

# Technical Rules and Legal Rules in Online Virtual Worlds

Vytautas Čyras [\[1\]](#), Friedrich Lachmayer [\[2\]](#)

Cite as: Čyras, V. & Lachmayer, F., "Technical Rules and Legal Rules in Online Virtual Worlds", European Journal of Law and Technology, Vol. 1, Issue 3, 2010.

## Abstract

In this paper we reflect on the legal frameworks which affect three-dimensional virtual worlds. Here visualisation and symbolisation precede formalisation on the way to construction and legal knowledge representation. Thus visualisation of virtual world issues can have a favourable effect on modelling, formal representation and implementation. The paper also identifies a legal informatics approach which is worded "*From rules in law to rules in artefact*". The approach concerns regulation by computer code. Rules are divided into classes, such as legal, technical, professional, reputation, etc. Modes of effect are distinguished, too. Differences of technical rules and legal rules are in the focus. The development tackles a virtual world platform within the FP7 VirtualLife project, which pursues the goal to create a secure and legally ruled collaboration environment.

The work described here is the outcome from the EU funded VirtualLife consortium of 9 partners. Maria Vittoria Crispino and Francesco Zuliani have lead the project. Project details are available. [\[3\]](#)

## 1. Introduction

The paper explores constructing legal frameworks for online virtual worlds [\[4\]](#) (see Fig. 1). In addition to normative regulation of persons, we consider the behaviour of avatars. 'Serious' virtual worlds - as opposed to leisure-based ones - are viewed as an application domain; see a scoping study by Sara de Freitas (2008).

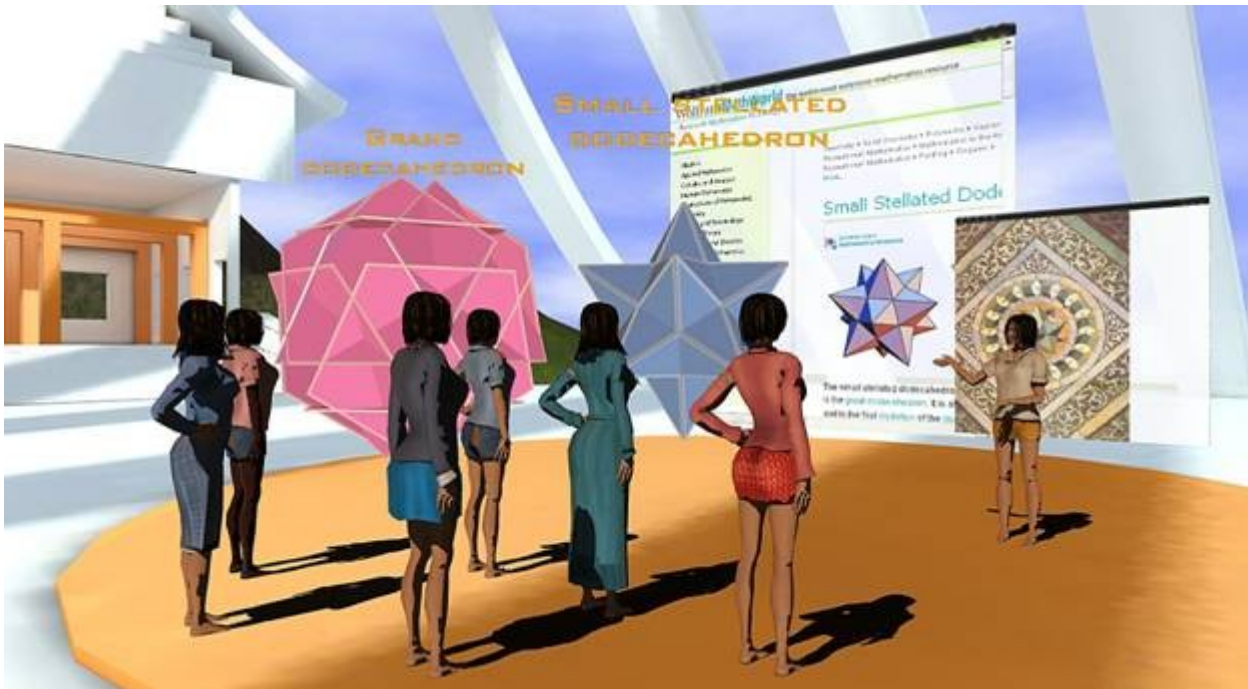


Fig. 1. Interacting with a complex 3D geometric object, a dodecahedron, in the context of a geometry lesson within a virtual world (Čyras and Lapin 2010).

To explore the above mentioned issues, normative multi-agent systems are reviewed. Actions and obligations of software agents have been investigated traditionally by computing community: computer science researchers proposing formalisms and programming languages for operationalisation of norms in software.

This paper addresses the difference between legal rules (norms) and technical (technological) rules. Technical rules are impossible to violate, but legal rules can be violated. The terms "rule" and "norm" are treated as synonyms. We tackle the implementation of legal rules in virtual world software.

The explored issues concern a virtual world platform which is being developed within the FP7 VirtualLife [5] project; see Section 3 for a fuller outline. Here the legal framework being constructed comprises a Virtual Constitution.

A virtual world is quite different from a standard video game, where there is a story, a final purpose, and the system only allows for a limited set of actions. In a virtual world there is no determined purpose, there is no 'game over', people move their avatar and establish their second life, driven by different motivations and with different purposes. Thus the rules of play have to be replaced by a sophisticated legal framework, which is considered to be essential in order to guarantee the existence of a secure and safe virtual world. In VirtualLife the legal system must take into account both real life values and virtual world laws (Bogdanov et al. 2009).

Sketching the legal issues of virtual worlds is first dealt with in this paper. This is depicted by the metaphor of a stage. Such a general sketch presents a personal reflection of the authors; it serves as a visualisation [6]. It plays the role of a model, a symbolisation of the conceptual framework of the virtual world. It is generally called spatialisation.

All the rules are subject to implementation in virtual world software. In this context, law enforcement is a tough issue. The addressee concept of classical rules - persons - is supplemented with avatars. A sample "toy" rule 'Keep off the grass' can illustrate constraints on avatar behaviour. Various methodologies are investigated worldwide to program the rules. Programming languages include external tools and script languages (e.g. LSL, Python, Lua, etc.). As a programming exercise, consider a virtual world and the following scenario. Suppose you build a house with a door which is controlled by a rule which permits entering avatars from a certain group only, for instance, your trusted friend avatars; other avatars are forbidden. In Second Life, this rule can be programmed by LSL (Linden Script Language). To program rules, each virtual world platform needs a specific framework.

Our focus on visualisations sets aside mathematical formalisations. Relevant logical formalisms are investigated in computing extensively, for example, by the normative Multi-Agent Systems (MAS) community, cf. Boella et al. (2009) and Section 5 further. Formal notations bring the following risks. First, the spirit of law can be lost. For instance, a variety of obligations and permissions is richer than can be expressed with deontic logic. Second, legal scholars can experience difficulties understanding formalisms. An advantage of legal scholars is informal knowledge of key legal concepts. This knowledge differs from formal language semantics; see Leith (2010) on legal expert systems and formalising legal knowledge.

## **2. The Frame of a Virtual World**

This section describes informally different kinds of rules in three dimensional virtual worlds that are inspired by a metaphor of architecture. Such an immersive virtual environment is different from 2D menu paradigm. A virtual world is a kind of networked virtual environment (NVE) that allows users to interact with each other and the world through avatars.

The frame - the reality of a virtual world - is constitutive. The entities are comprised of avatars, and 3D objects such as buildings, rooms, information stands, avatar inventories, vehicles, etc. (see Fig. 1). An avatar is a computer user's representation (usually a 3D model). Every avatar is monitored by its user. The avatar can also be viewed as the cursor on the screen.

The frame of a virtual world is established from the outset; this framework is not discussed in this paper. A conceptualisation of the "theatre" is depicted in Fig. 2. The entities of major importance are avatars, their actions and rules, which regulate the behaviour. The avatars can also engage in joint actions. Avatar chat communication can be via voice or text chat.

