

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

# Legal problems of commercial transactions in cyberspace: an overview

Georgios I Zekos<sup>1</sup>

## 1. Introduction

The Internet began, as ARPANET, in 1969 at the Advanced Research Project Agency. It was developed as a way to connect the military, defense contractors, and educational institutions conducting defense research. The network spread from government agencies and universities to corporations and individually as other networks formed and connected to ARPANET<sup>2</sup>.

State law is based on borders and jurisdiction. Legal rights and responsibilities are therefore dependent on where one is located in space<sup>3</sup>. State law determines court jurisdiction within constitutional boundaries<sup>4</sup>. Hence, at present, law is in general territorial, extending no farther than the borders of the jurisdiction whose government has enacted the law.

What we call 'cyberspace' can be characterized as a multitude of individual, but interconnected, electronic communications networks. The Internet is not a physical object with a tangible existence, but is itself a set of network protocols that has been adopted by a large number of individual networks allowing the transfer of information among them. Moreover, the Internet is a medium through which a user in real space in one jurisdiction communicates with a user in real space in another jurisdiction. The world of cyberspace has no physical existence beyond the computers on which it resides but this fact does not keep it from being real because it is a world of information that have real consequences and a real existence. It is the interplay between the vast number of largely centralized individual networks and the decentralized Internet work through which they can communicate that will prove to

---

<sup>1</sup> BSc(Econ), LLB, LLM, PhD, <http://www.diaulos.com/zekos>, Department of International Economics, Democritus University of Thrace, Attorney at law, Amvrosia-Komotini, Greece. This paper is a further development of a presentation in the international conference Eurolog2000 organized by the ELA and ILME and took place on 14-16 May 2000 in Athens. <http://www.ilme.gr>

<sup>2</sup> *ACLU v Reno* 929 Fsup 824

<sup>3</sup> D. JOHNSON, D. POST, *Law and Borders-The role of law in cyberspace*, 48 Stan L R 1367.

<sup>4</sup> L. LESSIG, *Reading the Constitution in Cyberspace*, 45 Emory LJ 869. American Civil Liberties Union <http://www.aclu.org/issues/cyber/burning.html>, L. LESSIG, *What things regulate speech* <http://www/si.umich.edu/prie/tprc/abstracts97/lessig.pdf>

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

be a fundamental importance in determining the efficacy with which state law can be imposed on individual network communities. Hence, the key feature of the Internet is that the net is set up to operate logically rather than geographically.

Has the Internet a controlling body? The Internet has no controlling body and thus, at first sight, the Internet is designed without a centralized control mechanism. It exists only by virtue of the numerous computers and networks that are linked to it. The Internet has no real central management or ownership, but somebody enters the information on the net and so there is a control of the provided information. A common language was developed which allowed different operating systems, such as windows, Macintosh and Unix, to speak to each other. Networks are capable of promulgating substantive rules of conduct, namely the 'network protocols'. A domain name is a significant part of an Internet address that determines where data packets are to be sent<sup>5</sup>. Domain names do not effectively reside in a physical location and the efficacy of the domain system requires expansion beyond territorial boundaries and in to globally integrated laws. An effective domain name system will function properly from both a technological and management standpoint. The entity in a position to dictate the content of these network protocols is a primary "rule-maker" in regard to behavior on the network. Each network has its own message origination and routing rules. Hence, communication networks are defined at a minimum by a set of rules specifying the medium through which messages can travel and the characteristics of the messages, which are permitted to enter the network. The fundamental question is how to devise appropriate rules of law to be applied by the courts to a commercial issue where the essential facts are spread over more than one sovereign state.

The state's ability to impose sanctions on law-violators is contrasted by the need for physical proximity and control. Besides, individual sovereigns can impose their rules on entities or persons not physically present in the area over which the sovereign has control. Such mechanisms entail additional enforcement costs, both in terms of the direct costs of coordinating and harmonizing the legal regimes of competing sovereigns and costs of projecting sovereign power extra-territorially<sup>6</sup>. Cyberspace undermines the relationship between legally significant phenomenon and physical location. The power to control activity in cyberspace has the most slender connections to physical location.

---

<sup>5</sup> A. JOHNSON-LAIRD, *The Internet: the good, the bad and the ugly*, <http://www.jli.com>, IANA <http://iana.org/aboutiana.html>, Network Solutions <<http://rs.internic.net/domain-info/domflow2.html>>

<sup>6</sup> L. LESSIG, *The zones of cyberspace*, 48 Stan.LR 1403.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

The technology is so exhilarating that there is a tendency to claim that the changes we observe in sovereignty, the state, jurisdiction and law are caused by cyberspace<sup>7</sup>. The growth in the use of the Internet has been one of the most interesting technological and political developments of the late twentieth century. International relations are influenced by internal political phenomena, and the interaction of non-state actors across borders. Events on the Internet occur everywhere but nowhere in particular. What law should we apply to protect the transactional data? Has the legal world established a jurisprudence of cyberspace? Has the law met electronic technology with a coherent doctrine that takes into account the transnational dimensions of global computer networks?

The choice of law is one of the most important contractual elements to be agreed upon between the parties. The parties' choice of law has certain limits. Thus, a party who makes a choice of law so as to circumvent the applicability of an undesired law will not deserve protection. Have the contracting parties made a choice of law in their agreement? The rules or principles on the basis of which the judge may decide a dispute come under different categories: first law chosen by the parties; second rules of law chosen by the parties; and third decision *ex aequo et bono/ as amiable compositeurs / according to equity*. There is a need to realize the difference between the terms 'the law' and 'rules of law'. The term 'the law' refers to one particular national law as being the law governing a contractual relationship. Besides, the term "rules of law" may not mean a particular national law but also general principles of law, *lex mercatoria*, any transnational concepts of law and principles and notions reflected in international conventions. Have the parties made an implied positive or negative choice of law? Is there a hypothetical will of the parties?

## 2. *E-commerce.*

Electronic commerce is an application of Internet technology. The use of the Internet has turned into something easy and difficult, successful in some areas while resistant to change in others. Much commercialisation bends frontier technology to the needs of commercial users, a process that often involves many non-technical issues. The growth of electronic commerce has unleashed media hype about new ways of doing business in the information age. It has also raised the fees of consultants who devise strategies for exploiting new commercial opportunities<sup>8</sup>.

What is the typical empirical pattern by which commercial firms translate Internet technology into private value and, more broadly, into sustained economic growth?

---

<sup>7</sup> G. ZEKOS, *Internet or Electronic Technology: A Threat to state sovereignty*, JILT <http://www.law.warwick.ac.uk/jilt/99-3/zekos.html> D. ROWLAND, *Cyberspace - A Contemporary Utopia*, <http://www.law.warwick.ac.uk/jilt/98-3/rowland.html>

<sup>8</sup> M. LEMLEY, *Legal implications of network Economic effects*, 86 Cal LR 479.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

Doing business electronically over the cyberspace increased exposure to unfair market practises, insecure means of payment, loss of privacy and lack of enforceable remedies. E-commerce is defined as any actions undertaken by business, which requires a commercial transaction to be carried out over a network such as the Internet. E-commerce offers benefits to both seller and buyer. The seller can create a global presence and therefore reducing costs, increasing competition and allowing the ability to customise products. E-commerce has the ability to eliminate the time span between ordering, delivery, invoicing and payment by using the World Wide Web. E-commerce is global and its benefit would not be fully realised if it were not available worldwide. It is the basic consensus of the parties involved that e-commerce should be industry-led and governments should support industry by establishing the appropriate environment. It is difficult to regulate e-commerce for two reasons: Firstly, the scope of e-commerce and technology involved changes rapidly. Besides, the formulation of the law has been an evolutionary process, adapting to suit the needs of society. Secondly, the very nature of the technology involved means that it is transnational and so leads to problems as to which legal system has jurisdiction over e-commerce transactions. Digital communications media challenge our established notions of boundary. Computers replicate digitised content as they perform operations on it. Such replication is necessary to the functioning of the system and the copies are made automatically by the computers when executing routine operations. Because the Internet spans national borders, on line activity creates a variety of jurisdictional and choice of law problems. Hence, jurisdictional factors pose an additional cost to online transactions. E-commerce shrinks the world of business and consumers can go directly to producers without the need for traditional retailers and distributors in the case of intangibles. It succeeds in moving economic activity closer to some of the ideals of perfect competition: low transaction costs, low barriers of entry and improved access to information for the consumer. By contrast lack of trust, uncertainty about the regulatory environment, gaining access and logistical problems hinder its growth. Self-regulatory approaches might be necessary to be put within a legal framework to ensure enforcement and implementation. Users need access to network infrastructure and regulatory structures provide the market framework and incentives or disincentives to expand infrastructure capacity. Developing new kinds of commercial activities in the electronic environment depends on assuring consumers and business that their use of network services is secure and reliable. Hence, policies to promote electronic commerce must be directed firmly towards developing and implementing trustworthy technology and policies and secondly developing law enforcement mechanisms to respond to users who seek to misuse the technologies. While electronic transactions should be secure and reliable, they will involve a calculated risk and will be accepted when their value is greater than the perceived risks. In the rapidly changing world of information technology, governments and private sector

