"Some Thoughts on The Legal Aspects of New Technologies…"

María-Gabriela SARMIENTO
SARMIENTO NÚÑEZ & ASOCIADOS
Mailing address: P.O. Box, 63.194, Chacaíto Caracas 1060 Venezuela
Location: Edif EASO, p. 5, Of. 5-B,
Av. Fco. de Miranda, Urb. El Rosal, Caracas 1060 Venezuela
Tel. +58 212 952 36 83/66 80 ; Fax + 58 212 979 81 71
Emails escrisar@cantv.net ; gabriela.sarmiento@laposte.net

ABSTRACTS

This paper addresses legal and ethical topics raised by the use of Internet for concluding contracts, sharing information, exchanging documents, advertising, selling/buying goods and services, hosting contents of any kind through a service provider, signing any type of documents electronically, using email for commercial purposes and weakening the rights of authors. A description of the current legal framework in Latin America (with the exclusion of the Caribbean States) has been made through a comparative analysis of its provisions. Cases-law are provided as illustrative examples.

Keywords: E-contracting, E-signatures, Cyber-crime & SPAM, Applicable Law & Jurisdiction, Privacy, Copyright, Consumers.

1. INTRODUCTION

Informatics imposes new challenges and requirements relating for instance to intellectual property rights, privacy, security, and competition between Internet Service Providers (ISPs).
Precedents, international conventions and model laws and nationally enacted legislations in the area of electronic communications, have brought minimum levels of security and certainty to electronic transactions. However, the international community has not yet reached an agreement with regard to many of the areas mentioned above. Not even precedents are consistent since similar cases are not solved in the same manner in a country and within a short period of time. There is also a lot of concern among the Internet Society with regard to the conclusion of contracts through the Internet, the law and jurisdiction applicable to the transactions online (when not agreed by the parties), the data messages and documents electronically or digitally signed, online auctions, cyber-crime, the protection of online consumers and the protection of private data, to mentioned few of the areas where doubts have been raised all over the globe and which I will address in the subsequent chapters through a concise comment, examples of in force and drafted legislation in Latin-American and case-law from different regions.

2. CONSUMER PROTECTION

From the moment consumers can acquire products and services offered anywhere in the world, they shall understand in advance their obligations under the country-specific consumer protection regulations. Both, producers and consumers need to know what is the legal status of their transaction conducted on the Internet, what are the recourses available to a buyer in case the retailer breaches the contract, etc. In order to do so, consumer and sellers should base their relationship on a clear legal contractual framework to clarify the rights and protection afforded to consumers in different countries when engaging in B2C e-commerce.

When signing clip-wrap agreement, consumers must be aware in advance of the general and specific conditions of sales. Sellers should put a link to these conditions and encourage consumers to read them before they click on the "I agree bottom". Most consumers never read these statements and agree to enter into a contractual relationship without been aware of the forum that applies to it in case of conflict, to mention one case.

Consumers should benefit from secure electronic transactions… they should have access to certified websites, secure online payment systems (e.g. secure socket layer, etc.), full information on the company and contact details by email, phone, fax, and mail, full description, instructions of use and, if possible a picture, of the goods offered through the Internet. They should have the possibility to return the good, within a reasonable period of time as from the date of delivery, if it does not comply with what they ordered. Sellers should have online technical and after sales assistance for free. If goods or services are bought or acquired through an exchange of emails, these emails should have the same subject and, when possible, they should have been sent protected with encryption technology.

Most of these policies apply to traditional commerce. The difference is that these requirements should be adapted to the transactions concluded online and to the types of tools and services that might be available for sellers (e.g. private company, public entity) and consumers (e.g. private and public) within their B2C, B2B, and/or G2B relationships.

With regard to Spam or junk email, it is important to note that the standard policies are the well-known opt-in and opt out rules. Consumers have the right to consent or to refuse the reception of data messages sent to the general public as part of a marketing strategy of businesses.