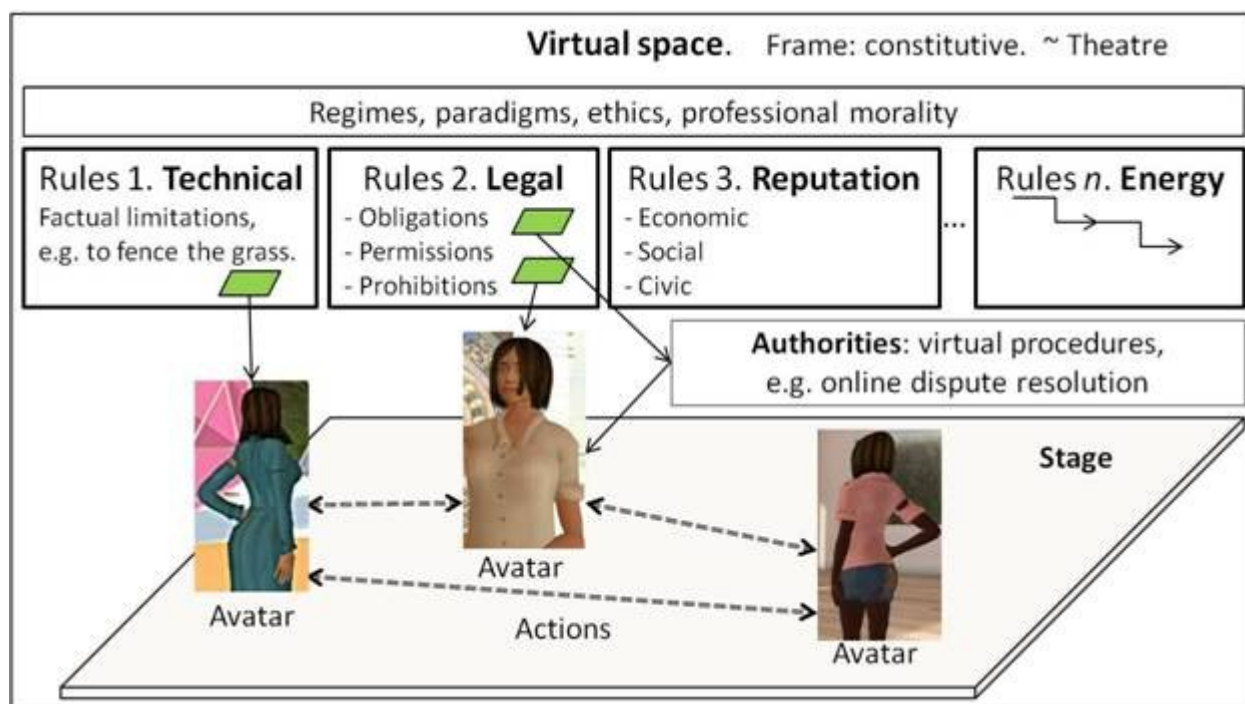


Fig. 2: A conceptualization - the elements of a virtual world.

Rules establish a regime (paradigm) of the virtual world. They can be divided into different classes such as technical rules, legal rules, reputation rules, energy rules, professional rules, etc.:

- **Technical rules.** They establish factual limitations. Real world examples are to fence the grass, to close the door to forbid entering, to refuse money by a cash machine if you do not provide the PIN code. Violations are impossible: there is no possibility of violating a technical rule unless you break the artefact completely. Hence technical rules are strictly enforceable.
- **Legal rules.** Their nature is that they *can* be violated. For example, you can step the grass, you can take a train without a ticket, etc. But you risk being sanctioned. A procedure is enforced by an authority such as police, peacekeepers in a virtual world, etc. A sanction is imposed with a certain probability. Hence the legal rules are not strictly enforceable. Herein is the spirit of law.

There is no strict boundary between the technical and the legal rules; a grey area exists.

The structural elements of legal rules are the same as of real-world norms. The subject is a natural person, a juridical person, etc. The modus is a deontic notion: obligatory, permitted, prohibited, etc.

Legal rules are of two kinds. The primary rules come first. Sanctions are determined by secondary rules. They are associated with authorities which enforce the rules. Virtual procedures can be raised for violations. For instance, online dispute resolution is a kind of procedure.

The modes of effect can be different. A sanction can be raised randomly with a

certain probability  $p\%$ . An example is a road rule which forbids crossing a street against traffic lights. You can go through a red light and if you are lucky a policeman will not punish you.

Legal rules are essential in virtual worlds - similarly as in the real world. It is impossible to implement normative regulation in a virtual world by means of technical rules only. Consider a norm that indecent content is prohibited in the virtual world. Such an abstract norm can hardly be implemented by automatic checking. For instance, a naked body need not be automatically treated as indecent content; this may be a picture of a statue in a virtual museum.

- **Energy rules.** They sanction in the following way. If a prescribed behaviour is violated appropriate "energy" points are reduced. The addressee can be sanctioned effectively, i.e. 100%.

This can be illustrated by security/trust rules, reputation rules and the avatar identity card in VirtualLife. Each avatar has an ID card, which contains information about both his virtual and real life identities; see Fig. 3 (Bogdanov et al. 2009). The ID card includes simple indicators of trust. A red (entrusted) bar means that the avatar is a guest and has not proved his identity; a yellow (weakly trusted) bar - the avatar has an identity, but it has not been verified by any certification authority; and a green (trusted) bar - the avatar's identity has been verified by a certification authority. Each avatar also has an economic, social and civic reputation, whose indicators are handled by a sophisticated reputation system, depending on the avatar's behaviour. Thus the rules are implemented in software by hard constraints.





Fig. 3: Virtual identity card in VirtualLife (Bogdanov et al. 2009). The reputation of avatars can be taken into account while chatting.

- **Professional rules.** Other kinds of rules comprise moral rules, professional rules, user community rules, etc. Examples are provided further from the VirtualLife project where the users can engage in a trusted community called Virtual Nation. Different communities are governed by different rules. For instance, Students and Teachers form different Virtual Nations in a University Virtual Campus that is purposed at learning support (Čyras and Lapin 2010).

### 3. About the VirtualLife Project

This section describes the VirtualLife project as presented in publications (Bogdanov et al. 2009; Bogdanov and Livenson 2009; Čyras et al. 2010; Čyras and Lapin 2010) and project deliverables co-authored with partners. The project aimed to develop a prototype of a virtual world platform which was innovative from the administrative, security and data protection perspectives, an evolution of 3D virtual worlds towards a stronger digital trustworthiness. The main innovative features to be promoted and exploited in a commercial way are:

1. a novel editable and enforceable Virtual Constitution,
2. an enhanced security framework, and
3. a peer-to-peer (P2P) network architecture.

VirtualLife represents a transition from existing virtual worlds administrator-centric (ruled by an almighty administrator) to a civil organisation ruled by a common *jus gentium*.

Security and trust contribute to legal values such as equality, avatar integrity, honour, reputation, privacy, free movement, freedom of thought, freedom of association, sanctity of property, etc. which are listed in the code of conduct within the Virtual Constitution.

A motivating example of identity verification and trusted service provision is business transactions, where parties need to identify each other to enter an agreement. Another example is a system the users' age to restrict access to age-specific content or provides age information to communication partners (Bogdanov and Livenson 2009).

To prove the concept, currently VirtualLife is targeted at scenarios focused on learning support, such as (1) a university virtual campus and (2) simulations of human and environmental interactions in costly or dangerous situations.

### **3.1 The Architecture of VirtualLife**

**Balancing goals.** In order for a platform to succeed, it must be accepted both by the users and service providers. The users are looking for a good experience and the service providers want to provide it with minimal expenses. In our research, we are looking into ways for balancing both goals using peer-to-peer technologies. P2P techniques are used to decentralize services like content distribution as they allow us to build a system that uses resources from all its participants. [7]

**Peer to peer.** VirtualLife has been built with P2P design in mind. The design of the network layer, identity management and virtual reality engine components is influenced by the paradigm of autonomous processing. For example, connections can be made directly between VirtualLife peers and these connections can be authenticated and encrypted. The virtual reality engine offloads computations and management tasks to other nodes in the same virtual zone. We note, that VirtualLife is a hybrid peer-to-peer system with some tasks left to the virtual zone and virtual nation nodes for easy accessibility and bootstrapping.

**Nodes, virtual zones and virtual nations.** Each virtual world in VirtualLife consists of a peer-to-peer network with nodes connected using a secure protocol. Control in each world (referred to as a virtual zone or shortly zone) is managed by a zone server (Z-server). A collection of zones forms a nation, consisting of a network of virtual zone servers. The use of Z-servers gives the end-user the full control over the fundamental components of the virtual zone and the persistence and protection of his critical data; see Fig. 4 (Bogdanov and Livenson 2009).

