# A world without boundaries: digital evidence and international cooperation in the criminal investigation[1]

## I.- Introduction:

The constant technological advances and especially the emergence of the Internet as a global network, have produced a radical change of the reality in which people develop, managing to interfere in each and every aspect of the life of individuals and society.

That reality that is constantly moving forward, must be accompanied by the Law, as its regulation is essential for the improvement of the quality of people's lives.

However, this permanent evolution of science and technology brings at least two problematic issues: the first is that the law, and in particular Argentinian criminal law, seems unable to reach its rhythm, and the second, is the niche that generates for the proliferation of illicit activities worthy of state persecution. The criminalization of those conducts in the substantive law and their investigation under the current procedural law, fails to find a complete response.

Then, we are in presence of the so-called "cybercrimes", a term coined by the doctrine to comprehend "(…) a set of conducts of different characteristics, that affect diverse legal assets and that are only grouped under this concept by their relation with computers or the computer systems. This amplitude of the concept (...) determines that, for the purposes of scientific legal analysis, it is an empty concept, without its own content, which can only be acquired with the specific description of the different behaviors it covers."[2]

---

[1] This work was developed for its exhibition in the summer school organized by the Professorship of Criminal Law, Criminal Justice, Legal Theory, Information and Computer Science Law of the University of Würzburg, Germany (Julius-Maximilians-Universität Würzburg), which was held in July 2018, with the topic "Digitization and Law".

[2] Own translation of the original text. SALT, Marcos. "Informática y Delito" in "Revista Jurídica del Centro de Estudiantes", September 1997. Consulted in: https://derechopenalinformatico.blogspot.com/search/label/DI%20Derecho%20Penal.

In the international order, jurists agree that the relationship between scientific innovations and the Law should be characterized as symbiotic, because of the mutual benefit that is generated: the former allows the latter to recognize, analyze and deal with the phenomena that concern it, while Law, on multiple occasions, fulfills the function of promoter of the development of science and scientific innovations, by enabling, for example, its launch to the market, once the corresponding legal framework has been sanctioned.

This work will not try to carry out an exhaustive analysis of the topic brought to study, nor the reach of the revelation of a truth, but will try to raise certain issues characterized as problematic by the dominant doctrine and jurisprudence, and that may be debatable.

II.- Reception of cybercrime in the country:

Regarding cybercrime in Argentina, it is necessary to keep in mind the crimes established in the Nation's Criminal Code and its modifications, particularly the one that occurred after the entry into force of Law 26,388.[3]

This act has allowed the incorporation into domestic law, of the topics related to new technologies, adapting the current regulations to achieve the inclusion of certain crimes that were immersed in a legal loophole, which often enabled their authors to escape from the actions of the justice.

In this regard, the deputy Nemirovsci in one of the ordinary sessions held, said that *"(...) when drafting the Criminal Code the legislator could not anticipate in 1921 (...) the commission of crimes through computing and new technologies (...) We are simply adapting the criminal types to the new criminal modalities, which find informatics as a means of typical action. (...) But in the same way as we go for these new technologies that mold society to adapt it to its practice, the people who commit crimes shape these technologies to adapt them to new forms of committing crimes."* [4]

[3] Sanctioned on June 4, 2008 and promulgated on June 24 of that same year.

[4] Own translation of the original text. Argentinian Chamber of Deputies, Parliamentary Secretariat, Parliamentary Information Directorate, 34th Meeting - 25th Ordinary Session, October 11, 2006. Written transcription consulted in: http://www1.hcdn.gov.ar/sesionesxml/mltsearchfull.asp#8. In this sense,

The situation at the time of the enactment of the law was compelling, since there were multiple existing cases of citizen's rights violations and illicit activities that affected society as a whole.

The existing legal loophole regarding cybercrime ended up motivating judicial resolutions with interpretations often bordering the violation of the legality principle, particularly in its requirement of *lex praevia* [5], and of *lex stricta*, that prescribes the prohibition of analogy *in malam partem.*

The law has replaced and incorporated articles, achieving the establishment in the Criminal Code of the Nation, of crimes such as the dissemination of pornographic images and shows of minors (article 128 - then modified by law 27,436),[6] the violation of electronic correspondence (article 153), hacking and cracking (article 153 bis), violation of the privacy of electronic communications (article 155), computer fraud (article 173, section 16) , computer damage (articles 183, 2nd paragraph and 184, sections 5 and 6), the interruption or obstruction of communications (article 197), among others. Then the crime of grooming was added through law 26.904[7], in article 131 of the same normative body.