National Legal Frameworks for online transactions: In **ECUADOR**, the consumer/user shall consent to use data messages in a relationship with a seller but before that he/she needs to be provided the details on the software and hardware required to access the data messages. If a dispute arises from an e-contract between a consumer/user and a seller, the forum will be based at the place of residence of the consumer, except otherwise agreed between the parties. Consumers should be informed of its contractual rights and obligations in a clear and precise manner, be provided with exhaustive information on the goods and services to be acquired (also in **PERU** and **VENEZUELA**) and be informed on how to access and update the personal data collected from them. In **MEXICO** the information consumers provide to sellers should be treated as confidential. Sellers cannot transfer or diffuse the collected

information to other third parties without the prior consent of consumers. Sellers should inform consumers of the technical tools used to provide security and confidentiality to this information. Sellers will be bound by the consumers´ decision not to receive any commercial advertisements. Before concluding an agreement, sellers should provide consumers with his/her contact details for any future complaints or requests for clarification (this also applies for **VENEZUELA**). Consumers are entitled to know the sale's terms and conditions, the costs and additional charges, the modes of payment, etc (this also applies for **URUGUAY, ARGENTINA**, and **VENEZUELA**). In **PERU, VENEZUELA, URUGUAY** and **ARGENTINA**, sellers are bound by the content of their offers and advertisements of the available goods and services that are distributed through any mean of communication. In **URUGUAY**, **VENEZUELA** and **ARGENTINA**, the content of the advertisement is considered part of the future contracts concluded with consumers. Consumers could withdraw the acceptance of offers made via Internet, unilaterally, within a fixed period of time after the conclusion of the contract or the reception of the good.

Case-Law: **GERMANY**: The court decided that failure by a company to disclose its name and address in a conspicuous manner, as required by law, was an act of unfair competition and that the claimant had a cause of action to demand the discontinuation of defendant's violation.[1] The court found that the offer by the seller of goods for sale through an auction engine was a valid undertaking to sell the goods to the highest bidder. Such an undertaking constituted an offer to conclude a contract, which the buyer had accepted through his bid. A valid contract had thus been concluded.[2]

3. DATA PROTECTION

These days, it is quite easy to collect a vast amount of data about individuals. Therefore, provisions shall be drafted to establish the obligation to collect and process personal data only for specified, explicit and legitimate purposes, and to ensure that such data is relevant, accurate and updated. Protection of data shall include the right of individuals to be informed about where would the data be available, the identity of the organization processing the information, and the purpose of such collect.

National legislations have adopted internationally standardized criteria for individuals to review their personal data collected for a specific purpose by any organism. Individuals can review, modify, and correct their personal data at any time…in the majority of the cases. Consumers have the right to know why is the information required, what is the purpose of the company for collecting such data, how would it be used, who will have access to it, etc. It is mandatory for businesses, in those countries benefiting of *habeas data* or privacy protection regulations, to manifest such reasons and provide all details related to the storing database.

National Legal Frameworks: **COLOMBIA**, **PANAMA** and **URUGUAY**: individuals have the right to know, update, and rectify information gathered about them in data banks and in the records of public and private entities. In **ECUADOR** and **PARAGUAY**, it is recognized the right of individuals to access his/her personal information on public and private databases to be aware of the reasons for collecting such information and be able to update, rectify or destroy its content. In **ECUADOR**, individuals should consent on the transfer and use of their collected personal data. Collected personal data should remain private and confidential. In a **Mexico**'s bill, collected data must be adequate, true, pertinent and in conformity to the reasons for which it was collected. The data can only be used for the purposes for which it was collected (this also applies in **ECUADOR**). Non-accurate data must be updated, rectified or cancelled and individuals must have access to its content in order to modify, update or cancel non-accurate information. Databases should be secured and confidential. Owners of an automated collected data should, in most cases, previously authorize the collection of personal information (these policies also apply in **ARGENTINA** and **CHILE**).

Cases-Law: **EMPLOYEE'S PRIVACY**: emails are a private correspondence and many courts have decided that when an employer reads the private electronic correspondence of its employees, they are breaching the employees' right to privacy and data protection. Cases where employers fired employees on the sole ground of the content of a private electronic correspondence have been decided in favor of the employee. **PERU**: individuals should have access to their collected personal data in order to rectify, update or exclude information that might be harmful[3]. An **ITALIAN**[4] court decided that held that it is an offence to compile and organize a client's private data in an electronic database to be used for promotional

[1] Oberlandesgericht Frankfurt. 17 April 2001. Case No. 6 W 37/01. JurPC - Internet Zeitschrift für Rechtsinformatik (IZR), WebDok 135/2001 (JurPC.de source)

[2] Amtsgericht Hannover. 7 Sept. 2002. Case No. 501 C 1510/01. JurPC - IZR, WebDok 299/2002 (JurPC.de source)

[3] **L.A. Tavara Martin - Habeas Data** (Constitutional Court of Peru)

[4] **Pretura di Palermo, 4 February 1999. Dir informatica 2000, 299 nota (Corrias Lucente)** (Infogiur source)

purposes without their consent, as it constituted illicit treatment/use of private data.

