be attributed moral personhood in the long term, if they gain the ability to make decisions that are functionally equivalent to moral decisions, in other words, when they acquire self-consciousness (or at least something that looks to us like self-consciousness).

We have paid most attention to electronic agents in our conclusion so far, because they are the most autonomic entities to date and thus the most likely candidate for 'stepping up' a category to become a legal person. However, we should bear in mind that legal personhood has different functions: it allows an entity to function smoothly in social and economic interactions, and it provides it with legal protection. Different contexts may lead to different forms of legal personhood. Pseudonyms, for example, will likely not become as autonomic as electronic agents, but they may acquire a 'personality' of their own (like Mark Twain, for example, is a better-known personality than his principal, Sam Clemens). The reputation gained by a pseudonym may make it economically attractive to allow trade of pseudonyms, or protection against defamation and slander. Although this can likely be effected very well with current laws and legal constructions, it could be worth exploring whether pseudonyms, if they indeed acquire an important societal function of their own, could not be given limited legal personhood, rather like a ship has been attributed legal personhood to solve the very complex interactions that ships have in global sea trade.

Also, perhaps a case could be made for comparing avatars to animals, and if the call for animal rights – often along with a plea for legal personhood for animals – continues to increase,[119] why could not avatars trigger a movement for avatar rights?[120] After all, people sometimes become very attached to their avatars (section 3.2), and the Tamagotchi is an example of a once-popular technological being that appeals to people's emotions for its continued existence. Perhaps avatars will become as cuddly as panda bears, and the social need to protect them from harm will lead legal scholars to argue for another type of limited legal personhood, in that they can defend themselves in court (at first represented by human beings, like companies are, but there seems no reason why, in principle, an avatar could not be represented by a lawyer-avatar). Echoing Teubner's provocative conclusion of his analysis of the ecological movement ('Trees do have standing'),[121] we might read, in twenty year's time, an eloquent argument that in the then technological world avatars are as common, persistent and important as ecological systems, and hence 'avatars do have standing'.

Whether it makes sense to speculate on such future strategies to deal with new abstract persons, will depend on one's outlook on law and technology, on what constitutes a true 'person', and on how the world is changing.

For the time being, our research question can fairly easily be answered: current legal constructions suffice to solve potential conflicts that arise through the increasing distance between emerging abstract entities and the persons who employ them. There is no need to give legal personhood, even of the limited type to enable contracting and paying civil damages, to abstract persons. As technology evolves and entities like pseudonyms, avatars, and particularly electronic agents become more autonomic and acquire a 'personality' of their own, however, it might be useful to treat them as new entities with their own identities in themselves, with certain legal rights, duties, obligations, and/or responsibilities.[122] Should their independence reach such a level that they move beyond autonomic-ness to become autonomous, we may even consider giving them full legal personhood.

[119] Cf. Teubner 2007, with literature references.

[120] Cf. PETS, People for the Ethical Treatment of Software, http://www.elsop.com/wrc/humor/pets.htm, which parodies the animal-rights activist group PETA, People for the Ethical Treatment of Animals.

[121] Teubner 2007, p. 16. Cf. also Matthias' analysis of social personhood and machines: Matthias 2008, p. 141-234.

[122] Cf. Andrade et al. 2007, p. 372, who conclude that ultimately, a 'choice must be made between the fiction of considering agents['] acts as deriving from human's will and the endeavour of finding new ways of considering the electronic devices['] own will and responsibility.'

In order to enable us to keep answering our research question in the future as technology develops – potentially triggering a different answer – it is useful to embark upon researching and debating some further questions that are suggested by our analysis. For example:

- How autonomic are other entities than those we have analysed in this report, what are realistic expectations of their development, and what could be considered a turning point to view them as autonomous?
- Can some consensus be reached on which factors are crucial for legal personhood and for how should we interpret these criteria? Various schools of thought and legal traditions (for example, civil-law and common-law systems, legal positivism and legal naturalism, functionalism and systems theory) should further debate what constitutes a 'person' in the technological, 'post-human' society.
- Is the personhood model outlined above, of five nested categories from abstract entities to social persons, robust enough to describe all currently existing types of persons? Can it be refined or adapted to allow an even more generalised conception of personhood?
- What are alternative solutions to address technical and legal problems caused by the distantiation between abstract persons and their principals? Constructions like strict liability, public registers, and victim funds, besides limited legal personhood, will have to be refined and their pros and cons analysed, in order to assess their relative merit.
- Could we experiment with limited legal personhood for electronic agents, to gather empirical data on the merits of this option? For example, an experiment could be set up in which software agents earn money and manage a bank account, some with and some without insurance, and with a control group of agents that are mere messengers for their principals. Killing two birds with one stone, such an experiment might even be done by avatars in a game environment!

