Developing an Autonomous and Interdisciplinary Teaching of Cyberlaw in Argentinean Universities

Patricio Alan Zermo Dopico
University of Buenos Aires (UBA)
Universidad Argentina de la Empresa (UADE)
Institute of Social Sciences and Project Disciplines (INSOD)
National Scientific and Technological Research Council (CONICET)

The conceptualizations that doctrine has elaborated on cyberlaw have a visible interrelation between two disciplines: law and computer science. For this reason, this paper proposes to provide a foundation on the importance of teaching its contents at the university level in an autonomous method: encompassing them in a single course, and interdisciplinary; analyzing the information and communication technologies that underlie the legal regulation. To this end, we will examine the curriculum of the subject of Computer Law at a university in the Autonomous City of Buenos Aires, and will also inquire about the current status of its inclusion in the curricula of other universities in the district.

Keywords: cyberlaw, university education, cybercrime, Argentine university

INTRODUCTION

The technological advances that have been taking place since the end of the 20th century, especially with the widespread use of electronic devices connected to the Internet by a large part of society, have brought about changes in various aspects of people's daily lives: commerce, education, work, entertainment, interpersonal relations, among others.

The Republic of Argentina is no exception: measurements by the National Institute of Statistics and Census (INDEC) show that in the fourth quarter of 2020, 90% of the country's households had Internet access, while 85.5% of the population uses this network.

Recently, the Covid-19 pandemic and the consequent measures of the Preventive and Compulsory Social Isolation (ASPO) dictated by the national government for the years 2020 and 2021, have forced or accelerated exponentially, depending on the case, the need to use IT tools to carry out activities that until now did not necessarily require it. Examples range from operating the bank account via home banking to communicating with loved ones through video calls using smartphones.

The lack of education and training in the use of information and communication technologies (hereinafter: ICT) has led to certain social sectors being forced to immerse themselves in a world that is totally unknown to them. It is no coincidence that certain cybercrimes such as computer fraud in its phishing version have increased during the quarantine.

It is clear that the increase in the use of devices connected to the Internet is bringing with it new situations and consequences that the law must protect, not only in the field of criminal law, but also in civil,

commercial and even labor law, making it imperative to review all these new technologies from a legal point of view.

The main questions that arise from this situation and which this paper seeks to answer are: How should future legal practitioners be prepared in their undergraduate careers to deal with these situations? Is it effective to teach Cyberlaw in an autonomous way or could its contents be included in other subjects? Is an interdisciplinary perspective with computer sciences necessary in these courses?

In order to address these questions, this paper aims to analyze the curriculum of the subject Computer and Intellectual Property Law at the Universidad Argentina de la Empresa (UADE), located in the Autonomous City of Buenos Aires (hereinafter: CABA), with special emphasis on the interdisciplinary teaching of legal and computer science contents in order to ensure satisfactory learning.

At the same time, we seek to examine comparatively the curriculum of the law degree in universities in the CABA to determine how many of them currently teach a subject that brings together all these topics.

THE CONCEPT OF CYBERLAW

Cyberlaw is defined by Altmark and Molina Quiroga as a "modern and thriving legal discipline that, with a research methodology whose factual presupposition is precisely IT in its diverse and increasingly complex applications, analyzes the phenomenon of the impact of IT on society, identifies the new problems and questions that such impact causes, and advocates the development of appropriate legal responses to the new phenomenon".

Fernandez Delpech conceptualizes it as "the set of principles and rules that regulate the legal effects born from the interrelation between law and informatics."

Within the Mexican academy, Julio Téllez Valdés defines cyberlaw as: "a branch of the legal sciences that considers computer science as an instrument (Legal Informatics) and an object of study (Computer Law)".

As can be seen, all the above definitions emphasize the interdisciplinary nature of law and computer science. If one were to approach the subject only from a legal perspective, one would end up isolating the disciplines in relation to the issues that link them together.