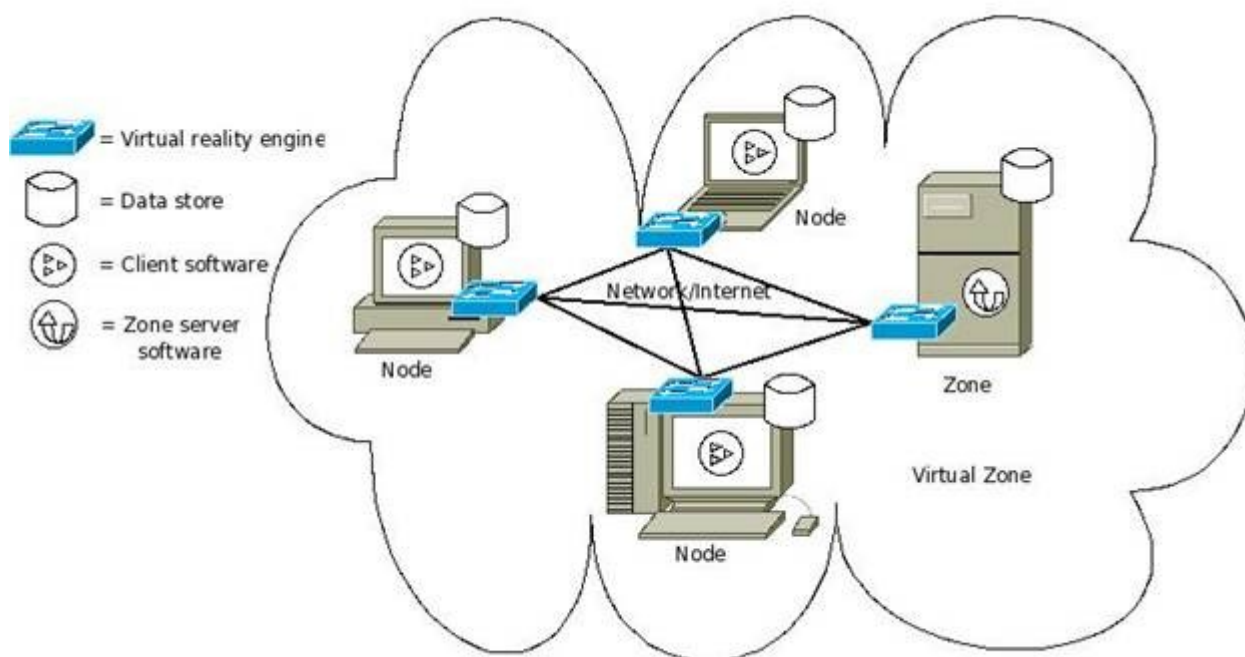


Fig. 4. Peer-based connection model of a virtual zone (Bogdanov et al. 2009).

The security layer provides a wide range of services that are used by other components. These services include data structures and operations for cryptographic primitives, certificate management and authorization. The system is built on top of the X.509 public key infrastructure standard (Housley et al. 2002), which is widely used for securing access to the sensitive services, for example, e-mail accounts and online banks. It defines a hierarchy of trusted third parties called Certification Authorities that issue temporary digital documents binding together a public key and identity information. These digital documents are called *certificates* (Bogdanov and Livenson 2009).

**Virtual zone server.** Unlike traditional client-server approaches, there is no centralized point of *truth* regarding the state of entities in the P2P virtual environment. The truth is maintained in a distributed fashion, where a single node on the network is the *Authority* for a particular entity. The authority node is the only node that sends 'update' messages to the rest of the peers, where the latter resolve their internal representation with the truth obtained from the authority.

The virtual reality engine of VirtualLife is designed to be a non-centralized mechanism that functions across a number of machines connected by a network. However, to maintain the goals of security, integrity and persistency, it is imperative that at least one of these machines have an extended role to perform these functions. We refer to this machine as the Z-server. Anyway, while performing some server-like functions, the communication system within a virtual zone is primarily peer-based (see Fig. 4).

The Z-server has the following roles within a virtual zone: (1) node authentication and authorization, and (2) persistency - the state of the virtual zone is regularly saved here.



## 3.2 Virtual Nation Overview

A virtual nation is a set of users sharing the same purpose and values. The virtual nation introduces concepts of the real world such as constitution, government, monetary system, register office in the real world (see Fig. 5).

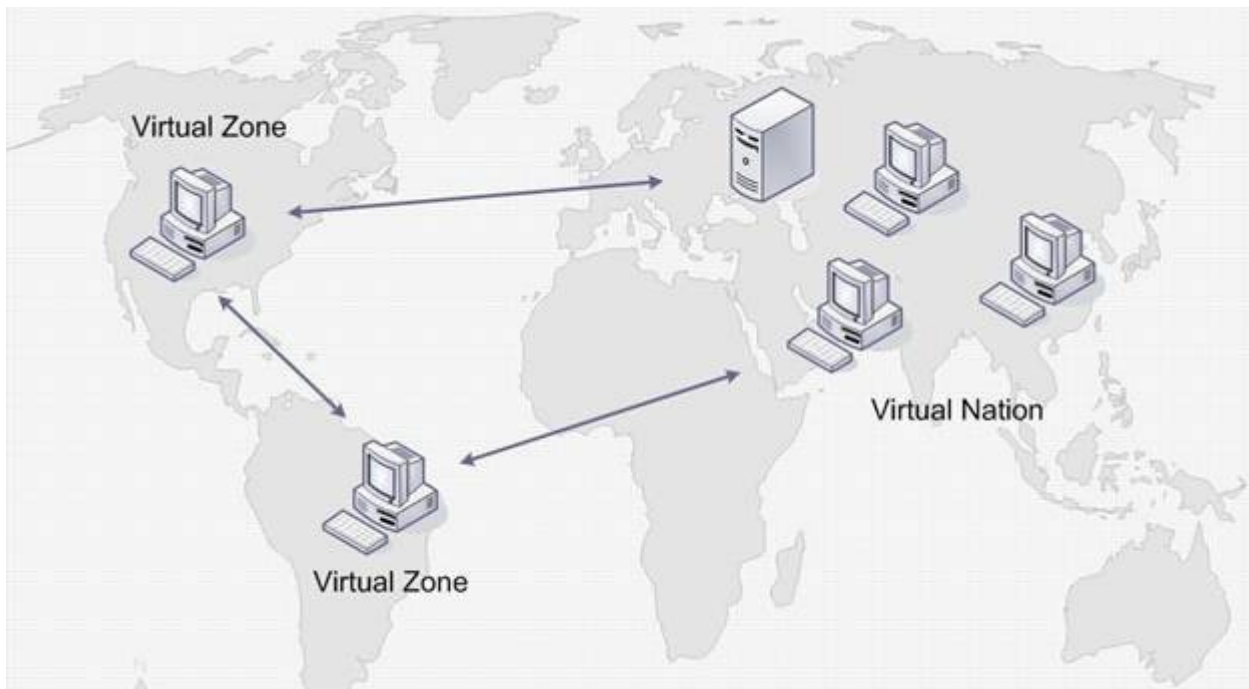


Fig. 5. Virtual nation (Bogdanov et al. 2009).

A virtual nation is defined by: (1) the list of virtual zones belonging to it; (2) the allowed avatars (virtual citizens), authorised by a certificate generated by the virtual nation; (3) the constitution (that will be mapped onto a set of technologically implemented laws); (4) the timing reference. The virtual nation attributes are hosted on an appropriate server that exposes an application capable to manage the virtual nation entity (i.e. to give the national timing, the ruling laws, the user membership, etc.).

## 3.3 The Trust Model of VirtualLife

An identity requirement is to assure that the user behind an avatar is this who he claims to be. Strong identities are required for the legal system. [8]

### 3.3.1 Responsibilities

The VirtualLife deployment consists of multiple nodes hosted by various organisations. In the course of running the virtual world, they will need to trust each other to perform certain duties and to refrain from actions that harm the other nodes.

Trust issues between VirtualLife nodes are reviewed by their responsibilities. For each node the tasks that the other nodes expect to perform are as follows:

- **Virtual Nation.** (1) Bootstrapping nodes with VirtualLife identities. (2) Processing

avatar and zone registration (login and authorisation) and profile management. (3) Maintaining runtime information about active avatar and zone nodes. (4) Providing nation-level services to other nodes in the nation (constitution management, electronic voting, online dispute resolution, NAT [9] punchthrough setup, etc.).

- **Virtual Zone.** (1) Maintaining and storing the state of the virtual world piece it manages. (2) Participating in the distributed simulation of the virtual world by sharing the world state with avatars. (3) Allowing authorised avatars to enter the world. (4) Allowing authorised avatars to modify the world state. (5) Allowing authorised avatars to store and retrieve their objects in any zone.
- **Client.** (1) Participating in the distributed simulation of the zone virtual world by sharing a part of his resources to simulate the world. (2) Responding to authorised communication attempts.

These responsibilities reflect the services provided by each node. Every host running any of these nodes should provide these services to any other node in the VirtualLife nation.

### **3.3.2 Trust Relations and Assumptions**

Whereas responsibilities represent promises that nodes expect other nodes to keep, we also need to consider actions that nodes are expected to refrain from. This list is typically more extensive, as any misbehaviour can be considered a security risk. Listing all restrictions is infeasible and therefore a set of security goals is selected for a system.

In security engineering, security goals are balanced with the expenses of implementing controls for achieving them. If a security goal is too costly to achieve, it may be relegated to be a security assumption. For example, in VirtualLife we assume that the nations and zones perform operations on behalf of the avatar only when the avatar has given the command directly or via a script.

This is possible thanks to the use of strong identities - every node can ask the other node to identify itself during data exchange. A node can refuse to communicate or provide a service when the other party fails to provide an identity proof.

This entire means that every node is at least partially responsible for its own security. This is a very reasonable assumption, because the peer-to-peer nature of the VirtualLife world allows for situations where information from a service provider reaches the client through third parties whom the client has no reason to trust. Therefore, in building VirtualLife, we have tried to minimize the trust nodes need for each other.