4. INTELLECTUAL PROPERTY

Intellectual property rights are legal means to protect and balance the interests of an individual against those of the public. This is done in terms of disclosure, dissemination, alteration, use and abuse of ideas, with an exclusive right to control and profit from invention and/or authorship of such intangible goods, services and ideas. In particular,

copyrights are the rights to ensure protection of information from duplication and distribution. Generally, the copyright owner has the exclusive right to make copies of his/her work. New technologies have accrued the cases in which copyrights are breached by mean of creations of illegal copies and distribution of those illegal copies. Music and record companies have intensively fought against piracy during the past ten years. They count with many successful court decisions were the defendants have been condemned to pay huge sums of money as indemnities to music and record companies but the problem is far from being solved. Of course, this problems existed even before the development of new technologies, the difference is that with the latter, violation to copyright has become easier, less expensive and of best quality.

In order to tackle the problems from its source, there is a need to formulate a system of laws that defines and protects intellectual property as a response to technology changes. WIPO, WTO, the EU, OECD, and ICANN have ongoing debates relating to intellectual property rights to find a suitable framework. Below are some comparative features aimed at protecting copyrights in The Americas.

National Legal Frameworks: The general policies for **ARGENTINA**, **CHILE**, **COLOMBIA, VENEZUELA, PARAGUAY, PERU, MEXICO, ECUADOR, URUGUAY, BOLIVIA, HONDURAS, EL SALVADOR, BRAZIL, GUATEMALA, NICARAGUA, PANAMA, COSTA RICA are**: All works expressed through any means are protected including databases and computer programs. Copies, reproduction, and redistribution of copyrighted material are forbidden except for scientific or didactic purposes or for a private use in). This provision applies to foreign copyrighted material. There is no harmonization of the period of protection (e.g. for life; for 30, 50, 80, 70, 75 or 60 years). **BELIZE** shares the same main copyright principles. **VENEZUELA, BRAZIL, URUGUAY, PERU** and **ARGENTINA** regulate free-software. Most of these legal texts reproduced the content of the WIPO Copyright treaty.

Cases-Law: **USA**: "*In July 2001, the music industry was successful in using copyright infringement litigation to shut down Napster. Following Napster's demise, a number of next generation services (with names such as Morpheus and Grokster) became the service of choice for file-sharers. The music industry sued these services under the same legal theory it had successfully used against Napster; namely, that such services were liable for contributory copyright infringement. However, on April 25, 2003, U.S. District Judge Stephen V. Wilson of the Central District of California granted the defendant's motion for summary judgment. The court relied on the fact that the Grokster-type services did not "contribute" to the end-user's infringement in the same way that Napster did. Specifically, while Napster was publicly touted as a "peer-to-peer" network in which users shared files directly with each other, in reality Napster hosted a central database of the files that were made available by each of its users and thus provided the unlawful "site and facilities" for the acts of infringement. In contrast, Grokster merely licensed the software that allowed users to engage in file-sharing. The users then interfaced directly with each other without any centralized assistance or control. The court found this difference dispositive, holding that the mere provision of file-sharing software, which could ostensibly be used for many legitimate purposes, was not contributory copyright infringement*."[1] **GERMANY**: "*The German Federal Court has rejected a claim that deep linking to copyright material made available on the internet infringes copyright or data base right*"[2]

5. LIABILITY AND DISCLAIMER

There is a need to identify the liability in respect of the sale of goods and services; the liability of end users reproducing infringing copies of copyrighted works by viewing them on their PCs, the liability of intermediaries; and liability of companies hosting defamatory material on mirror sites or acting as mere conduits for such material. Appropriate principles with the aim of establishing the legal framework to regulate rights and responsibilities for and on behalf of Internet Service Providers (ISPs) in terms of liability should be developed. New legislation shall apportion liability for loss or damage between the provider of the goods or services, distributors and those intermediaries that act as the mere conduits.