On the contrary, an interdisciplinary approach implies exchange and cooperation between them. Even in this case, since there is a high degree of dependence, one could speak of pluridisciplinarity: associating the two disciplines by virtue of a common object.

In this sense, Pascal has already stated in 1669: "...the parts of the world have such a relationship and such a concatenation with each other, that I think it is impossible to know one without the other and without the whole".

The aforementioned interdisciplinarity is not specific to cyberlaw, it can be observed in other branches such as environmental law, where it is desirable that the professional has knowledge of environmental sciences; in family law where knowledge of psychology or anthropology would be desirable. Even knowledge of history or specifically Roman law for any branch in which the profession is practiced is of utmost importance, it is no coincidence that the latter subject is taught in most Argentine universities.

Returning to the discipline of analysis, it should also be mentioned that there is not only a strong interrelation between law and cyberlaw, but also between cyberlaw and the rest of the branches of law, a situation that is increasing as ICT invade more aspects of people’s lives, as explained in the introductory section.

This creates as a problem the difficulty of delimiting the field of knowledge of cyberlaw, separating it from the other branches, a situation similar to what Salt says regarding the conceptualization of cybercrimes: "the concept of cybercrime encompasses a set of behaviors of different characteristics that affect various legal assets and that are only grouped under this concept because of their relationship with the computer. This broadness of the concept determines that for the purposes of legal analysis it is an empty concept, without its own content, which can only be acquired with the concrete description of the different conducts it encompasses."

If this discipline is understood as the "set of rules, principles and institutions that regulate the legal relationships arising from computer activity." but at the same time it is argued that today computer activity permeates most activities, it would not be unreasonable to ask: What is the boundary between computer law and the other branches of law?

It should be a mental exercise to think about what activities are carried out through computer media and have or could have potential legal consequences. Nowadays, and after the Covid-19 pandemic, it is simpler to imagine activities that are not carried out through these technologies.

To shed light on this problem, Zamora differentiates between pure and impure cyberlaw. The former alludes to elements that have no parallel with any other branch of law and will necessarily require the technological or computer element, and cannot be dispensed with. In the words of the author: "the figure cannot be subsumed and applied analogically to any known or contained in the framework of civil, commercial, labor, etc. law. [...] that fact that could not be considered unlawful or harmful thirty years ago, for example, due to the non-existence of the means to carry it out".

On the contrary, the impure cyberlaw is the one whose elements have contact with other branches of law and could be applied the regulations of these, giving as an example the spam, which in the past was done through postal mail and today by email.

But the issue is still intricate, since most of the activities that in the past were carried out without the use of ICTs today find a parallelism with their use: handwritten signature-digital signature; traditional contract-electronic contract; work-telework; crimes against copyrights-cybercrimes against copyrights, among others.

Some specific cybercrimes such as illegitimate access to computer systems (Art. 153 bis of the Argentine Criminal Code) or computer damage (Art. 183 of the Argentine Criminal Code) could be considered as part of the pure computer law.

For example, in relation to computer damage: although damage to property already existed, the article of the Criminal Code mentioned movable property, immovable property or animals as objects, and computer systems could not be classified in any of these categories, as stated in the Gornstein ruling, prior to the enactment of Law 26.388 on Cybercrime in 2008, which resolved the issue by incorporating systems into the article.

Then, going beyond the question raised above about the limits of the discipline, another problem arises, which has been widely debated in the academy: Does computer law have functional independence from the rest of the branches of law?

Part of the doctrine has been in favor of the negative, arguing that in reality computer law only provides specific solutions to other branches without having its own autonomy.

On the contrary, there are many jurists who argue in favor of its independence based on its own institutes, specific regulation and for having an autonomous field of knowledge.

As early as 1996, when the ICT massification process had become unstoppable, Barriuso Ruiz suggested that the interrelation between computer science and law could possibly give rise to an autonomous branch, and even if this does not happen, studies of these issues should be deepened in each prevailing branch of law.

Although the debate deserves much more depth than that devoted in these pages, it is mentioned because of its relationship with the objective of this paper: to delve into the need to include the subject in the curricula of the law career in an autonomous and independent manner.