Trust and reputation are more important in systems with a commercial component such as auction or sales environments. If many other users consider a seller to be trusted, more users have a reason to trust that seller. On the other hand, a seller with a negative reputation will be avoided by new customers.

### **3.3.3 Identity Verification**

Upon entering a VirtualLife nation the user must have an identity. This identity will later be used in all authenticated operations. VirtualLife identities are based on X.509 certificates

and a VirtualLife nation contains a certification authority to bootstrap users with no access to other sources of certificates. The identity system is described in (Bogdanov and Livenson 2009).

A virtual identity can use a number of different key pairs, issued by different certification authorities. Different certified key pairs have a different level of trust. There is no chance of having the same key pair as that of another user, unless the key pair has been stolen.

Two "traffic lights" are proposed to include in locations where the user must make a decision whether to trust another user or not. The first traffic light represents the strength of identity and the second one - the reputation. The identity traffic light has three states based on the policy of the certificate authority that issued the user certificate: (1) red (entrusted) - guest or temporary user; (2) yellow (weakly trusted) - certified by an authority that does not verify people's identities using a document and/or physical appearance; (3) green (trusted) - certified by an authority that verifies user identities. The reputation traffic light has three states as well, depending on whether the user has negative, neutral or good reputation.

### **3.4 Security**

Security is very important in on-line systems in particular for the protection of users and contents. In the analysis of competitors' virtual worlds, project partners did not find specific and well defined mechanisms which guarantee security when joining the community. Most of the platforms are focused on implementing a strong authentication system based on username and password. Some integrate the common login process with hardware or standalone devices in order to improve security.

Some mechanisms have been considered in order to assure the users, even in a weak way that the world is secure and reliable. Current virtual worlds usually introduce moderators in order to supervise avatars' in-world behaviour and user generated content. Moderators and system administrators are able to suspend or ban accounts depending on the severity of the offence that the related avatar has been accused of.

Innovative features in VirtualLife are the following:

1. Identities are harder to steal, as the PKI key-pairs of the user are not stored online but on the client side. This means that losing a password will not allow anyone to access an account from anywhere else.
2. True identification of communication partners.
3. VirtualLife outsources some state processing to other nodes, but only ones that the outsourcing party trusts.
4. No technical means is implemented to remove inappropriate content. It will be handled by a moderating process.
5. No tools for detecting cheating. In MMORPGs (massively multiplayer online role-playing game) servers need clients to behave well. In VirtualLife trust relations are more equal and aim towards rationality. Here the design philosophy with respect to trust is that a user must prove something to be trusted. Every party is in charge of

verifying the actions related to its data and rights. The machine of a client, zone or nation is considered to be a tool of its user and the others do not have to communicate with someone who does not play by the rules.

### **3.5 Innovative Features in the Virtual Legal Framework**

It seems that currently the only sources of rules in a virtual world are the end-user licence agreement (EULA) and the terms of service (also called terms of use). The EULA is not enough for many reasons, in particular:

1. It only partially governs the relationship between the provider and a user but not between users.
2. It is in most cases unilateral (it protects the provider's interests but not those of the user).

When the user enters a virtual world, he automatically becomes part of a community. This means that he interacts with other users. These interactions are, in most cases, peaceful but are also likely to produce conflicts. When a conflict takes place, the need for resolution arises.

Present virtual worlds try to prevent conflicts through the rules of conduct contained in the terms of service. But still, this regulation is not enough. The existence of rules does not prevent a user from adopting a bad behaviour towards another user. When a user feels that an injustice has occurred, the only way through which the user can seek justice is to report the abuse to the virtual world creators that can decide to ban or punish the griefer (the term to refer to someone acting "illegally" in a virtual world). In some cases the virtual world creators invest in specific techniques to keep the virtual world "under surveillance". For instance, this is the purpose of the peacekeepers in Active Worlds.

Thus an innovative feature in VirtualLife is a legal framework that is compliant with real world law. Following are some features of the legal framework:

1. In order to become a citizen, the user can be asked by the Virtual Nation to certify his real identity, in other words, the virtual identity of the user is bound to his real one (a certification authority guarantees this correspondence).
2. As soon as the user becomes a citizen of a virtual nation, he must accept the laws in force in that specific nation, specified within the Virtual Nation Constitution.
3. There are two different constitutions. First, a Supreme Constitution that is made of fixed rules (that cannot be changed by the user). Second, the Virtual Nation Constitution (one for each virtual nation) which will be made of modifiable laws that can be changed by virtual citizens, thanks to a voting system which is in force in each nation. The Supreme Constitution is a kind of EULA with a great innovation: the fact that the user of a virtual nation as well as the administrator of a virtual nation has to accept it. Therefore it does not protect the administrator's rights but binds him in the same way as it binds the user.
4. The constitution also contains a list of templates of contracts that can be used to regulate "business" relationships between users.

- Each virtual nation should have an arbitration service, i.e. a dispute resolution ruled by the nation with a mediator board made of virtual citizens.

### 3.6 Focus on VirtualLife Legal Framework

The VirtualLife's legal framework is a three-tier system; see Fig. 6 (Spindler et al. 2008). First is a Supreme Constitution. It contains fundamental principles of VirtualLife that every user has to adhere to. Additionally, it sets out the basic organisational rules according to which the laws of a virtual nation, the second tier of the framework, are formed. A Virtual Nation Constitution then contains special and more detailed provisions as regards, for example, the protection of objects used in that Virtual Nation under copyright law, the issuing of currency or the authentication procedure required to become a member of that nation. (Distinct virtual nations, for instance, a university virtual campus and a virtual mall, should be governed by different rules.) Both the Supreme Constitution and each Virtual Nation Constitution, as being ordinary contracts, are implemented by way of click-wrap agreements. The third tier consists of different sample contracts that the respective parties to a contract may deem relevant for their transaction, though they are still free to use their own contractual terms.

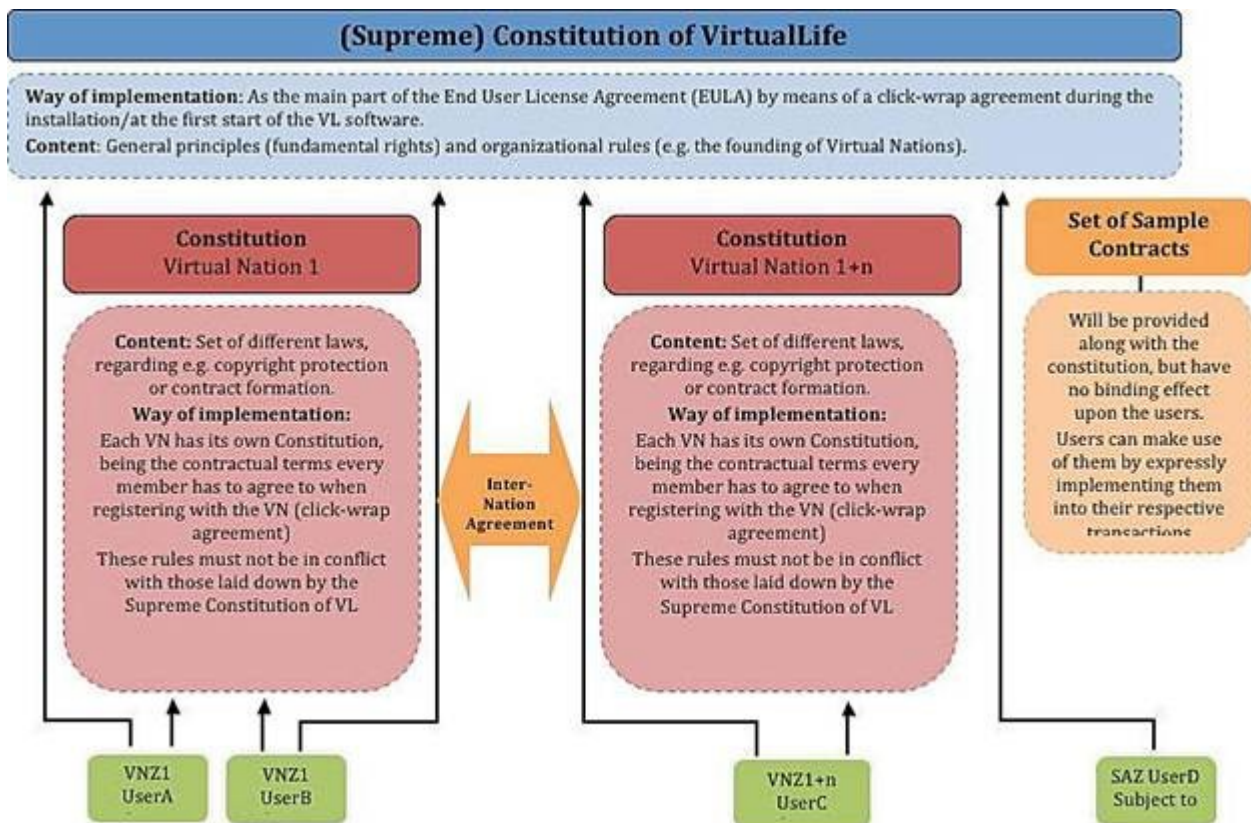


Fig. 6. VirtualLife legal framework (Spindler et al. 2008).