The **GENERAL TREND** for the ISPs liability is that they must notify the authorities of any illicit activity or content that they might be aware of. They should be fined if they do not notify the authorities in a reasonable time.

Cases-Law: In **CANADA**, an ISP hosting a website with pedophilia content shall remove the site from the Web whenever requested by a tribunal of justice.
The **EUROPEAN COMMISSION** proposed to establish minimum liability rules for services providers, who will be liable for the validity of certificate's content. In **FRANCE**, Web hosting companies and ISPs are not responsible for the content of the website – The web hosting company is obliged to provide the contact details of the owner of the website for judicial purposes.[5] In **FRANCE**, the tribunal de commerce de Rouen stated that the owner of a site and NOT the Webmaster is responsible for its content. In **ITALY**, if an ISP does not declare the identity of the owner of certain domain name or provides false information upon request of the authorities, it will be liable of fraud or cyber crime. In **SPAIN**, each Spanish website should be registered at a governmental organism and it's host is obliged to inform the authorities of any suspected content in a site.

6. CYBER-CRIME (including PORNOGRAPHY)

Crimes committed by individuals or groups of individuals through the Internet, in an operating system, a computer, online and off-line databases, electronic files, digital certificates, data messages, etc have become part of our day-to-day life. Copyright violations can also be considered as a cyber-crime.

[5] TGI de Paris. Ordonnance de refere. May 26, 2003. J´Accuse and UEJF V. Association eDaama.org, M.N.M. and SARL OVH (Juriscom.net source)

Millionaire losses and reduction of good reputation have been registered in companies due to a cyber-crime (e.g. viruses, hackers, Trojan horses or other illegal intrusions from a third party). These irruptions are now penalized in most of the legal texts adopted at a national level as the cyber-crime acts. In November 2001, a new framework to fight against cyber crime was borne: The Budapest Convention on Cyber-crime.

National Legal Framework: Who reveals and diffuse restricted data stored in a computer system commits a crime under the laws of **CHILE, GUATEMALA, ECUADOR, COSTA RICA, VENEZUELA** and **BRAZIL**. Is considered a crime in **ARGENTINA** [Bill], **CHILE, PERU, COSTA RICA, COLOMBIA, VENEZUELA, ECUADOR, BRAZIL, MEXICO** [it refers specifically to the violation of computer systems and data of financial institutions] and **GUATEMALA** the illegitimate access to restricted computer systems or data stored electronically. In the above-mentioned countries, who modifies, destroys, cancels or makes a computer system or data inaccessible or, more generally, causes any damages to it commits a crime penalized by law. The computer fraud is penalized in **ARGENTINA** [Bill], **MEXICO** [Sinaloa State], **PERU, COSTA RICA** and **VENEZUELA.** This last country, **ECUADOR** and **BRAZIL** penalize the falsification of electronic documents. The possession of equipment for sabotage or falsification or the provision of such services; the violation of private data and communications; the intellectual property violation; the fraudulent use and illegitimate acquisition of smart cards; the theft through informatics means; the illegitimate acquisition and provision of goods and services; and false or fraudulent advertisements are crimes in **VENEZUELA** and most of them are crimes in **GUATEMALA** and **ECUADOR. PERU** (which forbids kids from accessing pornographic sites), **ARGENTINA** [Bill], **VENEZUELA,** and **COLOMBIA** have adopted legal provisions against online child's pornography. The violation of private electronic correspondence and personal data is considered a crime in **ARGENTINA** [Bill] and **PERU** [Bill]. The Convention on Cyber-crime is in force since July 2005 to fight against racism, xenophobia, and any other type of crimes committed through the Internet. It was signed by the USA and Canada. Bush asked the US Senate to ratify the Convention.

Case-Law: A **Canadian** who took pictures of his teenage girlfriend with a mobile phone and uploaded them to be diffused on Internet was imprisoned. [3]

7. NON-SOLICITED EMAILS (SPAM)

No need to be inventive in its definition, SPAM emails are very well known by all of us as unsolicited e-mail, mainly of a commercial nature, sent to multiple mailing lists, individuals, or newsgroups online. There are hundred of indicators showing the economical prejudices caused by these type of emails. Laws have been enacted to fight spammers; ISPs have implemented mechanisms to block SPAM emails and to process the complains related to the reception of SPAM emails and Courts have positively applied the Anti-SPAM acts but still the problems seems not to be solved nor even reduced considerably.