Whether one adopts a position for or against the functional independence of computer law, what is undeniable is its close relationship with the contents of computer science.

That is why, as will be analyzed in the following paragraphs, due to the difficulty that the teaching of these subjects separately within other courses would entail for the training of students, it is more efficient to group them within a single subject located at an advanced stage of the career, addressing them all together from an interdisciplinary point of view.

THE CONTENT OF THE SUBJECT AND ITS TEACHING IN THE UNIVERSITIES OF THE AUTONOMOUS CITY OF BUENOS AIRES

In order to analyze the current state of the situation in the CABA, the curricula of the fifteen public and private universities where law degrees are taught were surveyed. From the results obtained, it can be seen that only in four of them is the subject of Computer Law or similar denomination stipulated as mandatory in their curricula; being optional or not included at all in the rest of the houses of study.

The name varies in all of them: Computer and Intellectual Property Law (UADE); New Technologies Law (UMSA); Computer and New Technologies Law (UCES); Law and New Technologies (USAL).

It is observed in the survey that only 25% of the universities include the subject in their curriculum as mandatory, without prejudice that the rest may or may not teach the contents in other subjects, for example: cybercrimes within the subject Criminal Law; computer contracts within Contracts; digital signature in Civil Law 1; etc.

As already mentioned, the non-implementation of a specific subject has a main shortcoming: the difficulty of teaching these contents without an interdisciplinary approach with computer sciences, something that will be more orderly and practical for the student if all the topics are grouped in a single subject..

At the same time, it should also be emphasized that there is a risk that some of these contents will not be covered during the course because they are not included in any other course.

The program of the subject Cyberlaw that will be analyzed in the following sections includes among its contents: legal protection of software; domain names; liability of intermediaries on the Internet, right to privacy, honor, image and freedom of expression on the Internet; protection of personal data; information self-determination; electronic and digital signature; computer and electronic contracts; cybercrimes; among others.

Within the same, all these topics are dealt with during the classes in parallel with the IT concepts of the ICT to which they are related and, at the same time, they are exemplified with very current judicial cases, in the same way as all the university manuals used as compulsory bibliography proceed for their approach.

As a corollary to what has been stated in this section, we quote one of the sentences with which teachers usually start the course each term: "We are not looking for you to finish this subject being computer engineers, but you will see that many of the legal contents are closely related to technical concepts of computer science, so you will have to be introduced to and handle the main concepts of that discipline".

THE NECESSARY INTERDISCIPLINARITY WITH COMPUTER SCIENCE. SPECIFIC ANALYSIS OF THE SUBJECT PROGRAM.

The following sub-chapters will analyze some of the main contents included in the Computer and Intellectual Property Law course at UADE, examining how they are approached during the course and their correlation with computer sciences, raising all the necessary issues that must be explained with respect to these technologies so that the legal concepts are clearly apprehended.

It should be clarified that for the brevity intended in this paper will not be carried out an analysis of all the topics included in the program, but will seek to provide an overview of them, delving more deeply into those that have more correlation with computer science.

The subject is taught during the fourth year of the course and has a four-month duration. The evaluation system consists of two written or oral mid-term exams that take place in the second and fourth month of the course, with the possibility of promotion if the student obtains a grade of seven or higher in both of them.

The structure of the following sections coincides with the order in which the subjects are taught during the four-month period due to their concatenation.

It is possible that some of the contents of the subject may differ in each university, since the elaboration of the program will be at the discretion of the authorities of the university and, as we have seen in the previous paragraphs, it may be difficult to accurately delimit the topics covered by the discipline.

Legal Protection of Software

The first topic included in the program of the subject is of great value for the future operators of the law due to the great development of computer programs that exists nowadays.

Whether the student decides in the future to practice as a lawyer, to work in-house in a technology company or even as a judicial officer, he/she must have a broad knowledge of copyright in relation to software.