One should note that placing the virtual constitution (the Supreme Constitution and a Virtual Nation Constitution) in the level of contract law contributes to law enforcement. The EULA represents soft constraints on users' behaviour through their avatars. Apart from this, a user of VirtualLife software is not ruled exclusively by the mentioned sources, but



also by the user's national law. It should be noted that the users cannot escape from the real-world law, cf. (Spindler et al. 2010).

### **3.6.1 Virtual Nation Scenarios**

A number of examples for allowing different scenarios can be proposed. Different values and rules are covered by NoCopy, CopyRight and CopyLeft nations [10]; see also (Čyras et al. 2010). Permission language tables serve to implement distinguished rights. The permissions are represented explicitly in computer code:

In a NoCopy nation, no one is allowed to make copies. In a strict copyright nation, only the author of the object can make copies. The receiver of the copied object cannot make copies.

In a non-strict copyright nation, the original author of an object can decide if the new owner can copy the object or not. By default, an author or owner can copy.

In a CopyLeft nation, the creator's information is preserved. Each user can change and copy its own objects.

In a Second Life model nation, you can sell objects controlling whether they are editable, copyable or sellable. The creator cannot modify a sold object. Of course, you can always move your own objects. For example, the seller can decide to sell non-copyable objects. This object cannot be duplicated by the new owner. Therefore if she puts them in her inventory they disappear from the world.

### **3.6.2 From Rules in Law to Rules in Artefact**

The editor of rules comprised in the VirtualLife platform is a tool to compose laws. The rule concept is approached taking into account (Vázquez-Salceda et al. 2008). A sample rule 'Keep off the grass' is transformed into 'The subject - avatar - is forbidden the action - walking on the grass'. Thus the concept of "Ought to Be reality" (see e.g. (Pattaro 2007)) can be extended from the real world to virtual worlds. Following are examples of rules [11]:

- An avatar is forbidden to touch objects not owned by him or a certain group.
- An avatar not belonging to a given group is forbidden to a given area of the zone.
- An avatar is forbidden to create more than a given number of objects on a given time interval.
- An avatar is forbidden to use a given dictionary of words (slang) while chatting.
- An avatar of age is forbidden to chat with avatars under age.
- An avatar is forbidden to execute authorised scripts in a certain area.

If an avatar violates a rule (e.g. steps on the grass), his reputation is decreased. Rule enforcement is implemented by triggers. They trigger the changes of the virtual world states and thus invoke avatar script programs.

### **3.6.3 Unfeasibility of Implementing Legal Rules**

We understand that it is unfeasible to implement legal rules in software in the full extent. Legal rules allow too much space for interpretation; see also (Leith 2010). Moreover, the limits of this space are interpreted by jurists - not programmers. However, technical rules can be implemented as they allow little space for interpretation. Despite the latter, law enforcement is still a problem.

Legal rules in VirtualLife legal framework texts are formulated in a human language. A norm is treated as it is generally accepted in law - a rule of human behaviour. As mentioned earlier, the concept of the subject of a norm (legal subject) can be extended to avatars. The operationalisation of rules aims primarily at preventing unwanted behaviour. Recall the rule 'Keep off the grass'. Software is required to translate rules into machine-readable format. Such a translation seeks capabilities of a whole team of experts. A team comprises at least a legal expert, a virtual world developer and a programmer. Translating legal rules requires natural intelligence. The translator copes with the following problems (including but not limited to):

1. **Abstractness of norms.** Norms are formulated (on purpose) in very abstract terms; cf. (Vázquez-Salceda et al. 2008).
2. **Open texture.** This can be illustrated by Hart's example of "Vehicles are forbidden in the park" and its analysis in (Bench-Capon 2002).
3. **Heuristics.** It serves to translate abstract high level concepts and invent low level ones.
4. **Teleology.** The purpose of a legal norm usually can be achieved by a variety of ways. They need not to be listed in the text of a statute and specified in detail.
5. **Legal interpretation methods.** The meaning (semantics) of a legal text cannot be extracted from the sole text. Apart from the grammatical interpretation, other methods can be invoked, such as systemic and teleological interpretation.
6. **Consciousness of the society.** Law enforcement is subject to complex social phenomena such as legal consciousness of the community. Modelling them is a tough task.

### **3.6.4 The Law of Avatars**

In this subsection, we focus on the law of artificial agents. We call this kind of ruling "virtual law". It aims at legally ruled behaviour of avatars. An example of a norm is that an avatar is prohibited to hurt other avatars, for instance, to commit a (virtual) crime over avatars. Thus we approach a code of avatars that is concerned by Koster (2006). [\[12\]](#)

**Law enforcement is a problem.** Enforcing the virtual law remains a problem for the reasons mentioned above. The rules of games such as chess can be programmed.

However this is not a case for legal rules within the code of conduct in a virtual constitution. A sanction for a norm violation might be very straightforward - to withdraw the artificial agent from the community (e.g. to ban it from the game). However this sanction is not the best solution; recall the history of real-world legal systems. In the virtual world, sanctions are required to be expressed in terms of technical rules in order to program them. Elaborate sanctioning should encounter multiple values which are imminent both in the real and the virtual world.

Extending the real-world law to virtual worlds raises the following question: Who is liable when an avatar A hurts an avatar B? Again, a straightforward answer is to attribute the liability to the human owner of A. However the effectiveness of virtual law enforcement requires a solution which prevents harmful behaviour. For this reason, prohibitive behaviour of avatars is required to be expressed by technical rules and programmed. However this is not always feasible.

**The rights of avatars.** The designers of actions over avatars have to care that such actions do not infringe the so called "virtual rights" of other avatars. For example, the physical integrity of the body of other avatars shall be preserved when my avatar takes an action - walks, moves, flies, etc. Here a question can be raised what the concept of the rights of avatars is. For example, Article 4 in Koster (2006, p. 68) states that "Liberty consists of the freedom to do anything which injures no one else including the weal of the community as a whole and as an entity instantiated on hardware and by software; the exercise of the natural rights of avatars and therefore limited solely by the rights of other avatars sharing the same space and participating in the same community." Setting aside high level answers, we aim at an implementation level solution. Programmers determine a right by actions which are permitted or prohibited to avatars in the virtual world program.

In a serious virtual world, it is impossible to provide an exhaustive list of avatar actions. Moreover, each action can be regulated by a separate "virtual statute". This is similar to the real-world law where specific relations are concerned by separate statutes.

## **4. Principles of Construction of a Virtual World Legal Framework**

Rules can form different normative systems. Virtual world rules have different modes of effect or relevance, such as "barrier", "occasional", "step-by-step", etc. (see Fig. 7).

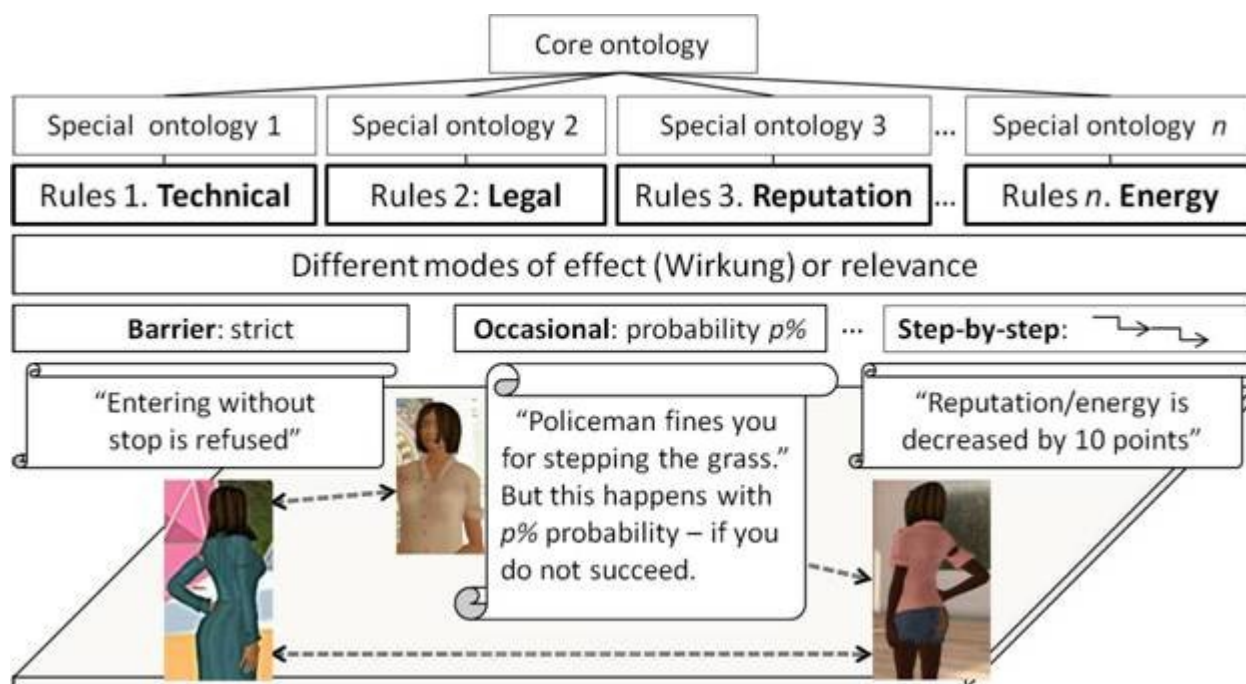


Fig. 7. Principles of construction of a virtual world legal framework.

