ITechLaw interview

One of the fastest growing areas in the Law of this new millennium is the one concerning technology. Issues arising from the Internet and new relationships originating from digital media impose a huge challenge to both judges and lawmakers. To discuss these new challenges and try to answer some of the questions born from the clash of Law with Technology, the Brazilian news website Consultor Jurídico has interviewed a group of specialists from the International Technology Law Association (ITechLaw), an organization created in 1971 which gathers lawyers working in the technology sector all over the world. The questions were posed to ITechLaw by the international correspondent Aline Pinheiro and were answered by eleven experts from the association who, together, aggregate the knowledge to talk confidently about e-commerce, arbitration, data protection, social media and other matters in the current globalized scenery. The interview was made in English and translated to Portuguese for the convenience of ConJur's readers. Here is the English original.

ConJur – Which are the most challenging issues the Internet brings to law? How can they be dealt with?

ITechLaw – The Internet has created several challenges as it relates to the law, but two of the most challenging pertain to the uncertain jurisdictional issues created by the Internet and the undeveloped legal precedent caused by emerging Internet law issues.

The Internet, by its very nature, is global. As such, its use raises issues, among which some of the most important are: which jurisdiction's laws apply, when does a user subject herself to jurisdiction in a foreign country, and if foreign jurisdictions will enforce other foreign jurisdictions' laws in the same way. These become particularly applicable when an Internet Service Provider (ISP) is located in one jurisdiction and the user is located in another. It is difficult to find counsel that is versed in the laws that may apply throughout various jurisdictions. Website agreements and other

contracts governing the relationship between ISPs and users can provide insight into how these particular issues are resolved. Use of counsel with expertise in more than one jurisdiction, especially if conducting business in more than one jurisdiction, is becoming extremely important. Thus, businesses and individuals alike should understand which activities may subject them to liability in a foreign jurisdiction.

While the Internet has provided a new forum in which legal disputes may arise, traditional legal principles oftentimes apply. Statutes are regularly being introduced that address particular Internet laws, such as those related to data security breaches or online endorsements and testimonials. In addition, cases are regularly being decided that shape the jurisprudence as it relates to certain Internet-based disputes, such as whether use of keywords may amount to actionable trademark infringement. New issues are constantly emerging as a result of the Internet. Such issues may relate to substantive laws as well as ethical considerations for attorneys. The uncertainty with which such novel issues are to be resolved is the cause of much concern for attorneys and clients alike. In order to deal with the uncertainty, businesses are being forced to expend resources on legal opinions that may be speculative rather than based upon established precedent or law. However, the exercise of good faith in making such business decisions, coupled with the ability to adapt to the ever-changing legal landscape of the Internet, should be the goal.

Ultimately, we can all agree that the Internet is not going away. Instead, its use is ever-expanding, as evidenced by the explosion of social media and the associated legal issues. Therefore attorneys and businesses alike that can remain educated about and advised of, respectively, the ever-changing legal landscape, will remain in the best position to deal with what may come next.

ConJur – The Internet being a worldwide network, it reaches everywhere. Is it possible to regulate it? How?

ITechLaw – The Internet involves different forms of regulation, mainly a patchwork of legal measures. General national laws may apply to illicit actions committed on or with the help of the Internet but that have nothing

specific to the Internet: commercial and financial crimes, invasion of privacy, etc. But specific laws have been necessary to deal with Internet issues: liability and obligations of Internet providers, attacks on security systems, piracy, etc. These must work alongside legal rules that determine when the laws of a particular country will apply to an Internet-related issue. There are inherent limits to national laws, which are insufficient to regulate the Internet as the Internet does not have borders. International instruments had to be developed: treaties, customs cooperation, and rules developed by regional/international institutions (such as the WIPO for IP rights, in particular in relation to domain names). Some institutions like the Internet Corporation for Assigned Names and Numbers (ICANN) or Internet Assigned Numbers Authority (IANA) were created to meet the specific needs of a worldwide Internet regarding domain names and IP addresses. Other institutions may also offer alternative dispute resolution procedures, like the WIPO and its UDRP procedures for generic top-level domains. Legislation is not always the answer. Private actors (mainly corporations and associations) also play a significant role in regulating the Internet, by adopting voluntary codes of conduct and charters, and by entering into bilateral agreements. Good examples of self-regulation are the agreements that intellectual property right holders may enter into with marketplace websites or online payment service providers so as to regulate counterfeiting. If necessary, these private actors may also use technical measures to block access to content, and thus limit the risks of counterfeiting.

ConJur – Is it possible and desirable to have an international law or should each country have its own?