The class begins with an introductory debate that again has its origin in computer science: the difference between hardware, software and firmware; as well as their differences in terms of materiality and tangibility.

To enrich the discussion, it is valuable for the student to understand how computer architectures and components evolved, so a short video on the history of computing is shown, which covers from the first computers to current devices.

This is essential for students to understand the arguments behind the doctrinal positions on protecting computer programs through copyrights, patents or the creation of a sui generis right.

Having elucidated the issue of the Argentine legislator's choice of the copyright system in the light of Law No. 25.036 amending Law No. 11.723 on Intellectual Property, as well as the analysis of international treaties and comparative law, we will delve into two central concepts of computer science, which are included in the aforementioned law in its section 1: 'source and object computer program'.

The former is defined by the doctrine as: "that which is written in programming language, which is readable by human beings" as opposed to the object code which "is the language resulting from the conversion of the language of the source code to the language of the machine, which is expressed in binary alphabet and is therefore unintelligible to human beings".

For a law student who has had no contact with this type of concepts throughout his career, it may be complex to transpose these theoretical definitions into practice.

That is why it is enriching for its understanding to show how the source code of a computer program looks like and from there to explain what the programming language, machine, assembler, etc. implies.

Subsequently, the three stages of legal protection of software in the Argentine Republic (Generic, deficient and perfected) are analyzed, which although it has a greater legal content, it ends up having as a basis the aforementioned knowledge of computer science.

From this point on, it will be possible to introduce the student to the difference between proprietary and free software, analyzing within the latter the models of the General Public License (GNU GPL) created by the Free Software Foundation (FSF).

The previous development of computer terms is also crucial for this, since without their understanding it would not be feasible to analyze the so-called "four freedoms", the possibility of releasing and modifying the source code of a computer program, the viral effect, etc.

Finally, the criminal offenses included in sections 71 and 72 of Law 11.723 in relation to software are analyzed through a paradigmatic ruling for the issue in Argentina: Autodesk, Inc.

Taking into account the above, some questions arise in relation to the main topic of the paper: Could a legal professional register a computer program created by his client without being able to correctly identify the source code? Could he correctly defend a person accused of plagiarizing software licensed under the GNU GPL? What would happen if a case of this type is brought before a court and the magistrate does not have this knowledge?

The answers would seem to be negative, as could be noted throughout the sub-section, the teaching of the topics raised in an interdisciplinary way with computer science plays a decisive role for their correct apprehension.

Domain Names

Within the curriculum of the subject, domain names start with a technical introduction, which is necessary to allow students to later analyze the legal nature of domain names, their forms of registration, the rights of their owners and the possible conflicts that may arise, such as cybersquatting and parasitism.

As a trigger for the class, the following questions are usually asked: How does each device known to which other device to send the requested information? For example: if I search for something on Google, how will the search engine know to whom to send the answer back?

Following this, the basic principles of Internet operation are explained, as well as the Domain Name System (DNS) and its relationship with the Open Systems Interconnection (OSI) model, with special emphasis on network layer three and transport layer four, thus including the concepts of networks, IP addresses, etc.

The second aspect to elucidate is the basis and utility behind domain names and their importance in relation to trademark issues. It is necessary to point out that having previously introduced the aforementioned concepts of computer networks, this discussion becomes more fruitful.

At this point the students are the ones who usually answer correctly to the question posed, realizing the importance of domains within the Internet and making it clear that they are replacements of IP addresses in a language that human beings can memorize more easily and can even relate them to a brand, a personal name, a geographical place, among others.

This is exemplified and closes the most computer-intensive part of the class when the teacher enters the IP address of Facebook, Google or some other well-known website in the browser to demonstrate that its content can also be accessed in this way.

From this point on, the legal content begins, discussing with the students the legal nature of domain names: Are they rights in rem, personal rights or a special category? At the same time, the doctrinal arguments that support each position are mentioned.

The next topic addressed in the class is registration and conflict resolution. For this purpose, the concepts of global top-level domain (gTLD) and country code top-level domain (ccTLD) are explained.