National Legal Frameworks: In **BRAZIL** [Bill], any unsolicited email of commercial or illicit content is illegal. ISPs are entitled to block the transmission of such emails (like in **ECUADOR**) and should provide mechanisms to denounce SPAM. In **COLOMBIA** [Bill], **BRAZIL** [Bill], and **PERU** non-solicited commercial emails are illegal if they do not title their email with the word « advertisement » or « non-solicited email », if the message lacks of a complete information related to the contact details (including an email account) and of any mechanisms to opt-out, and if the email was sent to a recipient who had previously opted-out. In these three countries, fines and indemnities can be requested for the damages that unsolicited emails may cause. Non-solicited emails will also be illegal, if their content is false in **COLOMBIA** [Bill], and **PERU**. Note that in both countries ISPs are not held liable for the reception of these kinds of emails. In **ECUADOR**, email recipients can apply the opt-in or opt-out rules in order to accept or reject the reception of data messages that are sent for advertising goods and services of any kind periodically. These messages must contain full information of the email sender and a mechanism to opt-in/out. **COLOMBIA** [Bill], **BRAZIL** [Bill], and **PERU** have adopted the opt-out option. **VENEZUELA** and **URUGUAY** do not directly regulate SPAM but some privacy and data protection provisions may be applicable to unsolicited emails. In the **US**, « *the CAN-SPAM Act mandates certain disclosures, including: clear and conspicuous identification that the message is an advertisement or solicitation; a valid physical postal address for the sender; and, notice of the opportunity to opt-out from receiving further messages. Marketers shall give recipients a functioning return e-mail address or Internet-based mechanism by which they may do so. The Act prohibits the use of deceptive header information intended to mislead recipients as to the contents or source of a message, e-mail address harvesting, and the fraudulent use of computers for the purposes of sending SPAM*. »[4]

Cases-Law: COLOMBIA: Claimant sued Respondent for sending Spam to his inbox constantly even though claimant had informed Respondent of his will to be taken out of Respondent's mailing list and never receive again information on the products he offered. The Court decided that the respondent did send Spam to Claimant.[6] **JAPAN**: Companies to indemnify an ISP for sending Spam e-mail through its server.[7]

8. APPLICABLE LAW and JURISDICTION

The multi-jurisdictionally feature of the Internet is not a mystery anymore. This notion is now well extended into all continents. As we all know, the cost and speed of message transmission on the Net is almost entirely independent of physical locations thus cyberspace has no territorially based boundaries. No physical jurisdiction has a more compelling claim than any other to attract international transactions exclusively to its laws. In consequence, this fact raises problems to identify the jurisdiction applicable to electronic transactions including many cross-border transactions and the law to be applied to the contract. Jurisdiction raises the question of which national court or arbitral tribunal will hear the dispute and the Applicable Law raises the question of which country's rules and regulation should apply to the contractual relationship.

Precedents have established a way of identifying the applicable jurisdiction to international operations where the parties did not choose it (e.g. passive and active website). However, these decisions have not solved the uncertainty in the trade relationship. International conventions have established internationally harmonized standards in order to establish the applicable law and jurisdiction to a contract where nothing is

[6] Juzgado Segundo Promiscuo Municipal Rovira Tolima. 21 July 2003. Juan Carlos Samper V. Jaime Tapias, VIRTUAL CARD. Rad. 73-624-40-89-002-2003-053-00 (Alfa-Redi source)

[7] Tokyo 2003. NTT DoCoMo Corp. V. Unknown (Perkins Coie)

said but these contracts were drafted for traditional transactions. (e.g. Rome, Brussels, Lugano, and Hague Conventions; the UN Convention on contracts for international sale of goods; the UNIDROIT principles of international commercial contracts)

Legislation should ensure certainty on the applicable jurisdiction. But more importantly, businesses shall notify customers of the relevant jurisdiction and applicable law to the electronic contract they conclude. Moreover, in international trade, it is highly recommended to promote arbitration as dispute resolution mechanism, preferably online, instead of appointing a national jurisdiction. These mechanisms could be based on the UNITAR Alternative Dispute Resolution Methods; the UNCITRAL International Commercial Arbitration and Conciliation rules; or WIPO's Arbitration and Mediation Center.