ITechLaw – This purpose is more desirable than possible. Given that the Internet is international, we should have an international legal frame. This has been argued in reputable international forums in the late 1990s. The result was the UNCITRAL E-commerce Model Act in 1996 as universal frame regulating the main aspects of e-commerce contracts and documents. The UNCITRAL E-commerce Model Act has been considered worldwide for developing regulations in each jurisdiction. However, this was not enough and in practice each country actually developed its own

regulations.
On the other hand, regulation of e-commerce contractual issues is just one aspect of international Internet law. Other technology contracts, IP issues, and data protection have largely been deferred to each jurisdiction. In the EU, many of these laws are harmonized, but it has been left to individual EU states to apply and interpret the provisions, often resulting in divergent decisions as well as extensive delays while the European Court of Justice (CJEU) determines issues of interpretation. Decisions of the CJEU are often difficult to apply in practice, as they leave it up to national courts to apply the law to the facts of the case. This highlights the difficulties of developing effective international laws.
Thus, to answer the question directly, although it is desirable to have an international law, it will never be entirely possible to achieve this effectively.

ConJur – If each country has its own rules for the Internet, which national law should one court use to rule disputes for international cases? For instance, when an entity from one country hosts its website in another and commits an offense on the Internet?
ITechLaw – When a signed contract governs the relationship between entities from different countries it is usual to submit the effects of the contract to one national law. In such case it is advisable to submit the disputes related to the contract either to arbitration or mediation. Arbitration is the best means to resolve a dispute in a reasonable timeframe, wherein the award issued by the independent arbitrator/arbitrators is then directly enforceable by the parties involved according to the New York Convention.
As regards the application of national regulatory requirements, some jurisdictions have found that the law where the server is located governs. Others apply the law where the breach or offense has occurred. The difficulty in the latter case of course is the impracticality of complying with multiple different laws. The application of these principles should also differ according to whether the website was actively directed at a particular country, as opposed to merely being accessible there.

ConJur – Apple has been filing law suits against Samsung all over the world and in each country results are different. How should this situation be dealt with, different decisions on same issues, involving the same parties, but in different countries?

ITechLaw – We would disagree that the decisions arise from the same issues or that the results are necessarily in conflict. For the most part, intellectual property rights are national rights and are to be interpreted according to the national law of the place where the alleged infringement occurs. This is particularly the case in relation to patents. The ability to bring proceedings in different countries can confer tactical advantages, and the potential cost and liabilities can act as a deterrent to litigation. If the enforcement of intellectual property in multiple countries becomes easier and cheaper, this might benefit relatively small companies with respect to the cost of enforcement, but equally may benefit so-called patent "trolls" seeking to enforce patent rights that they have acquired from third parties. Furthermore, if enforcement is to be dealt with multi-nationally then validity must be as well, which means the risk of losing one's intellectual property entirely in a single blow as a result of one decision. Many would see this as highly undesirable.

Proposals exist in the EU to introduce a single EU patent and a unified patent litigation system. These proposals have been heavily criticized, first because they introduce the German "bifurcation" system, which makes it very easy to obtain injunctions on the basis of invalid patent rights. Secondly, the proposals will for the first time bring European patent law within the jurisdiction of the CJEU for decisions on interpretation of the new EU-wide legal provisions. This latter point is likely to introduce severe delay into the resolution of patent disputes, based on experience in the EU with trademark and copyright cases. In the meantime it is possible to obtain a cross-border preliminary injunction in patent cases under certain conditions, notably from the Dutch courts.

As to the broader question of a uniform system to resolve disputes concerning e-commerce, major state actors are for the moment reluctant to achieve uniformity in the regulation of the Internet and in the resolution of Internet disputes. The issue should be addressed by governments through international institutions, such as UNCITRAL and WIPO, pressing countries

and the entities in each country to accept the submission to an international regulation and arbitration system.
It would be of interest to create an international court of arbitration focused on the Internet, IT and Telecoms sectors, with appropriate arbitrators experienced in the Internet and technology world. Otherwise, conflicting situations will continue creating a patchwork of global dispute resolution.
For the moment, disputes between parties on IP matters, and others without a prior contract, only could be addressed to arbitration if both parties accept it. This is difficult in practice and in each jurisdiction the affected entity who envisages a bad result very much prefers the domestic judge for solving such conflict, expecting a better decision than would be expected from the arbitrator.