For the first case (.com; .net; etc.) the competences of the Internet Corporation for Assigned Names and Numbers (ICANN) are examined, the list of registrars authorized by the organization is shown and finally the procedure before its dispute resolution system is explained in the light of the Uniform Domain Name Dispute Resolution Policy (UDRP) and its attached regulations.

In the case of national domains (.com.ar; .net.ar; etc.) students are shown the website of the Network Information Center of Argentina (NIC.AR) and the search for domain name availability for registration and dispute processing is exemplified.

The competences and history of this public instituion and the various resolutions in force and historical resolutions that regulated on the matter (43/2019, 45/2019, 110/2016, 20/2014, etc.) are explained.

Finally, the procedure for conflict resolution based on resolution 43/2019 of the Legal and Technical Secretariat of the Presidency of the Nation is explained.

The discussion closes the class by discussing the concepts of cybersquatting and parasitism. In turn, two emblematic cases are exemplified: Colegio Público de Abogados de la Capital Federal v. Splix Networks in the orbit of the World Intellectual Property Organization (WIPO) and Freddo of the local justice system.

Could this type of discussion be introduced to students without first explaining to them the role of domain names in the functioning of the Internet? And even more important: Could the function of domain names have been correctly transmitted without having explained the IP protocol?

Once again, we can see how the contents are concatenated, always starting from computer science, in accordance with the definitions given in the second section.

Freedom of Expression on the Internet. Responsibility of Intermediaries

A very topical issue dealt with in this area is the tension between freedom of expression and access to information on the Internet and the possible infringement of other rights such as privacy, image, honor, intellectual property, among others.

The analysis of this issue is based on the leading case Belén Rodríguez.

Based on the discussion of the right to freedom of expression and the prohibition of prior censorship, as well as the examination of the set of laws in which it is included, it is necessary to delve into various computer concepts put forward during the hearings in the aforementioned case.

In the first instance, the main notions about the Internet network architecture taught in the class corresponding to domain names are reviewed.

Next, the operation of search engines is explained, focusing on the automatic indexing of the sites that are then displayed in the search results, as well as on the concepts of cache memory and thumbnails.

The rationale behind it is given in the need to understand the intermediary role played by search engines, this implies that the student can differentiate between them and who is creating and publishing content on the Internet.

Based on this, the main debate in this case is introduced, the strict or subjective liability of search services, including the legal arguments that support each position.

Both positions are understood in greater depth by the students from the explanation given in the first instance about the functions of search engines on the Internet.

Protection of Personal Data

The topic begins with the analysis of the foundational work on the right to privacy: "Right to Privacy" by Warren and Brandeis, with special emphasis on the historical and social context of the year 1890, date of its publication and raising the differences with the current reality in relation to the massive use of ICT.

There are two highly topical cases related to the subject and which arouse great interest in students: "Cambridge Analytica" and "Snowden".

The lesson is introduced by relating both with the right to privacy of individuals from the analysis of the National Constitution, Civil and Commercial Code and related international regulations, with a special focus on the value that this information has today for governments and companies.

From this point of view, we seek to take a current look at our Law No. 25.326 on Personal Data Protection, which was enacted in 2000 when many of the current technologies did not yet exist.

It is valuable to emphasize this last point by delving deeper into the new technologies that are used today for data collection and analysis.

At this time, certain concepts related to new technologies are under discussion: big data, data mining, data science, machine learning, deep learning, among others.

By adding to the class a brief explanation of these tools, the student's understanding of the subject is broader, giving an adequate and current context to the importance that personal data has gained due to its use for behavioral analysis of individuals, segmented advertising, facial recognition, etc. Likewise, it is appropriate to talk to students about the importance of providing them with a correct protection, which is in accordance with the new technologies.

This makes it easier to understand the foundations of the right to privacy at present and the analysis of the institutes covered in the articles of Law 25.326: consent of the data owner; right of access, rectification and suppression; assignment; international transfer; among others.