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

should play an increasingly important role. States should implement technology-neutral policies, so, as not to reduce e-commerce or create regulations that will hinder on line transacting. The lack of physical clues that permit identification and the ability to make perfect copies and undetectable alterations of digitized data complicate the use of cyberspace. The development of a consensus among government, companies and citizens is necessary in order to guide the formation and implementation of e-commerce. Enforcement of intellectual property rights has become important and international protection agreements have set up various forms of minimum standards<sup>9</sup>.

Globalization of markets involves the growing interdependency among the economies of the world. Development of new technology and the proliferation of new products<sup>10</sup> contribute to the globalization of markets. Whereas only a few multinational companies dominated international trade a couple of decades ago, today companies from all parts of the world are participating in worldwide business. There are fundamental shifts in international transactions, which are summarized to the followings: a shift from nation state to individual enterprise, a change from nation-based advantages to firm based competencies and assets, a switch from competition to cooperation and a market diversity to market homogenization, and finally a transference from multilateral to bilateral trade relationships. Multinational operations necessitate production, sourcing and marketing activities in multiple markets. International organizations have made great progress in developing rules and guidelines relating to the matters in their jurisdictions. We should not duplicate the discussions of each international organization and we should identify first what is not being discussed elsewhere and also address selected matters in greater detail.

Cyberspace can alter the critical determinants of the competitive conditions of a market. The first is the cost of developing a product and then entering a particular sector by becoming a producer. The second is the cost of becoming known or gaining access to buyers, being able to tap into large pools of potential consumers. Cyberspace has the capacity to encourage: unique products, direct consumer-producer linkages, flexible working arrangements, and to easy entry to competitors from all over the world into equally dispersed market. Patterns of work might move away from fixed locations, offices and factories. At the moment it is uncertain if cyberspace will become a new frontier, a space for the democratic realization of human aspirations, or simply another infrastructure that makes existing societies more efficient. Extra-territorial application of state law has the potential to seriously undermine the utility of e-commerce. Companies planning to use cyberspace should

---

<sup>9</sup> C. BEACH, *Taxing the Internet* <http://www.slate.com/Gist/97-03-29/gist.asp>, A. HARTNICK, *Copyright & Trademark on the Internet*, <http://www.ljx.com/internet/02cptmint.html>

<sup>10</sup> K. HALVEY, *The virtual marketplace*, 45 Emory LJ 959, M. RUSTAD, *The commercial law of Internet security*, 10 High Tech LJ 213.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

take meaningful steps, and make continuing efforts, to control the scope of its interactions with other forums. Use of the cyberspace for delivery of goods and services and the retail sales of tangible items is on the rise, and if the current trend continues then information technology can be expected to drive economic growth for many years to come. Advance in information and communications technologies have improved the ease with which products or art forms can be created, reproduced, and disseminated. Universal access to knowledge is the greatest benefit of the digital economy. Cost savings and improved customer convenience are stimulating an expansion of the cyberspace retail sector. Besides, matters such as proprietary rights, access, accuracy, privacy, confidentiality, responsibility and equity pose challenges to the future scope and direction of the digital era. The electronic marketplace must be competitive and transparency refers to the ability of the consumer to understand fully the value of the good or service prior to purchase. The ease with which digital property can be located, accessed, copied, and distributed is without precedent. Computers can archive, compare, manipulate and distribute data with astonishing facility. The field of technological protection for digital property is developing rapidly, but at the moment the most common approaches include server and file controls, encryption, complementary keys, and digital signatures. Digital signatures allow the receiver of a communication to authenticate the source and to verify that the original contents of the file have not been alerted. The digital signature is functionally similar to an encryption program, except that it verifies the sender rather than selecting the identity of the receiver. According to ABA report, digital signatures offer some advantages. First, they minimize the risk of dealing with imposters, the risk of undetected message tampering and forgery. Second they are more secure than handwritten signatures, with the threat of forgery virtually negligible. It could be argued that the simplicity of the handwritten signature together with the ease of discovering its forgery makes its use more advantageous for the ordinary consumers, rather than the complex and technical digital signature as it is offered at present time. E-commerce would not develop without the regulatory liberalization of the communications network environment. Competition has opened new opportunities for new economic actors. The plethora of new types of business ventures attempting to take advantage of the opportunities created by the digital revolution has put pressure on pre-existing monitoring and regulatory authorities whose primary task it is to protect the consumers/citizens interests<sup>11</sup>.

---

<sup>11</sup> UNGERER, *Ensuring efficient access to bottleneck network facilities* <http://europa.eu.int/en/comm/dg04/dg4home.htm>, BRONCKERS, *Telecommunicatings services and the WTO*, 31 JWTL 5, E. Commission <http://www.ispo.cec.be/convergencegp/wienno98.html> Commission Notice on access agreement in the telecommunications sector 98/C265/02 OJ 1998, C265.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in Ciberspazio e Diritto, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

### 3. *Personal jurisdiction under traditional rules and cyberspace transactions.*

Jurisdiction concerns the power of the state to affect people, property and circumstances and reflects the basic principles of state sovereignty, equality of states and non-interference in domestic affairs.<sup>12</sup> Jurisdiction is a vital and central element of state sovereignty, for it is an exercise of authority, which can alter or create or terminate legal relationships and obligations. The preceding notion of jurisdiction is based on a physical reality that does not exist in cyberspace. It may be achieved by means of judicial action or by executive action. The grounds for the exercise of jurisdiction are not identical in the cases of international law and conflicts of law rules<sup>13</sup>. Actions in the virtual world of the Internet have legal ramifications in the real world. The duty of non-intervention within the domestic jurisdiction of states provides for the shielding of certain state activities from the regulation of international law. Besides, judicial jurisdiction concerns the power of the courts of a particular country to try cases in which a foreign factor is present. The powers of the state that we refer to as 'sovereignty' has never been static. States do not control interactions among individual users of the Internet<sup>14</sup>. The development of cyberspace gives rise to new means of expression and allocation of power both to the state and to non-state entities. International law is the vehicle for revision of these allocations of power. The rise of economic interdependence and other technological changes must be considered alongside cyberspace.

Can all of cyberspace be free of state-bound law? Many recent initiatives in international regulation and in the trade world have started a co-operation among states to establish rules of prescriptive jurisdiction, harmonized laws, and international organizations to apply these rules. It is argued that cyberspace is not technically susceptible to regulation. Cyberspace either will raise the costs of regulation to the point where it is inefficient to regulate or the technological developments will enable cyberspace to provide its regulation. The allocation of jurisdiction to a particular state is not simply a technical issue and therefore it involves distribution or political choices. Thus, the development of cyberspace raises new problems of jurisdiction and creates consequently another understanding

---

<sup>12</sup> D. BOWETT, *Jurisdiction: Changing problems of authority over activities and resources*, 1982 BYIL p 1

<sup>13</sup> L. KRAMER, *Rethinking choice of law*, 90 Colum. L.Rev 277, D. POST, *Governing Cyberspace*, 43 Wayne St L Rev 155, Unsolicited E-mail: cases

<http://www.jmls.edu/cyber/cases/spam.html>, D. GOLDSTONE, *The Public forum doctrine in the age of the information superhighway*, 46 Hastings LJ 335.