ConJur – In the digital world, one may share any content, such as music and film, with one's friends without any profit interest. Should that be considered piracy?
ITechLaw – Copyright law varies around the world. In the U.S., copyright owners have certain exclusive rights, including the exclusive right to copy and redistribute the copyrighted material. Copying or redistributing content without authorization constitutes infringement unless an exception applies. One exception is "fair use." One of the factors in determining fair use is the effect of the use upon the potential market. For content owners, one of the problems with enabling users to share with friends is that some users have many "friends." In fact, in this age of social media, many people have many hundreds or thousands of connections through their social networks. A single share of a song by one person could reach over a thousand people. If each recipient shares with just a few hundred of their friends, there can quickly be over a million copies shared. This is quite likely to have an adverse effect upon the potential market for the song. Even if the users who share the content do not profit, there are adverse consequences for the content owners. Even if a user only sends several copies to friends, the network effect has the potential to divest the content owners of potential profit. Moreover, trying to carve out a specific variable amount of "how many is too many" is a challenge. For at least these reasons, most content

owners would strongly argue that this is piracy. In contrast, content users would argue that to interpret the scope of fair use too narrowly is to effectively render the right ineffective. Each jurisdiction is still endeavoring to find the right balance between these two sets of rights.

ConJur – Should digital piracy be dealt with in a different way than traditional content piracy?
ITechLaw – When it comes to digital content, piracy is actually easier. There are differences in how piracy is policed due to the distributed nature of digital piracy (multiple users sharing with other users vs. one company making physical copies with expensive copying machinery). But from a legal perspective unauthorized copying of digital content (absent an applicable exception) should be dealt with in the same way as with traditional content. The problem is matching this legal notion to the expectations of consumers, when the reality is that friends and family will always share music and other content, believing this to be legitimate. The European approach is different, but has not been without problems. In most EU countries, legislation permits "friends and family" to make copies for personal use, and right holders are compensated through levy schemes (or occasionally, state compensation schemes). However, the levies can significantly increase the retail price of equipment as well as recording media, and the system has led to an endless string of disputes as eager collecting societies claim levies on an ever-wider range of equipment, in many cases despite the equipment being sold mainly for business use, or its primary purpose having nothing to do with reproduction of copyright material. In turn this has led to the need for the CJEU to resolve disputes and clarify the permitted extent of the levy concept under EU law. The levy system has thus been strongly criticized as arbitrary, inconsistent, unfair and opaque, but repeated attempts to improve it have failed. The UK is one of the few EU states committed to shunning any sort of levy system, but it in turn is now grappling with how to introduce a private copying exemption that is fair to both right holders and users, whilst reflecting the reality that private copying on a small scale cannot realistically be prevented. UK legislation on this is expected soon.

ConJur – Should Internet access providers be responsible for supervising what Internet users do using their services?
ITechLaw – At its inception, an Internet access provider was merely responsible for providing access to the Internet to users. However, over the

last decade, with the growth of the role of the Internet in global integration, the duties and responsibilities of all parties associated with the Internet have increased manifold. With easy access to content over the Internet as a source of information, such content may be used by vested parties to cause detrimental effects on society. For example, recently in India, circulation of mass emails, as well as content being posted on social media forums, informed members of a certain ethnic community that they would be subject to acts of aggression. Consequently, this resulted in mass exodus of the community members. Upon investigation, it was established that the mass emails, as well as the content that was uploaded, were based on mere rumors circulated by miscreants.

An Internet access provider is now expected to step out of its traditional role of being a mere service provider and assume a diverse role, which includes being responsible for content being uploaded on its platform. Most jurisdictions do not impose an explicit statutory duty upon an Internet access provider to supervise content. However, the Internet access provider is expected to use its discretion to undertake reasonable steps to ensure the quality and nature of the content being published or hosted by its users. In this regard, an Internet access provider should take due steps of diligence and exercise abundant caution to ensure that the platform is not being misused by the users to the knowledge of the ISP. That said, it would usually not be prudent for an ISP to adopt a universal monitoring policy, which would render it more likely to be held liable for content. Relevant problematic content could include content alleged to be blasphemous, defamatory, obscene, pornographic, pedophilic, invasive of another's privacy, hateful, or racially and ethnically objectionable. More broadly, ISPs are often involved in disputes about infringement of copyright. While an Internet access provider should not be made expressly liable for not supervising what Internet users do using their services, there should be an onus cast upon an Internet access provider to ensure that the platform is not knowingly misused. As a good practice, the Internet access provider must have an effective mechanism in place to promptly remove any such content, upon receiving notice of the same.