It is also valuable to examine the future challenges in the field of personal data protection and give an overview of the most modern protective instruments that have emerged, such as the European Union's General Personal Data Protection Regulation (GDPR) and the Argentine draft bill, analyzing concepts such as privacy by design and by default; express and implied consent; right of portability; data protection officer; notification of security incidents; etc.

Digital Signature

Within the subject of digital signatures, the first issue to be delimited is its legal nature and evidentiary issues in comparison with handwritten and electronic signatures in the light of the analysis of Law No. 25,506 on Digital Signatures. It is very useful at this stage to show visual examples of each type of signature.

Subsequently, and before examining the entities that make up the digital signature infrastructure in the Argentine Republic, among them: root certifying authority, licensing entity, certifying authority, licensed certifiers and the concept of digital certificate, it is necessary to delve into computer, linguistic and mathematical definitions that make possible the operation of the system.

Of course the first concept to be introduced is that of cryptography. It is interesting to explain to the students that cryptographic techniques date back to the antiquity of mankind and are not exclusive to computer science.

As it is a concept that may involve some theoretical complexity, it can be exemplified by showing a scene from the movie "The Imitation Game" which focuses on the Enigma machine.

It can also be pointed out how the cypherpunk movement has applied it to new technologies since the nineties.

Taking into account that the digital signature in our country uses public key systems (PKI) based on asymmetric cryptography, it is also important to give a brief overview of these concepts so that students can know specifically what is the computer nature of this institute as well as the security it provides, which will help them understand why the Argentine law grants it the same validity as the oleographic signature in its art. 3.

A practical exercise to observe how the system works is to generate together with the students a pair of asymmetric keys through a Pretty Good Privacy (PGP) service to encrypt a message with a public key and decrypt it with the private key, explaining that the digital signature works in reverse.

ELECTRONIC AND COMPUTERIZED CONTRACTS

The first approach of the students to this topic is through an introductory discussion on the difference between each contract through the display of a comparative table between the two.

After this, the students are introduced to computer contracts, taking into account that the object of these contracts is the provision of goods and/or computer services, including hardware, software, computer security services, hosting, cloud services, etc., as explained by Fernández Delpech.

In order to explain the purpose of this type of contract, it is extremely useful to recall the IT terms explained during the class on legal protection of software (Section 4.1), among which are: hardware, software and firmware.

At the same time, the object of the computer services contracts mentioned by the author is also investigated.

The student's apprehension of the implications of these concepts arising from computer science contributes to a better understanding of the object of computer contracts, which is a fundamental requirement in their professional training.

For the approach to electronic contracts: "those concluded without the physical and simultaneous presence of the parties, who give their consent at source and at destination by means of electronic data processing and storage equipment", as well as their main characteristics, issues such as smart contracts or smart contracts cannot be left aside if the aim is to provide a modern education adapted to new technologies.

There is a computer concept related to these that cannot be omitted for a full understanding of the subject: blockchain.

Without the explanation of this term, it will be very difficult for the student to assimilate the informatics and legal nature of smart contracts, since it is the blockchain what gives them support.

It can be noted that the order of the topics dictated in the four-month period is not random or capricious, but the computer science concepts included in each one is linked and become more complex as the course progresses

It would be unthinkable to explain what a blockchain and a smart contract are without the student having first understood what a decentralized network is or the difference between software and hardware.

However, it would be even more difficult for the student if instead of having all these contents in the same subject respecting the above mentioned learning order, they would have been taught in different courses.

If the subject of smart contracts is covered in the curriculum outside the subject of Computer Law, it would probably be included in Contracts or Civil III, depending on the school. The main problem with this will be to address the underlying computer contents (if at all) if the student has not grasped the concepts that precede them.

Explaining smart contracts and blockchain, without first introducing the learner to the most basic computer science terms, could be almost equated to wanting to teach polynomials without first teaching multiplication and division within mathematics.

Cybercrimes

Cybercrime is one of the most complex topics within the subject due to two main aspects: the first is the difficulty in defining the concept, as explained in the words of Salt in the second section.