<sup>14</sup> D. JOHNSON, *The new case law of cyberspace*, <http://www.eff.org/pub> N. MCCORMICK, *Beyond sovereign state*, 56 Mod LR 1. *United States v Montoya de Hernandez* 473 US 531, *The Chinese Channel Limited* <http://www.chinese-channel.co.uk/faq-e.htm> L. LESSIG, *The zones of cyberspace* 48 Stan. LR 1403, I. HARDY, *The proper legal regime for cyberspace*, 55 U Pitt LRev 993.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

jurisdictional problems. At the same time cyberspace provides intriguing new political solutions. Hence, the central and most difficult legal issue in cyberspace is jurisdictional. It is difficult to locate cyberspace conduct territorially because of the dispersed nature of the computer network that comprises the Internet. It could be said that since cyberspace cannot be combined in any single territory and assuming that territoriality is the single basis for jurisdiction, then no state could regulate cyberspace<sup>15</sup>. It could be argued that cyberspace creates global government. Internet regulation is a global problem and thus internal co-operation is necessary. Thus, states wishing to impose law on or in cyberspace will find that they do not have the physical control over the net necessary for lawmaking authority. The jurisdictional conundrums the Internet causes appear at the international level. Traditional international legal rules on jurisdiction (jurisdiction to prescribe, adjudicate and enforce) do not fit the Internet context. Furthermore, international legal rules on prescriptive jurisdiction are not very helpful in providing a way to resolve the potential clash of legal systems<sup>16</sup>. Hence, traditional international law on jurisdiction does not facilitate international co-operation on international regulation. Who will make and enforce the legal rules that will govern cyberspace? The Internet allows a relatively easy change of jurisdiction leading to the unprecedented situation of a market free of rules sets. Besides, governments are racing to establish a well-functioning virtual marketplace by imposing rules against legal infringements<sup>17</sup>. Since transactions can involve computers in many countries at once, it is difficult under current jurisdictional analysis to assign liability. It could be argued that a way to regulate the net is to allow Internet service providers to serve as enforcers and regulators by virtue of the market.

National treatment has not caused a significant problem for choice of law or territoriality principles because few nations are likely to be involved in a single enforcement action. The legality of the allegedly infringing actions must be judged by the laws of the country presented with the infringement claim. The nature of cyberspace makes it increasingly likely that users in many nations will have been involved in alleged infringements. For example, the ability of individual users to transfer information from one country to another without personally crossing any borders complicates the enforcement of intellectual property rights. The place of the wrong in cyberspace is a computer network rather than a discrete state. Cyberspace could be seen as an area with distinct legal boundaries. Hence, if a computer network were a discrete place then a system of international laws would have to be

---

<sup>15</sup> J. P. BARLOW, *Declaration of independence of cyberspace*, <http://www.eff.org/pub/publications/john-perry-barlow/barlow-0296.declaration>

<sup>16</sup> W. BYASSEE, *Jurisdiction in Cyberspace: Applying real world precedent to the virtual community*, 30 Wake Forest LR 197, T. BASS, *Obscenity in cyberspace*, 1996 U Chi Legal F 471.

<sup>17</sup> C. YANG, *Law creeps onto lawless net*, Bus. Week May 6, 1996 p 58.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in Ciberspazio e Diritto, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

promulgated to regulate and define it. Location-oriented choice of law approach is unable to identify a legal locus as the place of wrong.<sup>18</sup> The notion of the most significant relationship may be helpful in cyberspace cases, if a method can be established to identify which physical contacts comprise that significant relationship. The extension of physical world laws and government jurisdiction to cyberspace will prove ineffective because of the fast paced and unique nature of this global medium. The courts must address the question of which lawmaker has jurisdiction over actions taking place on cyberspace. Regulation must conform to cyberspace rather than cyberspace will conform to regulation. Does change in the medium necessarily mean that a new single system of law must be created to solve the problems on the Internet?

Cyberspace breaks down barriers between physical jurisdictions and has no territorially based boundaries. Substantive and procedural laws vary from jurisdiction to jurisdiction. The questions of what laws govern transactions over cyberspace and where the buyer and seller are subject to jurisdiction can be important. Notions of jurisdiction are based on a physical reality that does not exist in cyberspace. However, actions in the virtual world of cyberspace have legal ramifications in the tangible world. Personal jurisdiction arising from cyberspace contacts presents the most difficult application of traditional law, when business is being contacted via electronic means. Contract formation may require a meeting of minds, but it does not require an actual meeting of the parties involved. Personal jurisdiction is the right of a court to call a person before it to answer allegations made by another party. The plaintiff, by virtue of filing suit, chooses the jurisdiction in which it elects to have the dispute heard. Courts created the minimum contacts test that allows for jurisdiction over a nonresident when such contacts exist between the defendant and the forum state. A nation state's jurisdiction extends to people who reside within the country or to the transactions and events, which occur within the national borders of the nation. Does the global nature of cyberspace forms a separate legal area? Does cyberspace need a separate set of laws or current laws are adequate? A court must have jurisdiction over a person or a subject matter of the suit. For example, the US constitution permits the courts to exercise personal jurisdiction over persons who have sufficient minimum contacts with the state. Non-residents who are not physically present in the US can be sued in a US court as long as the person or entity has minimum contacts with the nation. New technology creates new situations which existing law cannot control. Any application of law to cyberspace must be examined in terms of the impact to the technology and the progress of cyberspace. Can jurisdiction be considered as an anachronism in a borderless world where time and distance have little meaning?

---

<sup>18</sup> J. COPPEL, *A hard look at the effects doctrine of jurisdiction in public international law*, 6 Leiden J Int'l L 73, T SCHILLER, *International jurisdiction in cyberspace*, 50 Fed Comm LJ 117.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

Change in the medium does not necessarily mean that a new single system of law must be created to solve the problems on the Internet. Cyberspace users may be unaware where the resource being accessed is in fact physically located. Jurisdiction over a person was premised on the physical presence of the individual in the forum, which continues to be a viable jurisdictional basis. The presence of cyberspace' users takes another form but it continues to be a presence in other words a virtual presence of the user of the network is created which means that this presence can be seen as a viable jurisdictional basis as well. Hence, jurisdiction would be proper when some effect of defendant's actions is felt within the forum state. Where jurisdiction from cyberspace contacts is at issue, physical presence of the defendant within the forum state will likely be the exception rather than the rule. Given the nature of cyberspace transactions, those contacts will be solely cyberspace-based contacts. The unique aspect of cyberspace commerce is that the net allows not only negotiation and payment on line, but also delivery of goods if the goods are digitized information products, music, data and the like. Cyberspace alters not only the physical aspects of traditional methods of communication, but also its interactive capability allows and encourages individuals to adopt new online identities. This feature result in the creation of multiple personalities (electronic personae) unconstrained by the geographical boundaries of a single, corporeal existence. Cyberspace has an undeniable power to create and deliver a powerful, albeit non-physical presence to anyone, anywhere, at any time.

The interactive website differs substantially from a passive website in that it can engage in communication with consumers who are situated in a specific geographic location, and can establish a pattern of geographically specific activity through its contacts with those persons. As mentioned above, Cyberspace is not a physical or tangible entity, but rather a giant network, which interconnects innumerable smaller groups of linked computer networks. Courts are continuing to struggle with the application of traditional jurisdictional principles to cyberspace transactions, because cyberspace issues turn the notion of territorial sovereignty on its head. An allowance of personal jurisdiction based solely on an Internet web site would produce global jurisdiction over all information providers on the www. Is a web site a sufficient enough contact with the forum state to establish personal jurisdiction in the forum state? The nature of the cyberspace is such that it is very difficult to determine its size at a given moment. Cyberspace exists and functions as result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decide to use common data transfer protocols to exchange communications and information with other computers. Moreover, there is no centralized control point and storage location for the cyberspace and it is not feasible for a single entity to control all of the information conveyed on the Internet. An Internet user traveling from site to site is exploring cyberspace with no geographical location of the other transacting party. Jurisdiction is the right of a court to decide

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

the fate of a certain person (personal jurisdiction) or certain matter (subject matter jurisdiction). Personal jurisdiction represents the geographical restriction on where a plaintiff may choose to sue a defendant for a certain claim. Some courts have taken the position that a new body of law needs to be developed to provide for the issues addressed in electronic transactions. Besides, cyberspace transactions can be compared to existing situations that take place in every day life. Cyberspace transactions seem to appear merely in a different form and so ordinary people are conducting the transactions and these people exist within territorial boundaries. Cyber activity is not above the law.