National Legal Framework: VENEZUELA: Whoever commits a cyber-crime, established by law, outside the Venezuelan territory causing its effects inside the territory can be judged by Venezuelan criminal courts, if he/she had not been judged for the same crimes abroad or has evaded the judgment of foreign tribunals. **ECUADOR**: The parties to an e-contract can mutually agree of the terms and conditions to rule their relationship, in particular, they can choose the forum or jurisdiction for any dispute that may arise from the performance of the contract. If they did not agree on any jurisdiction the issue will be solved by the Civil Procedural Code, except in those cases where a consumer is party to the contract. In such cases, the courts of the place of permanent residence of the consumer will constitute the right forum. The parties could also choose arbitration as the mean to solve their controversies. The arbitration could take place through the use of electronic means.

Cases-Law: **ITALY**: An actress sued the author of a defaming article, published through a newsgroup, in the place of her residence alleging that the damages were caused there (Lecce). The Supreme Court decided that the Tribunal in Lecce was competent to hear the case on the grounds that Lecce was the place where the actress suffered moral and economic damages due to the defamatory article. **AUSTRALIA**: A person allegedly defamed over the Internet had the right to protect his or her reputation in the place where the web article was published.[8] **FRANCE**: The Court stipulated that the jurisdiction to hear of a crime was the one of the permanent residence of the defendant, in criminal cases committed online, while the court to hear of any disputes raised within a contractual relationship is the one of the place where the contract was performed.[9] **USA**: The Plaintiff, a nationally known public figure who resided in Virginia, sued a non-resident for defamation and violation of the Anticybersquatter Consumer Protection Act as a result of critical statements the defendant made on a website he operated at a URL bearing the plaintiff's name. Finding that defendant had not, by his activity, expressly targeted a Virginia audience, the court dismissed the suit for lack of personal jurisdiction.[10]

9. ELECTRONIC CONTRACTS & DOCUMENTS AND DATA MESSAGES

On-line transactions continue to be a source of revenues however some obstacles keep restricting the possibility of concluding valid and recognizable online cross-border contracts. The use of e-commerce still raises a number of issues, which might better be addressed through contractual processes "*à defaut de*" legislation and precedents providing certainty, validity and legal effects to any e-contractual relationship.

Difficulties are encountered to determine: a) the moment when and offer has been accepted or when a counteroffer has or not been accepted; b) the applicable law and a jurisdiction to a contractual relationship if the parties did not agree on any; c) the moment where reception/delivery of data messages take place and when the data message is considered as sent; and d) who are the parties to a transaction and the place of its conclusion. It is also unpredictable whether a) data messages are intercepted by third parties because of a lack of security; b) the transaction will encounters physical or automated errors; and c) the electronic communication and data storage will be granted recognition and legal effects. Distribution problems, like in traditional contractual relationships, and payments bottlenecks could also be a source of conflicts. Unexpected troubles may also appear in online auctions, Click-Wrap Agreements and incorporated contract terms.

There is an urgent need to enact legislation to ensure the legitimacy and enforceability of e-commerce contracts and ensure contracts made and signed electronically have the same force in law, as when they have been made and signed via the traditional means. Laws providing clear guidelines on the admissibility and evidential weight of electronic records are required.