The second is that each criminal type includes a computer term, which must be known since it will determine whether the action will be typical or not, which is of vital importance for students who in the future will practice as defense lawyers, prosecutors or judges in the criminal jurisdiction.

The first part of the class consists of analyzing the concepts of computer crimes provided by various authors (Altmark and Molina Quiroga, Fernández Delpech, Salt, Téllez Valdez, among others) and seeking to construct with the students a definition of their own, always bearing in mind the difficulty behind the delimitation.

Subsequently, the characteristics of cybercrime and the difficulty of prosecuting it are analyzed: to this end, computer concepts already seen previously are reiterated: centralized and decentralized networks, OSI model, IP addresses, Internet service providers, etc.

After that, the international regulatory framework is examined through the Budapest Convention and finally the amendments to the Argentine Criminal Code introduced by Law No. 26.388 on Cybercrimes, analyzing each particular criminal type.

As mentioned above, it is crucial to emphasize certain concepts related to information technology: electronic document, digital signature, electronic communications, hacking, virus, malware, phishing, pharming, computer system, etc.

All of them are related to the criminal figures included in the articles of the law, which the student must know perfectly to be able to delimit which are the typical actions that conform them.

It is within this topic where the concatenation between the previously dictated computer concepts and the ones introduced here becomes more relevant.

If computer crimes had been dictated within the subject Criminal Law, it would be difficult and impractical for the student to address issues such as pharming within the computer fraud without previously knowing what a DNS and an IP address are, or what computer damage implies without knowing the difference between hardware and software.

CONCLUSIONS AND NEW PERSPECTIVES

As it has been clear throughout the lecture, the contents of the subject of computer law are closely related to technical issues of computer science.

Due to the proliferation of new technologies some students bring with them self-taught knowledge related to them, which in many occasions makes the debates more enriching.

But the reality is that these represent a smaller percentage of the student body and many times this knowledge is not entirely accurate, having to be adjusted during the explanations in class.

Leaving aside these special cases, for the rest of the students most of the computer concepts are totally unknown to them, so emphasis must be placed on them in order to lay the foundations of the legal contents so that they can be properly understood.

If the foundations are not firm, the building will end up crumbling. Within the evaluative instances, the student will have difficulties to satisfactorily demonstrate the legal knowledge if he/she does not correctly assimilate certain merely informatics conceptualizations that support them.

If all these topics are stipulated to be taught every four months (including two classes for mid-term exams), it would be naïve to think that they can be satisfactorily taught by inserting them separately in other subjects of the study plan without sacrificing content, being probably the technical-computer science ones the first to be eliminated.

Could a legal professional advise his client on the registration or dispute over a domain name without knowing what an IP address or DNS is? Could he initiate a software copyright claim without knowing what a programming language is or the difference between source and object code? Could he understand the scope of the digital signature without knowing what a PKI is? Could a judge rule on a cybercrime without knowing what a proxy, a CGNAT or the Tor network is?

Throughout this paper we have tried to show that the answer is clearly negative.

An appropriate question that could arise from the presentation is whether a law professor (usually lawyers) is qualified to transmit this type of knowledge to students.

It is not an easy question to answer, since the teacher may have self-taught knowledge about the computer part of the subject, but could end up making the same mistakes as the students who are also in that situation.

The reality is that nowadays most of the postgraduate courses, whether specializations or master's degrees in computer law or even in ICT in general, can provide the lawyer with a solid knowledge base in relation to these concepts and even improve them, so it is desirable that he/she has a degree of this type.

It is also remarkable that many of these postgraduate courses usually have as regular or guest professors forensic computer scientists with a degree in engineering or a bachelor's degree in computer science or telecommunications, among others; this could also be positive if applied to the teaching of the subject at the undergraduate level, especially in the more complex computer science subjects.

This type of practice is extremely positive and contributes to the interdisciplinary nature of two fields of knowledge that are largely interrelated.