Thus, a range of questions related to abstract persons and the law await further research and debate. Timely embarking on the study of these questions will prepare society for the advent of truly autonomic, and who knows autonomous, technologies that are likely to gain a foothold in tomorrow's information society.

Bibliography

Allen, T. and Widdison, R., ‘Can Computers Make Contracts?’, 9 *Harvard Journal of Law & Technology*, 1996-1, p. 26-52.

Al-Majid, Waleed, ‘Electronic Agents and Legal Personality: Time to Treat Them as Human Beings’, BILETA Annual Conference, Hertfordshire, 16-17 April 2007.

Andrade, F., Novais, P. Machado, J., Neves, J., ‘Contracting agents: legal personality and representation’, 15 *Artif. Intell. Law* (2007), p. 357-373.

Bourcier, D., ‘De l'intelligence artificielle à la *personne virtuelle*: émergence d'une entité juridique?’, 49 *Droit et Société* (2001), p. 847-871.

Chin, B. Regulating Your Second Life: Defamation in virtual worlds, *Brooklyn Law Review*, Vol. 72, (2007), pp. 1303-1349.

Chopra, S. and White, L., ‘Artificial Agents - Personhood in Law and Philosophy’, in: *Proceedings of the European Conference on Artificial Intelligence*, 2004, pp. 635-639.

Deakin, S. Johnston, A. and Markesinis B., *Tort Law*, Calderon Press, Oxford, 2003.

Epstein, R. A., ‘Animals as Objects, or Subjects, of Rights’, in: Olin. J. M. *Law & Economics Working Paper* No. 171, 2002, available at, available at www.law.uchicago.edu/Lawecon/WkngPprs_151-175/171.rae.animals.pdf

Gibson, J., *The Ecological Approach to Visual Perception*, New Jersey 1986.

Goodall, J., and Wise, S. M., ‘Are Chimpanzees entitled to fundamental legal Rights?’, 3 *Animal L.* 61, 1997 available at www.nabr.org/AnimalLaw/Articles/Goodall_Wise_AreChimpanzeesEntitled1997.pdf.

Habel, Oliver. M., ‘Eine Welt ist nicht genug - Virtuelle Welten im Rechtsleben’, *Multimedia und Recht* (MMR), Beck, München, 2008, pp. 71-77.

Heldrich, A. and Steiner, A., ‘Chapter I „Legal personality“’, in: *International Encyclopaedia of Comparative Law, Vol. IV Persons and Family*, Mohr, Tübigen, 1995.

Hildebrandt, M., ‘Defining Profiling: A New Type of Knowledge’, in: Hildebrandt, M. and Gutwirth, S. (eds.), *Profiling the European Citizen*, Springer Dordrecht 2008, p. 17-30.

Hornung, G. ‘Elektronische Zertifikate, Ausweise und Pseudonyme - Voraussetzungen der Selbstbestimmung’, in: Rossnagel, *Allgegenwärtige Identifizierung?*, Nomos, Baden-Baden, 2006.

Jaquet-Chiffelle, D-O. (ed.), *D2.13: Virtual Persons and Identities*, FIDIS deliverable, March 2008, available at http://www.fidis.net.

Karnow, C.E.A, ‘Liability for Distributed Artificial Intelligences’, 11 *Berkely Technology Law Journal* 1996, p. 147-204.

Kegel, G., Schurig, K., *Internationales Privatrecht*, 9th Ed., Beck, München, 2004. Kephart, J.O. and Chess, J.M., ‘A Vision of Autonomic Computing’, *Computer*, January 2003, p. 41-50.

Kirtley, E., “Criminal Defamation: An ‘Instrument of Destruction’”, (2003), available at http://www.silha.umn.edu/oscepapercriminaldefamation.pdf.

Krasemann, H., ‘Onlinespielrecht - Spielwiese für Juristen’, *Multimiedia und Recht*, Beck, München, 2005, p. 351-357.