Electronic messages cross territorial borders and many online transactions have no necessary relationship to any particular physical location. The goal of cyber law is to protect users from arbitrary actions of their information service providers rather than form arbitrary actions of their governments. Have traditional legal authorities difficulty regulating a global electronic network? Who has authority to regulate cyberspace. A failure to protect online rights to liberty and property in the cyberspace would deter many potential participants and stifle online commerce. Rules online may be promulgated either by common practices developed by traders or as a result of private contract between user and provider. It could be argued that the most suitable form of contracts to be used in e-commerce is the contracts of adhesion<sup>19</sup> where there is a little or no opportunity for bargaining. Many contracts for Internet services provide that the user agrees in advance to abide by the rules of the specific system however arbitrary they might be or however often they may change in the future. As the number of users increase, the number of disputes and the magnitude of the interests affected by such disputes will increase. Local authorities cannot control a global net, may not have jurisdiction over all relevant parties. Those who control access to the interconnected systems have the power to discipline or deny interchange of messages to sites that fail to comply to come up with policies that govern the technical transmission of messages across the entire system. The technology of world wide electronic communication is developing so rapidly that it will be difficult to deal with many potential issues by means of such written rules. The protection of fairness for individual users in the cyberspace will rely less upon the law of territoriality based jurisdictions and more upon the actions of online societies. Hence, the efficacy of cyber law might depend more upon sysops who control on-off buttons and the reactions of their customers than they will upon theories relating to limits of state jurisdiction. The sysop can act as prosecutor, judge, jury and executioner.

An active web site is grounds for the exercise of personal jurisdiction when a defendant clearly does business over the Internet and so he makes a definite attempt

---

<sup>19</sup> People v Lipsitz 663 NYS2d 468.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

to entice people in the forum state to use defendant's web site.<sup>20</sup> Besides, a passive web site, which does little more than make information available to those who are interested, is not grounds for the exercise of personal jurisdiction because a defendant makes no attempt to entice people in the forum state to use defendant's web site. The court's exercise of jurisdiction is decided by studying the level of interactivity and the commercial nature of the exchange that occurs on the web site. Courts need to adopt a universal test. It could be argued that an additional contact test, further than the existence of a web site, should be established in order to exercise personal jurisdiction<sup>21</sup>. Hence, there needs to be additional contact in the forum state or business being contacted in the forum state. When a web site is published on the Internet, it is sent all over the world instantaneously and the site operator has no control over where the web site travels. Thus, courts run the risk of global jurisdiction and forum shopping, if they allow a web site, by itself, to create personal jurisdiction. Companies are unlike to use the Internet if they run the risk of submitting themselves to global jurisdiction and forum shopping. The territoriality principle would not allow extraterritorial application of national law. Under international law, countries can even incur international responsibility if they allow their territory to be used for unlawful activities directed against other states. The right of a country to regulate the conduct of its citizens or nationals anywhere in the world is like territorial jurisdiction, basically uncontroversial. The nationality principle is applicable to juristic as well as natural persons. The effects principle can be invoked when an act committed in one state causes injury in the territory of another state. It is not clear whether the downloading of files in a certain country makes the sender's activities subject to foreign jurisdiction. If customers have to subscribe to a provider's service and pay a fee then the publisher was aware that his material was entering specific jurisdictions, such as the US<sup>22</sup>. A court is at least entitled to prohibit access to the computer sites in the US. Hence, a country is not permitted to outlaw the activity completely unless it has jurisdiction based on territoriality, nationality or universality. Serious questions about the reasonableness of jurisdiction are raised if the sender is not aware of the recipient's country. It could be said that it is reasonable and justifiable that a state that is targeted in a specific way regulates this conduct, thereby subjecting individuals to its laws<sup>23</sup>. International law recognizes the right of a country to punish a limited class of offences committed outside its territory by persons who are not its nationals. In international criminal cases, jurisdiction to adjudicate depends almost exclusively in presence of the accused. In international

---

<sup>20</sup> *Cody v Ward* 954 Fsup 43, *IDS Life Co v Sunamerica* 958 Fsup 1258, *Bensusan Corp v King* 44 USPQ2d 1051.

<sup>21</sup> S. FLOWER, *When does Internet activity establish the minimum contact*, 62 Mo LR 845.

<sup>22</sup> *Playboy Enterprises Inc v Chacklebery Publishing Inc* 939 Fsup 1032.

<sup>23</sup> *Panavision LP v Toeppen* 938 FSUp 616, *Data Disk Inc v Systems Technology* 557 F2d 1280.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

civil cases the principle that plaintiff follows defendant to the latter's forum can be considered as a principle accepted virtually everywhere. There is a difference between the international law standard for civil cases (reasonableness) and for example the minimum contact standard required by the US law. Moreover, transitory presence<sup>24</sup> is not a sufficient basis for the exercise of jurisdiction to adjudicate under international law even though tag jurisdiction is in accordance with US law<sup>25</sup>.

Entrepreneurs demand self-regulation and the system providers can become the effective regulators of the net world. If system providers are not constrained by basic principles of fairness and respect for individual rights evolved within the context of cyberspace, then many potential participants would be deterred and avoid online commerce. Service providers (bankers, lawyers, securities dealers) can establish a virtual presence in all jurisdictions without physically entering any one jurisdiction. The establishment of a virtual magistrate is an answer for ruling on online disputes. The net by itself can facilitate thoughtful discussion of new rules, rational analysis of the facts, and expeditious adjudication of online controversies. The development of online due process rights will take the form of recognition that important personal and corporate interests such as trademarks and intellectual property are at stake. Those who control access to the interconnected systems have the power to discipline or deny interchange of messages to sides that fail to conform to a cyberspace norm. The Internet community has demonstrated its ability to come up with policies and protocols that govern the technical transmission of messages across the many networks and make the entire system work. It could be argued that the technology of global online communication is developing so rapidly that it will be difficult to deal with many potential issues by means of written rules. Due process in cyberspace may arise in the form of a general consensus among most users and sysops that ultimate enforcement tools available, banishment, cancellation of Ids, elimination of online addresses, ought not to be wielded arbitrarily.<sup>26</sup> Under US law due process is guaranteed by virtue of a written constitution, covering a particular geographically defined place and its citizens. The protection of fairness for individual users in cyberspace will rely upon the actions of online communities rather than upon the law of territorially based jurisdictions. Users can do business online without necessarily disclosing the details of their identity or the other roles they play in the real world. Hence, those who formulate the doctrine of online due process will need to decide whether such rights attach to any online <persona>. It could be argued that enforcement of rights online seems to be a solution rather than rights established online to be enforced on the real world. On the one hand corporations and other

---

<sup>24</sup> 18 ILM 8

<sup>25</sup> *Burnham v Superior Ct of Cal* 495 US 604.

<sup>26</sup> Gerber, *Constitutionalizing the Economy*, 42 AJCL 25, Humpe, *The implications of convergence for the markets and for the regulator*, <http://mars.coleurop.be/infosoc>.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in Ciberspazio e Diritto, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

organizations should be permitted to act as legal persons in order to protect their rights. On the other hand users maintain some protection against tyranny by virtue of their ability to move to another system. There is a need for actual understanding that due process in cyberspace will concern online personae rather than the citizens of a specific country. It will protect not only a different set of values such as the continuing life of an online identity, the liberty to engage in established activities free from arbitrary new rules and the property of an established domain name but also a differ in online environments on the basis of whether the local rules suit their needs. Can senders be liable under the laws of the receiver's location? Can the removal of liability from the sender for communications that do not violate the laws of the sender's jurisdiction, but do violate the laws of jurisdictions through which the communication passed or the laws of the receiver's jurisdiction be supported? The law of cyberspace will embody many principles that underline current due process doctrine: respect for the interests of individuals against the majority's oppression, rational evaluation of individual cases and opportunities to participate in creating and applying the law of cyberspace. Harm occurring in one geographically defined jurisdiction frequently results from conduct occurring in a different geographically defined jurisdiction.

#### 4. *Edi.*

EDI is the interchange of commercial data structured on the basis of approved standard messages between computer systems and affected by electronic means. Moreover, EDI facilitates international transactions irrespective of distance and time differences through the practically instantaneous transmission of data. Thus, EDI led the way in establishing the legal validity of transactions by developing trading partner agreements. The term electronic signature is used generally to cover any signature in electronic form, including digital signatures.