It is clear that this would not be possible, or at least it would be extremely difficult, if there were not a subject that brings together all the contents and they were taught in a distributed way in the rest of the courses that make up the university curricula.

Throughout the paper it has also been demonstrated with the various topics that make up the teaching program how arduous it would be for the student to be taught in different subjects due to the ordered concatenation of computer concepts that go from a basic level to a more complex one and that in turn make the legal.

As the authors Altmark and Molina Quiroga argue, computer law is a thriving discipline that is brimming with modernity but, being relatively new, it has not yet been incorporated as an autonomous subject in all universities.

After almost twenty-five years since the appearance of the first commercial Internet connections in our country and the profound expansion in the use of ICT in the XXI century, which cross almost all aspects of our lives, it is inconceivable that only four of the fifteen universities that offer law degrees in the CABA, stipulate the subject as a mandatory part of their curriculum.

As stated in the first section, the use of ICT has brought about cultural, social and economic changes and law cannot remain unaffected by this.

The authorities of each university must make an in-depth analysis of the situation and ask themselves whether they wish to train legal practitioners prepared for the new challenges of modernity or, on the contrary, to train professionals with insufficient and outdated training.

ACKNOWLEDGEMENT

Translated & edited by American Publishing Services (https://americanpublishingservices.com/).

REFERENCES

Altmark, D.R., & Molina Quiroga, E. (2011). Tratado de Derecho Informático. *La Ley*, 1.

Asociación Argentina de Lucha Contra el Cibercrimen (AALCC). (2020). *Importante Incremento De Delitos Informáticos En Cuarentena*. Retrieved July 2, 2021, from https://www.cibercrimen.org.ar/2020/05/03/importante-incremento-de-delitos-informaticos-en-cuarentena/

Barriuso Ruiz, C. (n.d.). Interacción del Derecho y la Informática. In H. Piña Libien, *El Derecho Informático y su Autonomía como Nueva Rama del Derecho*. Retrieved July 4, 2021, from http://www.ordenjuridico.gob.mx/Congreso/pdf/78.pdf

Cámara Nacional de Casación Penal, Sala I. Sentencia del 19 de julio de 1995. Caso: Autodesk Inc.

Centro de Arbitraje y Mediación de la OMPI. Decisión del 5 de noviembre de 2010. Caso: Colegio Público de Abogados de la Capital Federal c. Splix Networks.

Corte Suprema de Justicia de la Nación Argentina. Sentencia del 28 de octubre de 2014. Caso: Rodriguez, María Belén c/ Google Inc. y otro s/ Daños y perjuicios.

Fernández Delpech, H. (2014). *Manual de Derecho Informático*. AbeledoPerrot.

Instituto Nacional de Estadística y Censo (INDEC). (n.d.). Accesos a Internet. Cuarto trimestre de 2020 en Informes técnicos / Vol. 5, n° 43, Ministerio de Economía Argentina, 2020. Retrieved July 20, 2021, from https://www.indec.gob.ar/indec/web/Nivel3-Tema-4-26

Juzgado Nacional de 1a Instancia en lo Civil y Comercial Federal Nro. 7. Sentencia del 26 de noviembre de 1997. Caso: Heladerías Freddo S. A. c/ Spot Network.

Juzgado Nacional en lo Criminal y Correccional Federal N° 12, Secretaria Nº 24. Sentencia del 20 de marzo de 2002. Caso: Gornstein Marcelo Hernán s/ Delito de acción privada.

Morin, E. (2002). *La cabeza bien puesta*. Nueva Visión.

Pascal, B. (2003). *Pensamientos*. Editorial del Cardo.

Salt, M. (1997). *"Informática y Delito" en Revista Jurídica del C.E*. Universidad de Buenos Aires.

Téllez Valdés, J. (2008). *Derecho Informático*. McGraw-Hill.

Zamora, G. (2014). El Documento Electrónico en el Contexto del Derecho Informático como Rama Autónoma del Derecho. In H. Fernández Delpech, *Manual de Derecho Informático*. AbeledoPerrot.