**Barrier effect.** A door is an example of the barrier type technical rule. The technical rules are implemented with hard constraints. For implementation see Guideline 2. [13]

**Occasional effect.** The occasional type rule sanctions you with a certain probability. An example is a legal rule to buy the ticket when you take a train. However, you can succeed to travel without the ticket, but if a conductor does not sanction you.

A dream of programmers (knowledge engineers) might be to implement sanctions by means of the technical rules. However this is against the spirit of law; see also (Leith 2010).

**Step-by-step effect.** It is characteristic to reputation and energy rules. For example, each time you violate a rule, your points are decreased by 10%.

**Ontologies.** A core ontology is immanent within the whole set of rules. A special (material) *domain ontology*; is present within each kind of *rules*.

**Technical filters.** They can be set to enforce rules. For instance, in the context of e-law, the text of legal documents can go through an XML filter. A document cannot be put on the "transport belt" of legislative workflow in case the document's XML structure is flawed, e.g. marked-up with errors. Such a filter is an example of a technical rule. The ruling is of the type "Entering without stop is refused."

**Terminology of the technical rules.** The latter are treated as factual ones. They establish factual hindrances. For instance, a closed door is a hindrance to enter the room; a request from the cash machine for the PIN number is a hindrance to take money by unauthorized persons.

These "natural" rules have to be distinguished from natural laws such as gravitation - a physical law. Recall that the essence of a human being is examined when the behaviour is

regarded in natural law. Thus the factual rules can be divided into two classes - technical rules and natural rules (see Fig. 8).

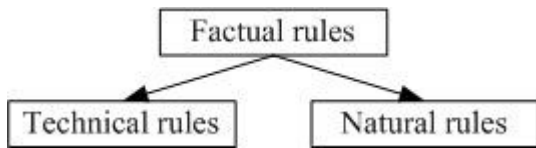


Fig. 8: A classification of factual rules comprises physical laws such as gravitation.

## 4.1 Three Legal Stages

Three legal stages can be distinguished within a virtual world: (1) the legislative stage, (2) the negotiation stage - the stage of the game, and (3) the judicial stage. This metaphor is depicted in Fig. 9. The functions of the stages accord with the functions of law which are distinguished in legal theory.

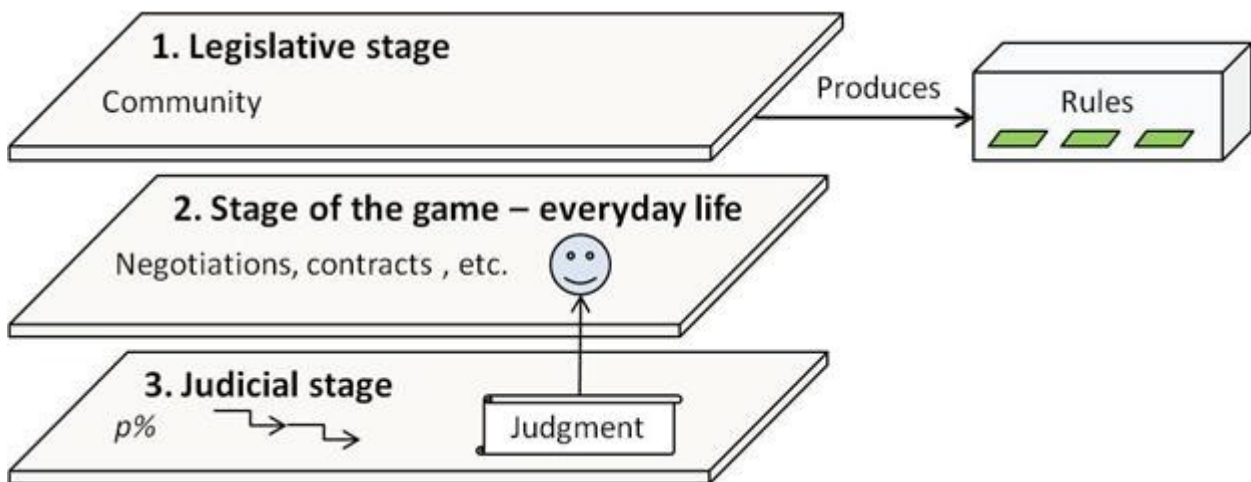


Fig. 9: Three legal stages of a virtual world.

The legislative stage serves to produce rules. Here the whole in-world community can be involved. Next, the negotiation stage serves for everyday life. Social games including contracts are performed here. The judicial stage serves for judgments. This stage is not entered in each case. Distinguished modes of (virtual) legal proceedings are already identified above. Here activities such as story-telling, adjudication dialogs and legal disputes can be invoked.

The legislative stage consists of two sub-stages. On the first one, 1a in Fig. 10, legislative (general) rules are produced. It is compared with parliamentary activities, but performed by the community. On the second sub-stage, 1b, contract (individual) rules are produced.



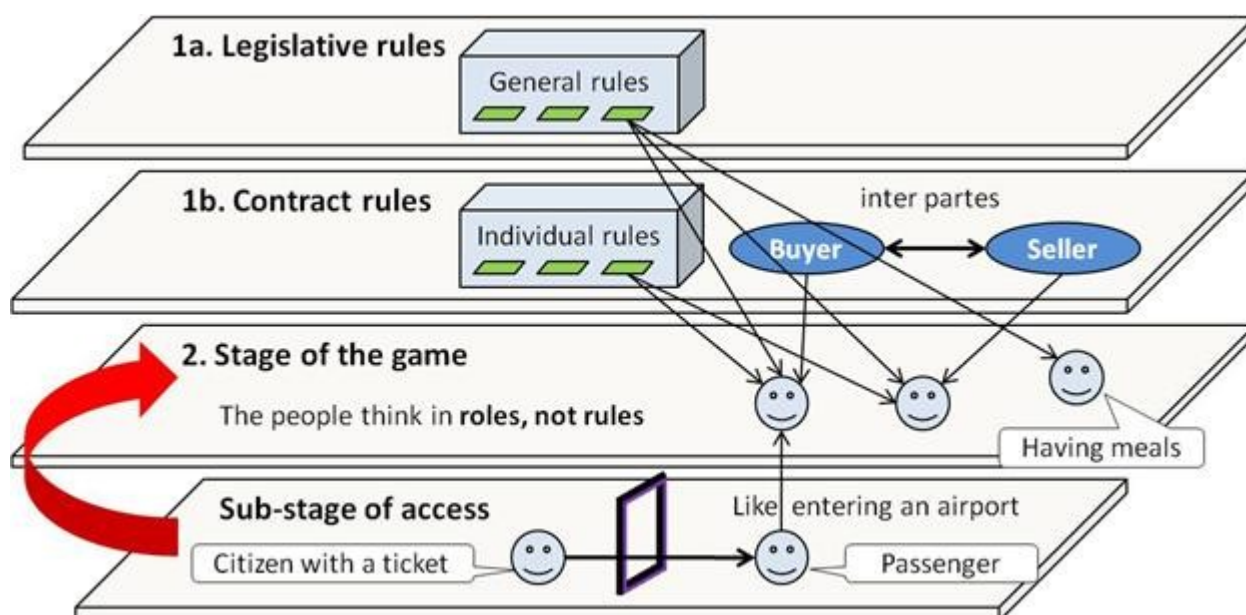


Fig. 10: Two legislative sub-stages serve to produce general rules and individual rules.

## 4.2 Formalising Rules

The concept of technical rule is formalised in terms of necessity (a causal relationship). A legal rule is formalised as a formula in deontic logic; see among others (Lachmayer 1977) and (Jones et al. 1992). Energy rule prohibits certain behaviour; if violated, addressee's "energy points" are decreased.

A sketch, a kind of symbolisation, is below. Formalising normative systems, modelling legal argument and operational implementation of rules attracted a broad research of other authors; see e.g. (Prakken 1997) and (Sartor 2007).

### 4.2.1 Technical Rules

Technical rules are based on natural necessity. They are formalised "If  $P$ , then  $Q$ ". In inference they can be employed with the *modus ponens* rule:

If  $P$ , then  $Q$ .