EDI is a form of electronic commerce concerned with the exchange of business documentation such as invoices and orders<sup>27</sup>. Companies have been cautious in adopting EDI due to high costs, limited consumer access to proprietary networks and the inability to automate only part of the transaction. EDI is a convenient and an efficient substitute for transmitting conventional paper documents between parties. The ABA's model<sup>28</sup> agreement is an attempt to create certainty with respect to the enforceability of EDI contracts between two contracting parties by creating a master agreement that the parties agree with control when legal issues arise due to EDI

---

<sup>27</sup> R. MCKEON, EDI:Uses and legal aspects in the comercial arena, 12 J Marshall J Computer&Info L 511.

<sup>28</sup> Aba, *Digital signature guidelines tutorial*, 1999 <http://www.abanet.org>.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

contracting.<sup>29</sup> Communications between computers are stored electronically. Although the data stored electronically can be printed at a later time, these EDI print outs do not have the immutability of paper-based writing. The reliability of EDI printouts may be questioned due to the fact that electronically stored data, unlike the paper counterparts, may be altered or deleted without a trace. Whether a printout of they electronically stored data will constitute an original for the best evidence rule purposes is uncertain. Electronically signed documents should be admissible to the same extent as other business records originated and maintained in a traditional written form. Often trade partners have a commercial relationship, which existed prior to their use of EDI to contract. Where an offer sent by letter specifies that the power of acceptance will be kept open for a certain amount of time, the mailbox rule mandates that the period be measured from the time the offer is received. An offer transmitted by EDI from A to B is not an effective offer until it is properly received by B. EDI is part of technologies for communicating business messages electronically including EDI, Fax, electronic mail, telex and computer conferencing systems (bulletin boards). The most popular public EDI standard in North America is ANSI ASC X12 and a popular public EDI standard outside North America is EDIFACT. Additionally, there are proprietary standards, which are EDI formats created for special purposes by particular groups of companies. EDI allows managers to be creative in the exchange of data between companies. Evaluated receipt settlement (ERS) and vendor managed inventory (VMI) are two EDI based systems which can be used by managers in order to simplify the business process. Among the factors determining importance are the value of the specific transactions in question, whether they form contracts and whether particular government regulations apply to them. It is common for each part of trading partners to enter a trading partner agreement (TPA) and the ABA model is a model but not a mandatory standard, which means that users may modify its terms as they deem appropriate. It is worth mentioning that judges have been permitting the admission of computer records into courtroom evidence for years. EDI systems need to be controlled to ensure that the records the system creates are accurate. A variety of controls might be installed to address this issue. Despite the widespread use of EDI in some sectors of the economy, such as manufacturing, many companies have not adopted EDI because of the effort and expense required to integrate EDI communication systems with existing computer operations. One of the appeals of Internet transactions is that the total cost of adopting electronic contracting practices may be lower than the cost of adopting EDI systems. The different electronic environment (closed-bilateral, closed bound community, closed-subscription, open-server security, open-client security, closed-robust local administration) in e-

---

<sup>29</sup> D. WILKERSON, *E-commerce under the UCC section 2: Are electronic messages enforceable?*, 41 Kan LR 403.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

commerce requires different authentication procedures. Whenever a party claims rights under a signed agreement, it is possible that the party seeking to avoid liability will deny the validity of the signature. Participation in EDI electronic contracting often required a substantial investment in proprietary network technologies. This requirement of an initial investment in proprietary communications technology served as a sort of defacto channeling mechanism, limiting the implementation of e-commerce procedures to parties with existing commercial relationships. Internet commerce brings problems of computer security to the forefront of the issues facing prospective participants. The contracting parties must consider not only all of the standard issues involved in any contract, such as the reliability of the representations or the creditworthiness of the other party, but they must also factor in the security of their own access to the Internet from the threat of attacks by interlopers. The openness of the Internet increases the magnitude of the threat of attack. The ABA digital signature guidelines do not purport to be a model law, but rather try to offer general statements of principle regarding the development of public key infrastructures. Additionally, one of the objectives of the guidelines was the promotion of a specific technology: the use of digital signature technology based on the X509 standard established by the international telecommunications union. The ITU X 500 series of technical standards provides the basis for constructing a multipurpose distributed directory service by interconnecting computer systems belonging to service providers, governments and private organizations. The consensus among the participants was that closed system applications of public key cryptography did not pose the same theoretical or legal challenges in their commercial development as the case of global stranger to stranger commerce over an open network. Electronic contracting over the Internet requires that parties wishing to enter into binding contracts have a means of ascertaining whether a message is actually coming from the party sending it and whether the message has been altered in transit.

##### *5. Digital and electronic signatures.*

Through the centuries several forms of signature have been used. Signatures serve a particular legal function: a) Identification of the signatory, a person has performed an action; b) Proof of the declaration of will of the signatory. The signature demonstrates the internal will of the signatory to perform an action. It is the material expression of the *animus signandi* of the signatory. The same concepts of the signature should be performed by the electronic one and the only difference should be limited into the way on which the signature is materialized.

Digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as public

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

key cryptography, which employs an algorithm using two different but mathematically related keys. One for creating a digital signature and another key for verifying a digital signature. A variety of methods are available for securing the private key. Although many people may know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that signer's private key and use it to forge digital signatures. This is referred as the principle of irreversibility<sup>30</sup>. The process of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer's. Digital signatures have been accepted in several national and international standards developed in co-operation with the accepted by many corporations, banks and governing agencies.

The technology specific statutory approach increases the legal community's ability to design legal models that closely track technology. Specificity allows for the careful consideration of the capabilities and limitations of a particular technology. Besides, technology neutral legislation allows for flexibility. It may be unwise to specify a given technology or implementation in a statute because information technology quickly changes and so the technology may be outdated even as the legislation is being debated. Additionally, there is a danger that states government may be setting one technological approach above others and that may have the effect of distorting the natural market flow toward better services and goods. The integrity of the legal system depends on the integrity of the mechanisms that bind individuals and create law. It is important to note that a signature is not part of the substance of a transaction, but rather of its representation of form. Economic reasoning should not be the guiding force and the integrity of the legal system is an overriding reason for government intervention. The confidence that the contracting parties have that their encrypted messages will remain confidential is a function of many elements that must be considered in writing the encryption software, installing the software in an operating system and distributing the secret keys.

#### *6. Digital negotiability.*

One of the identifying characteristics of a negotiable instrument is that it must comply with the formal requirements of negotiable instruments law to avoid being relegated to the status of an ordinary contract. Once the obligation has merged with the instrument, title to the instrument can be transferred by negotiating the instrument. Negotiability is synonymous with marketability and includes free transferability, recognition of special rights for good faith purchasers for value and certain procedural advantages in the enforcement of the obligation. Negotiability facilitates commercial transactions by minimizing the administrative burdens of

---

<sup>30</sup> Guidelines for secure operation on the Internet <ftp://ds.internic.net/rfc/rfc1281.txt>

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

processing information about property rights. Thus, negotiability has achieved the transactional efficiencies that result from the application of a well-defined and widely used set of rules. The digital signature guidelines Act copied elements of negotiability in the effort to improve the marketability of electronic signatures. Electronic technology (digitized negotiable instruments), like traditional negotiable instruments, should minimize the administrative burdens of processing communications and protect rights in information in e-commerce transactions. Negotiable instruments are the product of a centuries-long practice between merchants, lawyers and courts and so the digitalization of these instruments should conform to the needs of electronic transactions and the needs of modern trade. Hence, strict legal standard should build from either a given technology or from business practices associated with the use of that technology. Assimilating digitized technology into existing commercial practices is a daunting task. However, without standardization, the lack of coordination of e-commerce systems will present an obstacle to individual consumer, and this lack of guidance may stifle the rate of adoption of the technology. The use of negotiable instruments expanded because the value of property exchanged through those instruments could be increased by removing obstacles to the free transferability of the represented property. Cyberspace will not host a large amount of commercial transactions conducted over cyberspace until users feel satisfied that e-commerce security approaches that of closed-networks e-commerce systems. Moreover, commercial applications must be standardized to permit intersystem compatibility within an open network. Otherwise costs on the Internet may tend to be high because of the number of parties involved, the difficulty of locating the parties and the transborder nature of the medium. The use of PKI for digital negotiability is another major concern for lawmakers. Digital signatures are regulated by article 3 of UCC. However, articles 1 and 3 of the UCC do not yet recognize explicitly the effect of electronic documents and digital signatures made through the PKI process. The term digital signature is used to refer to signatures made through the use of a private key. By contrast an electronic signature is a much broader concept, including not only digital signatures but also names or symbols typed into an e-mail message whether or not those have the security protections of signatures made with a private key. The use of public key technology to sign negotiable instruments would make these instruments less vulnerable to theft than their paper-based counterparts. Can the use of PKI reduce or eliminate the risk that a digital negotiable instrument could be cloned by a holder? Until the threat of cloning can be eliminated the electronic negotiable instruments will remain only a theoretical possibility or in other words a digital dream. Another matter, which has to be solved, is the possession problem connected with negotiable instruments.