National Legal Framework: Digital documents are considered as to be in writing in **ARGENTINA**. In **CHILE** this requirement will be satisfied by documents and contracts electronically signed [with some exceptions]. In **VENEZUELA** and **COSTA RICA** [Bill], documents and contracts digitally signed will be considered as to be in writing. **BOLIVIA**, **GUATEMALA** [Bill], **ECUADOR** and **COLOMBIA** consider data messages as to be in writing if they can be consulted *a posteriori*. For **PANAMA**, electronic acts and contracts that could be subsequently consulted are in writing. In **EL SALVADOR**, electronic documents related to merchandise are considered as to be in writing and possess evidential weight. Moreover, electronic documents and contracts digitally signed and digitally supported by any mean are considered originals and have evidential weight in **ARGENTINA and GUATEMALA** [Bill] (if proven integrity and consultable a posteriori). In **CHILE**, all electronic documents and contracts are considered originals and those digitally signed have evidential weight (as data messages in **COLOMBIA**). In **ECUADOR**, **PANAMA, PERU, BOLIVIA** [Bill] and **BRAZIL** the evidential weight and the condition of "original" is provided to any electronic documents or contracts and data messages. The evidential weight and the condition of an original document or contract, in **MEXICO**, will depend on whether the information transmitted through electronic means could be consulted *a posteriori* and its integrity be demonstrated. In **VENEZUELA**, data message have the same evidential weight granted to traditional documents. Countries like **ECUADOR, EL SALVADOR, COSTA RICA** [Bill], **PERU, BRAZIL, ARGENTINA, MEXICO, VENEZUELA** and **URUGUAY** allow official documents and acts to be produced and transmitted electronically. The provisions cited under Items 8 to 10 were in part inspired by the UNCITRAL Model Law on e-Commerce. For Items 8 and 9, watch out the UNCITRAL Draft Convention on the use of electronic communications in

[8] Victorian Supreme Court.

[9] Paris Court of Appeal. March 7th, 2001.

[10] W.D.Va., March 4, 2003 Jerry L. Falwell V. Gary Cohn and God.Info. Civ. Act. No. 6-02CV0040 (Phillips Nizer source)

international contracts and the ICC eTerms and ICC Guide to electronic contracting

Case-Law: **GERMANY**: The court held that the e-mail printouts produced by claimant had no value as evidence, as ordinary electronic mails can be easily altered or forged. **USA**: A United States District Court concluded that a license agreement concluded through the Internet is a written agreement as from the moment it is printable and storable and license conditions where notified before the conclusions of the agreement.

10. DIGITAL SIGNATURES

One of the techniques available to confirm the integrity and authenticity of a data message is the digital signature and its cryptographic technology. Digital signatures are the most secure technology to digitally sign a data message. Digital signatures allow signatories to be identified by the recipients through the intervention of a trusted third party i.e. Certification Authorities.

In order to reduce the barriers for the adoption and full acceptance of digital signatures it is a mandatory requirement for governments to update their legal texts with regard to traditional writings and handwritten signatures. They should also draft regulations stating that digital signatures have the same validity as handwritten signatures and that documents digitally signed have evidential weight. Further, there should be a political will to recognize the services of certification providers/authorities and provide legal effects to digital certificates as mentioned in Item 10.

States should promote the adoption of a digital certificate by any citizen interested in the use of e-Administration tools and the conclusion of e-transactions. This service should be encouraged, promoted and subsided by governments. Businesses, when dealing with e-Administration services, electronic communication and transactions should be required to have digital certificates.

National Legal Framework: A digital signature is equivalent to a hand-written signature with regard to its validity and legal effects in **GUATEMALA** [Bill], **COSTA RICA** [Bill], **ARGENTINA, NICARAGUA** [Bill], **COLOMBIA, PERU, VENEZUELA, PANAMA** and **BRAZIL**. An electronic signature is equivalent to a hand-written signature with regard to its validity and legal effects in **BRAZIL, ECUADOR, VENEZUELA, PERU, PANAMA** and **CHILE**. Further, in **URUGUAY**, **VENEZUELA** and **NICARAGUA** [Bill] digital signatures are granted the same evidential weight as handwritten signatures. In **PANAMA**, electronic signatures are given the same evidential weight as handwritten ones and in **NICARAGUA** [Bill] and **URUGUAY** these types of signatures could be submitted as evidence into a court. In countries such as **URUGUAY**, digital and electronic signatures are allowed among officials. Many of these legal texts adopted provisions of the UNCITRAL Model Law on electronic signatures.

Case-Law: **USA**: A Court of Appeals concluded that no electronic or digital signature was needed in this case in order to fulfill the signature's requirement and therefore to provide written consent on a particular transaction another one concluded that neither the common law nor the Uniform Commercial Code requires a hand-written signature, even though such a signature is better evidence of identity than a typed one.

11. DIGITAL CERTIFICATION AND CERTIFICATION AUTHORITIES

Both businesses and consumers must be assured of security and safety in cyberspace transactions and the most important tool that can be used to protect people is the use of encryption. It is a technique that can turn your message into "gibberish", readable only by the person intended to read the message -- someone who has the proper key.