$P$ .

Therefore  $Q$ .

In the sequent notation,  $P \rightarrow Q, P \vdash Q$ . An example is the cash machine's rule that is worded:

**'if** PIN code is provided **then** the cash machine gives money'

Formally: *Rule* ( $pin \rightarrow money$ ).

The idea of the rule is the entailment that in the case the PIN code is not provided, the

cash machine gives no money:

*Rule* ( $\text{pin} \rightarrow \text{money}$ ), *Fact*( $\neg \text{pin}$ )  $\vdash$  *Fact*( $\neg \text{money}$ )

It can be discussed whether the notation of technical rules is "if and only if" (denoted iff or  $\leftrightarrow$ ), for instance:

**if** pin is provided **then** cash machine gives money, *and*

**if** pin is *not* provided **then** cash machine *does not* give money'

Formally: *Rule* ( $\text{pin} \leftrightarrow \text{money}$ ).

It should be noted that the technical rules do not have the structural element *modus*. Therefore 'ought' (obligatory) or 'may' (permitted) is not included in the grammatical formulation.

The technical rule concept can be compared with rules in rule-based knowledge representation and also active rules in databases.

#### 4.2.2 Legal Rules

Deontic status (e.g. obligatory, permitted, prohibited) is a structural element of legal rules. The nature of the legal rules is that a prescribed behaviour, *Q*, can be violated. Following is an example of an observed situation:

*Obligation* ( $P \rightarrow Q$ ) - rule.

*Fact* (*P*) - fact.

---

*Fact* ( $\neg Q$ ) - observed fact of violation.

For example, the traffic lights rule permits you to cross if and only if the lights are green: 'Permitted to cross iff green'. However, you can cross against the lights:

*Permission* ( $P \leftrightarrow Q$ ) - green **iff** cross.

*Fact* ( $\neg P$ ) - red is on.

---

*Fact* (*Q*) - you cross the street.

The observed behaviour is interpreted that you are simply a bad guy; nobody can stop you crossing.

Rule violations are sanctioned randomly with certain probabilities.

### 4.2.3 Energy Rules

Energy (reputation, etc.) rules prohibit certain behaviour. Consider you violate a rule. Therefore, your energy points are reduced. Hence, you are sanctioned 100%. An example is as follows:

*Norm* ( $\neg A$ ) -  $A$  is prohibited.

*Fact* ( $A$ ) - you violate the rule.

---

Points of  $A$  are reduced, e.g.,  $A := 0.9 * A$ .

Everyday interpretation is that your energy points are reduced to  $A_1$ , then  $A_2$  and so on to  $A_n$ . At last the state  $\neg A$  is reached, which denotes no energy at all (see Fig. 11).

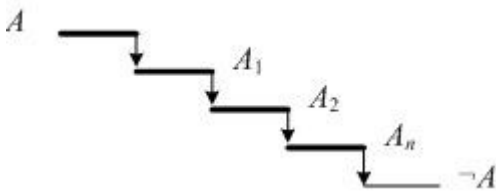


Fig. 11: Energy points are reduced upon the violations of a rule.

The shark illustrates an energy rule in the nature. If a shark swallows too much it drowns.

## 5. Related Work

**Multi-Agent Systems.** Relevant mathematical formalisations are investigated by JURIX, DEON and Normative Multi-Agent Systems communities. Their formalisms are mathematically more precise than our visualisations in this paper; see a whole Artificial Intelligence and Law vol. 16 (2008) no. 1 devoted to agents and AI & Law. Boella et al. (2010) concern violations of legal rules and address goal-based interpretation and conflicting goals. Dignum et al. (2002) seek a long-term goal to extend the Belief - Desire - Intention (BDI) model, at a theoretical and practical level, with social concepts such as norms and obligations.

**The obligation concept.** With regard to the analysis of obligations, we have found useful the thesis of Adam Wyner (2008). He considers deontic logic as presented by Paul McNamara (2006) and provides linguistic considerations and natural language syntactic and semantic analysis. Wyner's analysis of the Contrary-to-Duty Paradox (the Gentle Murder Paradox and the Good Samaritan Paradox) contributes to better understanding of obligations. The reader will understand the lexical semantics of obligations in case he finds mathematical axioms of deontic logic too heavy.

**Virtual Institutions.** Anton Bogdanovych (2007) work on non-game virtual worlds is very relevant. He developed the concept of Virtual Institutions (VI) "being a new class of Normative Virtual Worlds, that combine the strengths of 3D Virtual Worlds and Normative

Multiagent Systems, in particular, Electronic Institutions (Esteva 2003)". Virtual Institutions are targeted at e-commerce. In Virtual Institutions avatars are treated as agents. An avatar can stop for a while interacting with its human master and continue independently as an agent that is governed by rules. Following is an example a rule: "Only participants with certain roles are permitted to enter particular rooms". For instance, a Buyer is permitted to an Auction room but a Seller is prohibited.

Esteva (2003) sees Electronic Institutions as structures and mechanisms of social order and cooperation governing the behaviour of two or more individuals.

The ancient city of Uruk project (Bogdanovych et al. 2009) is interesting for the following reasons. Its specification is rather simple and consists of a dozen abstract norms.

Virtual Institutions are defined as "3D virtual worlds with normative regulation of interactions" (Bogdanovych 2007, p.69). A virtual institution is enabled by a three layered architecture. The Normative Control Layer employs AMELI to regulate the interactions between participants by enforcing the institutional rules. The Communication Layer causally connects the institution dimensions with the virtual world. The Visual Interaction Layer (supported by Second Life) visualises the virtual world. Electronic Institutions technology brings the set of tools for formal specification of the institutional rules, formal verification of those and a system that controls the enforcement of these rules (Bogdanovych et al. 2009).

**The rule of law and communities of programs.** Virtual law accords with the concept of a community of programs proposed by Lyubimskii (2009). He came to the conclusion that programs should interact similarly to humans: "the structure of the community of programs and the means of their interaction are largely similar to the structure and means of interaction in human society." Hence similar laws should rule the interaction of programs. Though the conclusion sounds simply, it took years of research and practice for Lyubimskii to come to it. The conclusion is also proved by both the history of computing and by current research on normative agents. The start was programming. Then came program synthesis (manual and automatic) - compiler development and programming automation. Here the rules of composing programs in order to synthesise new ones can be treated as the law of programs. Further continuation was implementation of communicating processes while developing operating systems. This field requires mechanisms which serve as "policemen", "judges" and "notaries" for programs that compete for common resources. Machine intelligence came next. The need emerged from raising the level of intelligence of software packages. GRID computing was a next step. It requires more elaborated policies to govern program interaction. Lyubimskii treated GRID activities as a step to the creation of worldwide artificial mind.

**Computer code is law.** The role of computer code in cyberspace can be compared with laws in real space. [14] In particular, MMOGs (massively multiple online games) are also "determined by the code - the software, or architecture, that makes the MMOG space what it is" (Lessig 2006, p. 14). Therefore the issues of the conception "code is law" are important for our research. Software engineers have to regard limits of programming and regulation by code. Jurists have to regard limits of territorially based sovereigns.

## 6. Conclusions

Virtual worlds are part of the real world. However legal and security virtual features need to be improved in order to guarantee safe and reliable virtual infrastructure. The paper reflects on this need and elaborates on possible solutions, including a legal framework.

The paper views a virtual world as whole. Therefore the stage metaphor is used. In the "From rules in law to rules in artefact" approach, we elaborate on an issue of regulation by computer code. The artefacts can be of different kinds. Additionally to embedded systems, the artefacts comprise software systems like virtual world platforms and virtual nations. The approach builds a bridge between law and informatics.

We aim to build a bridge between an Ought-to-Be reality and Is reality in the domain of virtual worlds. Here software developers identify the rules and implement them in computer code. A part of rules can be explicitly represented - the 'strong' interpretation (Boella et al. 2007). A part of rules cannot be represented explicitly. They are formulated explicitly in the system specification, namely, in the EULA text - the 'weak' interpretation.

Modelling virtual worlds and implementing rules is a challenging task; not only for software developers. Therefore, the people think in roles, not rules. The names of roles, such as an author, an owner, a NoCopy nation, serve to describe situations. Therefore the metaphor of a stage is used. Formalisations and operational implementation require further research.

Law enforcement in virtual worlds remains a tough problem. Virtual worlds are just extensions of the real world. Legal rules are unfeasible to be programmed in the full extent in virtual world software.

We claim that the rule of law is required for both human and artificial agent communities. Different persons can pursue conflicting interests. Therefore the need arises for governance by rules. Similar behaviour is also observed in artificial agent communities. For example, concurrent computer programs compete for common resources. Operating systems perform the roles of "arbiters" in such a community of programs. Similarly, the behaviour of agents (avatars) in virtual worlds has to be regulated by rules that constitute the law of the virtual world.