Uniformity and harmonization of legal rules governing PKI appears unlikely to result from the process of random state legislation. PKI interoperability refers to the capability and PKI interoperation refers to the effect of logically linking multiple

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

PKIs to form a larger PKI supporting a wider community of users. Achieving interoperability and implementing interoperation are major challenges for the PKI industry.

The ICC<sup>31</sup> has issued very recently a document concerning general usage for international digitally ensured commerce with the objective of promoting the world business community's understanding of the issues relating to the use of techniques in electronic commerce. A goal of open electronic commerce that differentiates it from previous closed forms is the enabling of short term or *ad hoc* commercial transactions between organizations and individuals. Security procedures in open electronic commerce can ensure the confidentiality, integrity, and authenticity of electronic documents, maintain the evidential value of electronic messages, and provide proof to liability in disputes between electronic commerce users and network service providers. As mentioned above, a public-key infrastructure can provide the necessary support for conducting safe and secure trade. PKI is based upon Trusted Third Parties (TTPs)<sup>32</sup> that verify that the signer of a document is indeed who it claims to be. Verification takes place by means of certificates that are confirmations of identity as well as other attributes of the holder of the corresponding private key.

#### *7. The formation of electronic contracts.*

It is now possible that both the formation and the performance of the contract can occur within the bounds of cyberspace. The e-commerce has sparked much legal debate, primarily in the context of security and confidentiality of information passed between trading partners and the security and certainty of knowing with whom one is doing business are major problems. Traditional contract law in many jurisdictions established a formal signature. In signing an electronic document, the software makes a message digest of a file to be sent and the digital signature is a series of letters and numbers mathematically calculated to be unique to each message<sup>33</sup>. Moreover, the receiver's computer calculates the message digest, and matches it with the signature block created by the sender and if the message digest and signature block are identical, the signature is valid. A traditional handwritten signature is any mark or symbol affixed to a writing to manifest the signer's intent to adopt it as his own and to be bound by it. There is no requirement that a signature be witnessed to be effective. Digital signatures serve the same purpose as inserting a handwritten signature in a paper document. The first reason of digital signature is identification. It provides a unique number that identifies whom it belongs. Its second reason is authentication and so showing that the signer adopts the text. Lastly, there needs to

---

<sup>31</sup> [1998] 37 ILM 714

<sup>32</sup> M. FROMKIN, *The essential role of trusted third parties in e-commerce*, 75 OR LR 49.

<sup>33</sup> R. NIMMER, *Electronic contracting: Legal issues*, 14 J Marshall J Computer & Info L 211.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

be a mechanism that protects documents from tampering. The effective use of digital signatures will reduce costs and increase efficiency. Many states have either passed or are considering some form of e-commerce and digital signature legislation. Traditional information boundaries are stretched to adapt to the new legal challenges of the Internet, the existing information order breaks down. Information owners and users are no longer sure of their responsibilities and opportunities with respect to the use of information. New net information boundaries have arisen, which offer the potential for a further loss of public rights in information. The law targeted the commercial providers of information by imposing a series of checks that would force content providers to censor themselves. As a result of the uncertainty in the ability of the law to preserve the information status quo, policymakers, with the support of information owners, have reacted by seeking alternative measures to protect their interests. It could be said that the first inaccuracy is that conduct and content cannot be regulated on the Internet through law because the Internet is an open system, with no boundaries, and thus, law cannot practically apply. Besides, the reality of recent www litigation suggests that society is adopting legal concepts and concepts of virtual spaces. Essentially electronic messages produce the same legal effect as messages written in traditional format, such as on paper. If a company's trademark is not a domain name, the business should register it as such to prevent subsequent use by others and future litigation.

New legal concepts have to be introduced so that law corresponds to the needs of technology. As mentioned above, the new legal concepts cannot contradict the old concepts of law because new electronic commerce terminology is introduced to serve the traditional concepts of law. Of course, the introduction of new concepts of law cannot be prohibited since new developments of life bring forward new notions or concepts.

The functions of a traditional written document are: informative when information appears on it; probative or evidential when it consists proof of its contents ; and symbolic when it incorporates facts with legal value. Therefore, formal requirements concerning the validity of paper-based transactions inhibit the use of open EDI for electronic commerce. For instance, the existence of a paper document is connected with the conclusion of a real estate contract. Consequently, there is a need for a reconsideration of the approach to fulfilling legal requirements. Current legal formalities exclude several kinds of transactions from the scope of EDI.

Documents can assume one of the following three forms: documents, which have probative power (*ad probationem*); documents, which confer rights (*ad solemnitatem*); and securities. National laws require that documents that fulfill formal obligations assume a written form and they are signed. A broad interpretation of the existing legal concepts in order to include electronic means should be the first step, which can facilitate open EDI. Consequently, electronic transactions should be treated comparably to paper ones for contractual and other formal purposes. Identity must

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

be judged on the quality of evidence provided by a particular technology as well as any associated procedures or records. Even when identity is clearly established by an electronic signature, it is not legally binding unless made with requisite intent. Consequently, no electronic technology can demonstrate intent on its own. Hence, technologies that are implemented passively and automatically cannot generate a valid signature. Intent has to be established through a procedure in which the signer's active participation is showed to provide evidence of informed and voluntary subscription to a particular electronic transaction.

The Basic factor of the dematerialization of commercial transactions is referred to the admissibility of electronic documents as evidence. The admission of electronic documents must be based upon harmonized provisions with respect to form. The admissibility of a document as evidence should be independent of the format that a document takes and the medium that is used. Continental legal systems provide that all means of evidence can be admitted as evidence in court. In some countries civil procedure law sets out a list with the acceptable means of evidence. Greek law provides an exhaustive list for the acceptable means of evidence. article 444 of the Code of Civil Procedure provides for the conditions under which a document can be admitted as evidence in a civil law trial. In article 448(2) it provided that: «mechanical reproductions consist a full proof for the facts or things which are stated upon them, however, counter proof is permitted». Mechanical reproductions in the context of article 444(3) include «any video recording, facilitated by any means». On the one hand, there is no explicit reference to electronic means of evidence such as electronic documents that would facilitate the use of EDI generated documents. On the other hand, a broad interpretation might accommodate the admissibility of electronic documents. For example, for penal law purposes a computer memory is considered to be a written document (Act 1805/88). Accordingly article 1000(1) of the US, Federal Rules of evidence refer to mechanical recordings. Article 1000(1) includes electronic recording or other form of data compilation. According to article 1000(3) an original writing only needs to be readable by sight and there is no need to be printed out. Hence, computers should be placed in the same category of devices like video cameras or tape recorders that are explicitly recognized by law. The admissibility of electronic documents should be strengthened by attaching probative value to them.

A common risk in open EDI is that trading partners may not have enough information on the identity of their trading counterpart. Security measures are important to guarantee the reliability of information used in open networks. there are two kinds of remedies to the security in open EDI, technical and legal. Both remedies contribute to the security of the system and enhance the legal validity of it. Open EDI is necessary to achieve a high level of certainty with respect to the contents and the transmission of a message. Hence, it is important to draw the limits of liability of EDI users so that the necessary precautions can be taken. User liability

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

issues in open EDI refer to the interchange of electronic messages and, therefore, interchange considerations do not interfere with the underlying commercial transaction.

The European Union has the responsibility to ensure that communications networks are interoperable and are developed in a way to promote economic and social cohesion and economic competitiveness. Legal frameworks for electronic signatures should not be used as trade barriers, and such system should not result in being an obstacle to trade<sup>34</sup>. Hence, legal validity of electronic (digital) signature and interoperability of certificates and electronic signatures must be achieved. The global framework for electronic signatures should be market driven and offered to the public in a fully competitive environment, because the electronic signature and authentication systems are still under development. It could be argued that market forces and industry self-regulation are likely to be the most suitable and effective means to protect consumers from fraudulent and misleading conduct.