Krasemann, H. ‘Selbstgesteuertes Identitätsmanagement’, *Datenschutz und Datensicherheit*, Vieweg, Wiesbaden, 2006, p. 211-214.

Koops, B.-J. (ed.), *D5.1: A survey on legislation on ID theft in the EU and a number of other countries*, FIDIS deliverable May 2005, available at www.fidis.net.

Lange, J., Schmidbauer , K., ‘§ 823 BGBBGB’, in: *juris Praxiskommentar BGB*, juris, Saarbrücken, 2006.

Lober, A., Weber, O., ‘Money for Nothing? Der Handel mit virtuellen Gegenständen und Charakteren’, *Multimedia und Recht*, Beck, München, 2005, p. 653 et. seq.

Lucock, C., Yeo, M., ‘Naming Names: The Pseudonym in the Name of the Law‘, *University of Ottawa Law and Technology Journal*, 3:1 UOLTJ 53, Ottawa, 2006 available at: http://www.uoltj.ca/articles/vol3.1/2006.3.1.uoltj.Lucock.53-108.pdf.

Lyall, F., *An Introduction to British Law*, Nomos, Baden-Baden, 2002, p. 261.

Maeijer, J.M.M., *Mr. C. Asser’s Handleiding tot de beoefening van het burgerlijk recht, Vertegenwoordiging en rechtspersoon, De rechtspersoon* (Asser-van der Grinten–Maeijer 2-II), Deventer: Tjeenk Willink 1997.

Mahr, J. T., *Der Beginn der Rechtsfähigkeit und die zivilrechtliche Stellung ungeborenen Lebens: Eine rechts vergleichende Betrachtung*, Lang, Frankfurt, 2006.

Matthias, A., *Automaten als Träger von Rechten. Plädoyer für eine Gesetzänderung*, diss. Berlin, Humboldt Universität, Berlin, Logos Verlag, 2007. Mahr, Jürgen Thomas, Der Beginn der

Pfitzmann, A. and Hansen M., *Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology*, 2008, available at: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

Prins, C., 'Editorial - Virtual Victimisation', in *Electronic Jorunal of Comparative Law*, Vol. 11.2 2007, available at: http://www.ejcl.org/112/issue112.html.

Sartor, G., 'Agents in Cyberlaw', Sartor, G. and Cevenini, C. (eds), *Proceedings of the workshop on the Law of Electronic Agents (LEA02)*, 2002, available at http://www.lea-online.net/publications/Sartor.pdf (accessed 8 May 2008).

Schack, H., *Internationales Zivilverfahrensrecht: Ein Studienbuch*, Beck, München, 2006..

Schilling, T., *Internationaler Menschenrechtsschutz*, Mohr, Tübingen, 2004.

Schlauri, S., *Elektronische Signaturen*, Zürich, 2002, available at: http://rwiweb.uzh.ch/oberassi_schlauris/Dissertation.pdf.

Schmitt, J., '§ 1 BGB', in: *Münchener Kommentar zum Bürgerlichen Gesetzbuch*, Beck, München, 2006.

Shepherd, M., Dhonde, A., Watters, C., 'Building Trust for E-Commerce: Collaborating Label Bureaus', in *ISEC 2001*, LNCS 2040, 2001, pp. 42-56. Solum, L.B., 'Legal Personhood for Artificial Intelligences, 70 *North Carolina Law Review*, 1992, p. 1231-1287.

Teubner, G., *Rights of Non-humans? Electronic Agents and Animals as New Actors in Politics and Law*, Max Weber Lecture Series 2007/04, European University Institute.

Van Esch, R.E., *Electronic Data Interchange (EDI) en het vermogensrecht*, diss. Nijmegen, Deventer: Tjeenk Willink 1997.

Wettig, S. and Zehendner, E., 'A legal analysis of human and electronic agents', 12 *Artificial Intelligence and Law*, 2004, p. 111-135.

Yee, N., 'The Psychology of Massively Multi-User Online Role-Playing Games: Motivations, Emotional Investment, Relationships and Problematic Usage', in: Schroeder, R., Axelsson, A., (eds.) Avatars at Work and Play Collaboration and Interaction in Shared Virtual Environments, Springer Netherlands, 2006, pp. 187- 207, available online at http://vhil.stanford.edu/pubs/2006/yee-psychology-mmorpg.pdf.

Zweigert, K., Kötz, H., *Einführung in die Rechtsvergleichung*, Tübingen, 1996, p. 598 et seq.