**Acknowledgments.** The work was stipulated by the whole VirtualLife consortium. Maria Vittoria Crispino and Francesco Zuliani have coined the project and currently are pushing it to the targets.

## References

Bench-Capon T (2002) "The Missing Link Revisited: the Role of Teleology in Representing Legal Argument", *Artificial Intelligence and Law*, 10(1-3):79-94.

Bogdanov D, Crispino MV, Čyras V, Glass K, Lapin K, Panebarco M, Todesco GM and Zuliani F (2009) "VirtualLife Virtual World Platform: Peer-to-Peer, Security and Rule of Law", in *eBook Proceedings of 2009 NEM Summit Towards Future Media Internet*, Saint-Malo, France, 28-30 September, pp. 124-129, Eurescom GmbH.



- Bogdanov D, Livenson I (2009) "Virtuallife: Security Management in Peer-to-Peer systems", in Daras P and Mayora O (eds.), Proceedings of the First International Conference on User-Centric Media, UCMedia 2009, Venice, 9-11 December 2009. LNICST, vol. 40, pp. 181-188. Springer, Heidelberg.
- Bogdanovych A (2007) Virtual Institutions. PhD thesis, University of Technology Sydney, <http://utsescholarship.lib.uts.edu.au/iresearch/scholarly-works/handle/2100/536?show=full> .
- Bogdanovych A, Rodriguez JA, Simoff S, Cohen A and Sierra C (2009) "Developing Virtual Heritage Applications as Normative Multiagent Systems", in Proceedings of the Tenth International Workshop on Agent Oriented Software Engineering (AOSE 2009) at the Eight International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS 2009), Budapest, Hungary, 10-15 May 2009, pp. 121-132.
- Boella G, Governatori G, Rotolo A and van der Torre LA (2010) "Formal Study on Legal Compliance and Interpretation", in Proceedings of the 13th International Workshop on Non-Monotonic Reasoning, NMR 2010, 14-16 May, Toronto.
- Boella G, Pigozzi G and van der Torre L (2009) "Five Guidelines for Normative Multiagent Systems", in Governatori G (ed) Frontiers in Artificial Intelligence and Applications, Vol. 205, Proceeding of the 2009 conference on Legal Knowledge and Information Systems, JURIX 2009, pp. 21-30, IOS Press, Amsterdam.
- Čyras V, Glass K and Zuliani F (2010) "Transforming Legal Rules into Virtual World Rules: A Case Study in the VirtualLife Platform", in Schweighofer E, Geist A and Staufer I (eds.) Globale Sicherheit und proaktiver Staat - Die Rolle der Rechtsinformatik. Tagungsband des 13. Internationalen Rechtsinformatik Symposions IRIS 2010, 25.-27. Februar 2010, Universität Salzburg, pp. 579-586. Österreichische Computer Gesellschaft.
- Čyras V and Lapin K (2010) "Learning Support and Legally Ruled Collaboration in the VirtualLife Virtual World Platform", in Grundspenkis J, Kirikova M, Manolopoulos Y and Novickis L (eds.) ADBIS 2009 Workshops, Proceedings of Associated Workshops and Doctoral Consortium of the 13th East-European Conference, Riga, Latvia, September 7-10, 2009. LNCS, vol. 5968, pp. 47-54. Springer, Heidelberg.
- de Freitas S (2008) "Serious Virtual Worlds: a scoping study". The Serious Games Institute, Coventry University Enterprises, JISC, <http://www.jisc.ac.uk/media/documents/publications/seriousvirtualworldsv1.pdf> .
- Dignum F, Kinny D and Sonenberg L (2002) "From Desires, Obligations and Norms to Goals". Cognitive Science Quarterly, **2**(3-4), 407-430.
- Jones AJI and Sergot M (1992) "Deontic Logic in the Representation of Law: Towards a Methodology". Artificial Intelligence and Law, **1**, 45-64.
- Eppler MJ and Burkhard RA (2006) "Knowledge Visualization", in Schwartz DG (ed) Encyclopedia of Knowledge Management. Idea Group Reference, Hershey, pp. 551-560.
- Esteva M (2003) Electronic Institutions: From Specification to Development. PhD thesis, Institut d'Investigació en Intelligència Artificial (IIIA), Spain.
- Housley R, Polk W, Ford, W and Solo D (2002) Internet X. 509 public key infrastructure

certificate and certificate revocation list (CRL) profile. RFC 3280.

Koster RA (2006) "Declaring the Rights of Players", in Bulkin JM. (ed) *State of Play: Law, Games, and Virtual Worlds*. New York: NYU Press, pp. 55-67, <http://site.ebrary.com/lib/viluniv/Doc?id=10176208&ppg=64>. See also <http://www.raphkoster.com/gaming/playerrights.shtml>.

Lachmayer F (1977) *Grundzüge einer Normentheorie: Zur Struktur der Normen dargestellt am Beispiel des Rechtes*. Schriften zur Rechtstheorie, H. 62, Duncker und Humblot, Berlin.

Leith P (2010) "The rise and fall of the legal expert system", in *European Journal of Law and Technology*, Vol. 1, Issue 1.

Lessig L (2006) *Code Version 2.0*. Basic Books, New York.

Lyubimskii EZ (2009) On the path to building a community of programs. *Programming and Computer Software*, Springer, 35(1): 2-5, 2009 [translated from *Programmirovanie* (in Russian)]. See also [http://www.gridclub.ru/library/publication.2005-11-23.7283041869/publ\\_file/](http://www.gridclub.ru/library/publication.2005-11-23.7283041869/publ_file/).

McNamara P (2006) "Deontic logic", in Gabbay D and Woods J (eds.), *Handbook of the History of Logic*, Vol. 7, pp. 197-288. Elsevier.

Pattaro E (2007) *The Law and the Right: A Reappraisal of the Reality that Ought to Be. A Treatise of Legal Philosophy and General Jurisprudence*, vol. 1. Springer, Heidelberg.

Prakken H (1997) *Logical Tools for Modelling Legal Argument: A Study of Defeasible Reasoning in Law*. Kluwer, Dordrecht.

Spindler G, Anton K and Wehage J (2010) "Overview of the Legal Issues in Virtual Worlds", in Daras P and Mayora O (eds.), *Proceedings of the First International Conference on User-Centric Media, UCMedia 2009, Venice, 9-11 December 2009*. LNICST, vol. 40, pp. 189-198. Springer, Heidelberg.

Spindler G, Prill A, Schwanz J and Wille S (2008) *Preliminary Report of the Legal Fundamentals Concerning Virtual Worlds*. VirtualLife deliverable D7.1.

[Vázquez-Salceda J, Aldewereld H, Grossi D and Dignum F (2008) "From Human Regulations to Regulated Software Agents' Behavior. Connecting the Abstract Declarative Norms with the Concrete Operational Implementation". *Artificial Intelligence and Law*, **16**(1), 73-87.

[Wyner A (2008) *Violations and Fulfillments in the Formal Representation of Contracts*. PhD thesis, King's College London. <http://www.wyner.info/research/Papers/WynerPhDThesis2008.pdf>.

---

[1] Vilnius University

[2] University of Innsbruck

[3] <http://www.ict-virtuallife.eu>.

[4] Non-game virtual worlds such as Second Life, developed by Linden Lab, <http://secondlife.com/>, are in the primary focus.

[5] VirtualLife project "Secure, Trusted and Legally Ruled Collaboration Environment in Virtual Life", 2008-2010, co-funded by EU FP7 ICT under DG INFSO Networked Media Systems, <http://www.ict-virtuallife.eu>.

[6] Eppler and Burkhard (2006, p. 553) emphasise the role of visual cognition and perception and note that a majority of our brain's activity deals with processing and analysing visual images: "If visualization is applied correctly, it dramatically increases our ability to think and communicate".

[7] Annuk S, Bogdanov D, Glass K, Jaeger J, Jagomägis R, Livenson I, Ristioja J, Todesco GM (2010) P2P Infrastructure Specification and Validation Plan. VirtualLife deliverable D12.1.

[8] This subsection is based on Bogdanov D, Laud P (2010) Secure Communication Prototype, VirtualLife deliverable D3.3.

[9] Network Address Translation, a technique for mapping an IP network into another one.

[10] The descriptions and designs in the virtual reality engine of VirtualLife software are mainly by Kevin Glass.

[11] Cordier G and Zuliani F (2009) Virtual Nation Laws - Technical Specifications. VirtualLife deliverable D7.3.

[12] "That avatars are the manifestation of actual people in an online medium, and that their utterances, actions, thoughts, and emotions should be considered to be valid as the utterances, actions, thoughts, and emotions of people in any other forum, venue, location or space." (Koster 2006, p. 57).

[13] "Make explicit why your norms are a kind of (soft) constraints that deserve special analysis" (Boella et al. 2009)

[14] "In real space, we recognize how laws regulate - through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different "code" regulates - how the software and hardware (i.e., the "code" of cyberspace) that make cyberspace what it is also regulate cyberspace as it is." (Lessig 2006, p. 5)