Electronic commerce facilitates established business-to-business commercial relations, sales by companies to consumers, and exchanges between consumers. Thus, e-commerce is changing the way people do business. We have moved from an industrial economy where machines dominated productivity, to an information-based economy where intellectual content is the dominant source of value added and which knows no geographic boundaries. Freedom of contract should be the guiding principle for business-to-business relationships.

As mentioned above, EDI agreements are a means by which commercial transactions are conducted electronically and become legally binding. Private companies have created new EDI systems, which allow cross-industry electronic transactions via Internet agreements. The increased flexibility of these systems circumvents the conflict between the two EDI programming standards. The UNCITRAL model code on EDI transactions would enable nations to enter into bilateral agreements under traditional contract law to establish EDI agreements with one another and grant legal protection to such agreements. The US has a wide variety of statutes designed to regulate computer transactions on the Internet resulting in the most developed body of Internet law in the world. State legislatures have moved to incorporate the recognition of digital signatures and EDI agreements into their state commercial codes. Besides, the EU<sup>35</sup> establishes EDI agreements in several industries in Europe by using the UN/EDIFACT standard, which is rapidly becoming the global standard for e-commerce. Additionally the European Commission intends to prepare

---

<sup>34</sup> M. MELAND, *Europe: The next frontier*, 1999 Forbes March 29 <http://www.forbes.com>, L. HELM, *www living up to its name* 1999 Nando Times News March 28 <http://www.techserver.com>

<sup>35</sup> COM(97) 157 European Commission: A European initiative in e-commerce. COM/97/503 A European Framework for digital signatures.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Ciberspazio e Diritto" (<http://www.ciberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in Ciberspazio e Diritto, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.ciberspazioediritto.org>

guidelines for self-regulation of e-commerce and Directive 1999/93/EC of the European Parliament and of the Council of 13 Dec 1999 introduce a community framework for electronic signatures (OJ 2000 L13/12). The Commission proposes articles 57, 66 and 100A as the legal basis for the directive. The purpose of the directive is to clarify the regulatory framework and to safeguard the rights of users of e commerce. E commerce presents the EU with an opportunity to advance its economic integration. Electronic signature allows the recipient of electronically sent data to verify the origin of the data and to check, that the data are complete and unchanged and thereby safeguard their integrity. Besides, even the verification of the authenticity and integrity of data does not necessarily prove the identity of the signatory that creates the digital signature. The different initiatives in the member states of the EU lead to a divergent legal situation. Divergent rules regarding the legality of digital signatures is detrimental to the further development of e commerce and to economic growth and employment in the EU. It could be argued that diverging situation could create a serious barrier to communication and business via open networks throughout the EU, by inhibiting the free use and supply of electronic signature related services. World wide electronic communication and commerce are dependent upon the progressive adaptation of international and domestic laws to the rapidly evolving technological infrastructure. Article 2 of the directive defines the terminology used in the directive. Each member state ensures the establishment of an appropriate system that allows for supervision of certification service providers. Signatures, which are created by a secure signature creation device, should satisfy the legal requirements of a signature in relation to data in digital form in the same manner as a hand written signature satisfies those requirements in relation to paper based data and are admissible as evidence in legal proceedings. There is a need that member states ensure that certification service providers and national bodies responsible for accreditation comply with the requirements laid down in directive 95/46/EC (OJ 1995 L281/31) regarding the processing of personal data and on the free movement of such data. The requirements for qualified certificates, certification service providers issuing qualified certificates and service signature creation devices are stated in the attached annexes.

The self-regulation system provides a local solution to an Internet problem. The restrictions on encryption technology and the aim of international EDI cooperation seem to result in conflicting outcomes. The only efforts made to coordinate encryption or digital signature policies have been advanced by the OECD<sup>36</sup>, which issued multilateral encryption standards. The advent of global computer networks has rendered geographic boundaries increasingly ephemeral. As the community of the Internet users grow disputes of every kind may be expected to occur. Online contracts will be breached, and online torts will be committed, online crimes will be

---

<sup>36</sup> <http://www.oecd.org>

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

perpetrated. Although many of these disputes will be settled informally, others may require formal mechanisms for dispute resolution. EDI is both a convenient and an efficient substitute for transmitting paper documents between individuals or enterprises. Contracts can be formed, performed, and broken in cyberspace. The net brings inexperienced persons from different jurisdictions together in contractual relationships. Electronic contracts will not be widely accepted until there is an agreed upon method between parties on recording a digital signature. The more favored design in the Internet field is to use some form of public key encryption combined with certification to serve as a digital signature. For digital signatures to gain widespread acceptance in legal situations, there will need to be legal recognition of digital signatures in each state's statutes. On cyberspace two main ways of contracting can be used. First, offer and acceptance occurs in e-mail. After receipt, the messages are stored by host computers in <mailboxes>, where the addressee can collect them. The traditional mailbox rule may apply to offers, acceptances, modifications and revocations sent by mail or EDI transmission. Second, online catalogs and order forms are found on the web. When starting to use EDI trading, partners will conclude <master agreement>, regulating their relations. The transactions will then be carried out by computers programmed to automatically accept orders and control delivery. Hence, messages may be exchanged directly or via one or more service providers. Computer-based contracting can deal with any subject matter namely sale of physical goods, supply of digitized products and supply of services and facilities. Contracts are based on the decisions and actions of individuals because a contract will come into being if the parties intent to conclude it. Interactive web sites enable users to transmit information directly by filling an electronic form. Offeror and acceptor must express their willingness to be bound explicitly or it must be implicit in their actions. Where computers make choices without human (the parties' involvement), the validity of any concluded contract should be invalid. The responsibility remains with the parties, who decide to use software with the intention of being bound by their declarations via a complex program and sophisticated software by a previous programming. It could be argued that the involvement of a computer has no legal consequences because it is the result of prior human intention. Thus, automated declarations of offer and acceptance should be valid<sup>37</sup>. Moreover, disputes will arise regarding the formation, performance, and payment of contractual obligations.

It could be argued that the formation of a contract on the Internet starts with a consumer looking at the website of a supplier who offers products for sale. One could view a website as similar to a shop window and, so, regard the description of goods on a website as being an invitation to treat. Besides, commercial website serve both as 'shop displays' and 'shop sellers' - they fuse the advertising and the selling. It

---

<sup>37</sup> Thornton v Shoe Lane [1971] 2 QB 163.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

could be argued that court can construe websites as being invitations to treat. Somebody should look at the objective intention<sup>38</sup> behind the website of a company. Moreover, the principle of misrepresentation is highly possible to arise very often in cases of sales of goods on the Internet. The next step to a binding contract is the acceptance. The acceptance has to be unequivocal; any change to the original offer would amount to a counter offer. The general rule of *Felthouse v Bindley*<sup>39</sup> should apply where the supplier made the offer and it is up to the consumer to accept it. However, security is essential to create certainty with respect to the contents of the message and the parties involved in a transaction. Another important issue is the timing of the acceptance and the question of when a contract over the Internet was formed. Therefore, the time and the place of the formation of a contract, which are basic elements of a contract, are applicable to the conclusion of a contract over the Internet. Thus, the traditional concepts of the law of contract are still applicable in electronic transactions as well. Trade practice has developed a number of rules for the time and place of the formation of a contract. For instance, in English law there are two rules that could apply: the 'instantaneous transmission rule' whereupon the contract is formed once the acceptance is received and the 'postal rule' according to which the acceptance is deemed to be effective at the time of sending. The postal rule applies to all contracts the acceptance of which is notified by mail. When the phone or the telex are used then a contract is formed at the place and the time that the acceptance of a contract is received by the offeror<sup>40</sup>. The reception rule is applicable in many jurisdictions, which is suitable for EDI as well. The acceptance by e-mail and over the web when the consumer clicks a button on the seller's website to confirm acceptance are the expression of acceptance as it has been perceived in the law of contract. E-mails differ to a crucial extent from means such as phone or fax. The message of acceptance is not sent directly from the offeree to the offeror- they are sent from provider to provider and need to be picked up by checking the personal in-box at the provider's server. E-mail is not sent 'like it is'- it is converted into digital form and broken into digital chunks. The sender does not know whether and when the e-mail was received and whether it was complete. It could be argued that the postal rule should apply. Besides, if the acceptance is made by the offeree clicking a button on the web seller's page, the partners know whether their message was received or not. Hence, an acceptance made by communication over a website should be effective once it is received by the offeror.