Based on the above, while it is not recommended for Internet access providers to undertake stringent monitoring duties, a stance of complete dissociation with the content being uploaded onto the Internet (via its platform) is also not recommended. Ideally Internet access providers should adopt a middle path wherein, while not strictly supervising all content being handled by users, it does take reasonable measures to act when notified, and imposes clear policies on users. So, while an express

response to the query is no, an Internet access provider should not be responsible for the actions of its users, this exemption should only be applicable if the Internet access provider has either acted responsibly or exercised due care and diligence in providing the platform.

ConJur – How should privacy be balanced with the duty to fight online criminal offenses? Should Internet access providers be bound to keep and give potential evidence of crime upon request?
ITechLaw – The crux of the balance between the duty to fight online criminal offences and concerns about privacy lies in the interpretation of the notion of “reasonable expectation of privacy”. It is essentially two elements that contribute to this expectation: an effort must be made to keep something private, and society must agree that it should be private in the circumstances.
Due to the fluid and global nature of the Internet, in order to be able to prevent criminal acts online and identify culprits of a cyber offence, there must be a reasonable tradeoff between individual privacy and criminal enforcement, by putting obligations on service providers to identify perpetrators of a criminal act online when requested, and retain for a reasonable time limit, or as per directions of the court, relevant electronic evidence so as to be able to bring to justice the perpetrators of criminal offences.
Two practical issues arise: first, the cost of administering such procedures, including the cost of physical storage, which should be borne fairly. Secondly, it is important that innocent individuals are not wrongly accused, and involved in investigations or prosecutions, as a result of incorrect data being supplied to law enforcement agencies by ISPs. The use of innocent individuals’ PCs in "botnets" is an example of criminal misuse of computer networks, of which ISPs and law enforcement agencies must remain aware and fully informed so as to target the true criminals.

ConJur – Anything that is put into the Web may be accessible forever. If someone is charged with any offence, even if afterwards acquitted, news about his charge might be accessible to everyone indefinitely. How to deal with freedom of expression and protect one’s reputation?
ITechLaw – The right to freedom of expression carries with it duties and responsibilities necessary in a democratic society, for the protection of the reputation and rights of others, for preventing the disclosure of information received in confidence, and for maintaining the authority and impartiality of the Judiciary. The laws of defamation apply to the Internet, and website

owners and ISPs have a role to play in removing content notified to them as being allegedly defamatory. If necessary, courts can be asked to intervene. One might add that if it is easy for news of a criminal charge to proliferate, then individuals also have at their disposal ready means of disseminating the news of an acquittal.
A more subtle point concerns implementation of data privacy principles to the online world, in particular within social media. The proliferation of data that may be inaccurate, and the difficulty of erasing or correcting it, has led EU authorities, for example, to propose a "right to be forgotten," enforceable in law *[if such proposal were implemented, people would have the right to request that information related to themselves be deleted].*

ConJur – How can the technology help Justice?
ITechLaw – Technology can help Justice by making the court system more accessible, more efficient and quicker. A court system allowing judges, court staff, lawyers and citizens to access, exchange and file documents and information in a networked environment increases transparency and avoids costly physical movement of persons and files. This saves time and can undoubtedly contribute to reduce the court backlogs. Although the initial financial investment can be very high, the use of technology can allow Justice to cut budgets in the middle or on the long term. Fewer people will be necessary to “shuffle papers,” and judges will be able to focus more on their core task, i.e., rendering judgments. Technology also facilitates accessing and sharing legal expertise. With the Internet, legal rules and free legal advice are nearby and easy to access for any person. The Internet also allows the distribution and sharing of new case law, insights and legal developments on a worldwide scale and at the speed of light. This is in a way a kind of democratization of law. Many jurisdictions have adopted or are adopting technology in their legal systems, such as Brazil and Belgium. The cost of such progress and the lack of training of court staff are often the most important obstacles to the introduction or rollout of technology in Justice.

ConJur – The United Kingdom has been implementing virtual courts. What is your opinion about it?
ITechLaw – Both courts of justice and arbitration tribunals should use technology in hearings, including secure videoconference systems that

ensure that confidentiality and privacy of the parties and the case are maintained. So-called virtual courts have been introduced, for example in the early stages of criminal proceedings, and can clearly bring cost savings and efficiencies. However, in major trials we foresee significant obstacles, not least that the judicial process should be entirely open to public access. Furthermore, the concept of virtual courts at any stage of proceedings has been criticized as obstructing the defendants' access to their lawyers during proceedings, and imposing constraints on defendants arising from the environment from which they are forced to participate in the video link (for example, they may be seated in a police station). On the other hand, lengthy in-person proceedings are not always necessary in civil proceedings between experienced business parties, provided that a need for cross-examination of witnesses does not arise in the particular case.