Digital signatures allow signatories to be identified by recipients through the intervention of a trusted third party i.e. Certification Authorities (CAs). The CA creates a digital identification certificate, which establishes a link between the person of the signatory and his/her pair of keys (public and private keys). In order for this to work, States should regulate certification and CAs and provide the legal basis for accrediting certification service providers. It is also important to include the mutual homologation and recognition of foreign digital certificates when comprising the same requirements as the national certificate.

National Legal Framework: **COSTA RICA** [Bill], **NICARAGUA** [Bill], **VENEZUELA** (with some particular provisions with regard to the reciprocal recognition of foreign digital certificates), **PANAMA, URUGUAY, MEXICO, ARGENTINA, ECUADOR, COLOMBIA, CHILE and PERU** have adopted legal instruments to regulate certification authorities, digital certification and mutual recognition of foreign digital certificates. I have a doubt with regard to crossed recognition of digital certificates in **BRAZIL** and **GUATEMALA** [Bill].

Examples of Certification Authorities in Latin America: ARGENTINA: Certificado Digital S.A., Aptix y SECAPH. **COLOMBIA**: CertiCamaras. **BRAZIL:** CertiSign. **CHILE**: e-CertChile y Cámara Nacional de Comercio, Servicios y Turismo (CNC). **URUGUAY**: ID-Digital y Cámara Nacional de Comercio y Servicios del Uruguay. **PERU:** Peru Secure E Net. **GUATEMALA:** Bancared. **ARGENTINA** y **CHILE:** CertiSur (Clerk's digital certification)

12. REMARKS and RECOMMENDATIONS

We found it very difficult to decipher on the Net what are the Acts in force in each Latin-American country and which laws are under review. The Net lacks of concentrated, complete and accurate information when it comes to legislations. Hyperlinks are never kept for a long period of time, causing prejudices to researchers and tripling the search-work previously undertaken. Websites are not always up to date and, in some cases, the legal instruments published as part of the current legal framework of a country are abolished by a more recent Law or Decree.

We noticed that Latin-American countries do not use the same vocabulary for equal legal texts. Digital and electronic signatures are used with an unclear understanding, which, ones interpreted by judges of different jurisdictions, might produce unexpected judicial precedents. It is regrettable, that most of the judicial precedents be originated in the European and Asia-Pacific regions and the USA. COLOMBIA and ARGENTINA's courts are leading in Latin America with regard to new technologies.

We remarked there are several certification service providers in the region for such a small demand. Still Today, citizens (not specialized in this domain) ignore what are digital signatures, what are they used for, where can they be obtained or what are the certificate's support (e.g. smart cards, or tokens).

Out of some 21 Latin American countries, we found legal texts for online consumers protection in six countries; for online privacy and data protection in eight; for copyright in 18 (good score); for cyber-crime in 15; for Spam in six; for child's pornography in four; for e-contracts and documents and data messages in 15; for e-signatures in 12 and for digital certification in 13 countries. The results talk by themselves and it should be noted that some of the texts are not yet in force. Policy and decision makers should recognize the imperative need for domestic policies in line with other countries' legal framework and international market trends aimed at creating a proper legal atmosphere under which e-commerce, e-health, e-learning and e-government tools could flourish in order for the region to derive the full benefits from information technologies. Our legislative framework should be friendly and internationally acceptable.

General principals for the region should be drafted on the following grounds: recognition of electronic signatures and digital signatures, recognition of electronic documents and contracts, freedom of contract, intellectual property protection, consumer's protection, privacy and data protection, fighting against cyber-crime (and pornography, SPAM, etc), encouraging alternative dispute resolutions (preferably online), use of digital certificates, mutual recognition of foreign digital certificates, and technology neutrality, among others. New rules and regulations for securing electronic transactions should be technology-neutral and flexible.

An understanding of the technology is needed to regulate computer information system content and system operator liability. Thus, lawyers should stop drafting legislation without the assistance of computer engineers and vice versa.

13. REFERENCES

[1] SKADDEN. Top 10 Information Technology Legal Developments in 2003. February 12th, 2004.
[2] Norton Rose Newsletter. December 2003.
[3] Murielle Cahen Newsletter. June 2004.
[4] Jones Day Commentaries. February 2004.