Another major issue is how standard terms and conditions may be incorporated into a contract over the Internet. The terms need to be brought to the consumer's notice

---

<sup>38</sup> *Harvela Investments Ltd v Royal Trust Company of Canada Ltd* [1986] AC 207.

<sup>39</sup> [1862] 11 CBNS 869.

<sup>40</sup> *Bribinkon Ltd v Stahag Stahl* [1982] 1 All ER 293. *Entores Ltd v Miles Far East Corporation* [1995] 2 QB 327 for acceptance by telex.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

prior to the conclusion of the contract<sup>41</sup>. There are different ways for a web seller to bring its standard terms and conditions to the consumer's notice. As mentioned above, he may attach a hypertext link to his page, which reveals the terms or he can point out to terms and conditions contained in the seller's FAQ (frequently asked question) or the supplier could alternatively refer to an e-mail address where the consumer can demand the terms.

For e-commerce to be viable, electronic contracts must be recognized and given equal standing and effect on law. Legal problems often arise because there is a conflict of viewpoints in how to best characterize space on the Internet. Harmonization is a term used to describe the process of conforming national laws to some basic international standard. Recent WIPO treaties protect copyrighted material in digital environments and to provide stronger international protection to performers and producers of sound recordings<sup>42</sup>.

Whose laws apply when litigation arises from activity in cyberspace? The dispersed location, the rapid movement of data together with the geographically dispersed data processing activities are complex factors causing problems in choice of law in the case of international computer networks. It has been said that it is the forum's choice of law rules that direct the court to the applicable law. As mentioned above, the principle that parties to a contract can chose the applicable law is recognized. If the parties do not make a choice then the applicable law is left to be decided by the national rules of the forum state<sup>43</sup>. The courts had a number of mutually inconsistent choices of law rules at their disposal and felt free to use whichever one of these rules would permit them to reach the desired result. Two rules were applied to contracts. One was that questions of validity are determined by the law of the state where had occurred the last act necessary to create the contract which would be the state where the offer was accepted. Questions of performance are determined by the law of the place of performance. In the area of torts and contracts, a degree of flexibility was concealed within a system. Courts have a single choice of law rule in torts but two principal choices of law rules in contracts. The applicable law should be that of the state where most of the contacts were grouped. The most important basis was that weight should be given to the law of the state, which had the greatest interest with the specific issue raised in the litigation<sup>44</sup>. The basic policy in contract is protection of the expectations of the parties and therefore calls for the enforcement of a contract in accordance with its terms. This principle could not be changed if we had a contract concluded on the Internet. A choice of law clause provides the best way of

---

<sup>41</sup> *Thorton v Shoe Lane Parking Ltd* [1971] All ER 686.

<sup>42</sup> Digital Millenium Copyright Act of 1998 12 Stat 2860. G. ZEKOS, *Conflict of laws and the contractual role of bills of lading* 1998 Managerial Law Number 3.

<sup>43</sup> *The Amazonia* [1990] 1 Lloyd's Reports 236.

<sup>44</sup> *Babcock v Jackson* 191 NE2d 279.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

insuring that the desired law will be applied. It is the choice of law rule of the forum that directs that the law chosen by them should be applied.

Burnstein<sup>45</sup> has suggested that the access provider should be the certain factor of reference in order to resolve interuser choice of law problems. This approach might bring a certainty and predictability but it might be unfair for many users. Networks are highly decentralized but it could be argued, as the first step, that rulemaking occurs at the lower network level, where the commercial or corporate provider can be both the legislator and enforcer. The party who is dissatisfied with a particular access provider's choice of law selection can simply seek a new provider<sup>46</sup>. A problem might be caused by the fact that it is difficult to have the same rate providers to choose one. No bargain between a user and a system provider could alter the responsibility of either one to a third party harmed by action of the one or the other. Forum selection clauses can bring order and stability to electronic contracts. In fact, contracts between sysops and users appear to be contracts of adhesion, with the users possessing no bargaining power. As long as the users are on notice of the nature of the contract and the applicable rules and obligations of the contract have clearly articulated, then they can choose to accept the terms as stated or find another system. Hence, inclusion of a forum and law selection clause in the access contract between user and provider could be the first step for solution in local level. Moreover, all legal systems accept the binding nature of trade usages in contracts between merchants and therefore there should be no obstacles to the general recognition of a customary law of international trade<sup>47</sup>. In the same way merchants knew the customs and usages in the *lex mercatoria*, so too should users in cyberspace be charged with a knowledge of the customs and usages of the online world. The ability of the law merchant to adapt rapidly to changes in the technical and, consequently to legal environments is an appealing aspect for its endorsement as a second step in choice of law problems. Thus, in an international level the chosen law would be a mixture of customs and accepted practices that had grown up with cyberspace. Besides, a choice of law regime should be established through a multinational treaty for actions in transnational transactions where traditional and self-governance rules cannot be applicable. Hence, sometimes sacrifice of fairness could be necessary in order to achieve certainty. The parties cannot by a choice of law provision escape a fundamental policy of the country whose law would be applicable if that of the parties' choice were to be disregarded. When the issue is one of validity, there would be a tendency for the court to seek to apply the law of a state that will uphold the contract. Moreover, it is possible that some nations' courts could

---

<sup>45</sup> M. BURNSTEIN, *Conflicts on the Net*, 1996 *Vad JTL* 75.

<sup>46</sup> *Carnival Cruise v Shute* 499 US 585.

<sup>47</sup> R. SEDLER, *Interest analysis and forum preference in the conflict of laws*, 34 *Mercer LR* 593; R. LEFLAR, *The nature of conflicts law*, 81 *Colum LR* 1080.

Attenzione: il presente testo è una bozza dell'articolo omonimo pubblicato nella versione cartacea della Rivista Scientifica "Cyberspazio e Diritto" (<http://www.cyberspazioediritto.org>). Si tratta di una BOZZA: può quindi contenere differenze e, soprattutto, imprecisioni, inesattezze o refusi che sono stati poi corretti all'atto della correzione delle bozze e della messa in stampa dell'articolo. Si consiglia, pertanto, di riferirsi, nelle citazioni, esclusivamente all'articolo pubblicato a stampa. Il riferimento dell'articolo che segue è Legal problems of commercial transactions in cyberspace: an overview, George I. Zekos, in *Cyberspazio e Diritto*, Volume I, Numero II, pp. 123-164.. Articolo tratto dal sito <http://www.cyberspazioediritto.org>

decline jurisdiction on *the forum non conveniens* grounds and justice be better served were the case to be heard in a different forum.

#### 8. Conclusion.

The expected commercial boom on cyberspace will not emerge unless obstacles to efficient contractual relationships are removed and so transaction costs incurred by the cyberspace' dealings are minimized. These costs include: risk of inappropriate law being applied, risks flowing from contractual uncertainty, and loss of time spent litigating<sup>48</sup>. The net can develop its own effective legal institutions. The most apt analogy to the rise of a separate law of cyberspace is the origin of the law merchant. Sysops acting alone or collectively have the power of banishment to control wrongful actions online. One nation's legal institutions should no monopolize rule making for the entire net. Given that the people engaged in online communications still inhabit the material world, local legal authorities must have authority to remedy the problems created in the physical world by actions occurred on the net.

On the one hand, change in the medium does not necessarily mean that a new system of law has to be created to solve the problems on the Internet. On the other hand, the appropriate focus should be on the end result, in other words the effects on the real world, not on the means by which the images were transferred<sup>49</sup>. The key to change lies in understanding how a medium affects patterns in communication. It is a reality that the advent of computer-mediated communication has created a new world with new rules. Hence, whoever controls the communications system within a country has effective control of the government. Electronic commerce over the Internet should be finally facilitated on a global basis. It could be argued that a new form of electronic (virtual) presence might be a fundamental element for an electronic jurisdiction rather than a physical one. However, a catalog of activities that will render one amenable to suit in a particular jurisdiction remains elusive. A broad effects test is incompatible with the nature of the net. A mere web site accessibility is not enough to have an active web site. Thus, problems caused by the Internet and not reflected upon injuries in the real world can be solved by the Internet itself and problems caused by the Internet in the real world should be solved in the real world by the traditional legal entities.

---

<sup>48</sup> UCC 2-205, 1-205.

<sup>49</sup> US v Carlin Inc 815 F2d 1367, US v Gilboe 684 F2d 235, Miller v California 413 US 15.