Furthermore, it should not be overlooked, that the multiplicity of criminal behaviors covered under the concept of "cybercrime" are particularly serious, since they are perpetrated by individuals with specialized knowledge, who hide behind computer systems, consummating their criminal behaviors from anonymity, seeking for themselves greater impunity, and without risks in relation to victims who are positioned in a special state of inferiority and vulnerability.

---

Deputy Charcchio said that: *"Against this background, and to get our country out of a lagged situation, (...) cybercrimes are established in our legislation to prevent the creation of loopholes of impunity , social damages and negative effects from the point of view of the general prevention of crime, protecting the integrity and privacy of people, as well as the interruption of communications, the alteration of evidence and the falsification of computerized documents"*.

[5] The principle that prescribes that a conduct may only be punished if criminal liability had been established by law before the act was committed.

[6] Published in the Official Gazette on April 23, 2018. Not only did it significantly increase the penalties imposed in the former article, but it also punished the simple possession of pornographic representations of minors and raised all the scales - by a third in its minimum and at its maximum -, for the cases of victims under the age of thirteen.

[7] Sanctioned on November 13, 2013 and promulgated on December 4 of that same year.

At present, the anonymity provided by existing technologies and in particular the Internet, added to the possibility of carrying out criminal conducts beyond the borders of the state in which the perpetrator is located, means that obtaining and safeguarding the evidence that proves the materiality and authorship of these crimes is really difficult, a circumstance that makes cooperation at the international level truly indispensable.

III.- Digital evidence and international cooperation:

III.a.- The Budapest Convention:

On November 23, 2001, the only international convention in force - since July 1, 2004 -, was subscribed in the City of Budapest, Hungary, regarding cybercrimes. Although there are other cooperation treaties in criminal matters, these were conceived taking into consideration the physical evidence, not the digital one. The Convention also has an additional protocol - January 28, 2003 - relating to the criminalization of acts of racist and xenophobic nature committed through computer systems.

This is the Convention on Cybercrime of the Council of Europe - Convention on Cybercrime -, commonly called as the "Budapest Convention". The National Congress approved this multilateral treaty through the law 27.411[8] and it will come into force for our country on October 01, 2018.[9]

In its Preamble, the States that produced it said that the profound changes caused by digitalization, convergence and globalization of computer networks and electronic information led to the concern that these were used to commit crimes and that the evidence related to them, was stored and transmitted through these networks.

In this sense, it is clear that the object of the Treaty is the protection of society against cybercrime, through the establishment of a common criminal policy, the

[8] Published in the Official Gazette on December 15, 2017.

[9] So far there are sixty (60) States that have ratified it and the full table can be consulted on the European Council website: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=kedek2La.

adoption of adequate and homogeneous legislation, and the improvement of international cooperation among States, which should be quick and effective. [10]

In Title I, Chapter III, the Convention establishes the general principles that govern the system of international cooperation in matter of punishment, which is not only oriented to investigations of cybercrimes or related to computer systems and data, but also to those investigations who seek to obtain digital evidence to proof other traditional crimes.

Mutual assistance between Member States should be developed in accordance with the provisions of the domestic law of the requested Party, or bilateral assistance treaties that are applicable to the case. In absence of regulation, the Convention determines the application of paragraphs 2 to 9 of the 27th article, and to ensure the agility and efficiency of the system, it also foresees the appointment of one or more central authorities by each Party, so that they can communicate with each other, send the requests for mutual assistance, answer them, execute them or send them to the competent authority for their execution.

In this way, States are allowed to access to measurements of provisional nature, such as the rapid preservation of digital data stored by computer systems within another Member State and the rapid disclosure of stored data -arts. 29 and 30 -, as well as to legal measurements such as having access to computer data stored in another jurisdiction - art. 31 -, cross-border access to public data, or data stored in another State with the consent of the person legally authorized to reveal it, obtaining in real time data relating to traffic and content of communications transmitted in the territory of another State - arts. 33 and 34 -, all of which are of incalculable value for the conservation and obtaining of transnational evidence in criminal matters.

The commitment adopted in the Convention was of such magnitude that the creation of a "24/7" network was established - art. 35 -, in order to achieve greater speed of communications between the States, through the designation of a point of contact that can be reached 24 hours a day, seven days a week, in order to guarantee assistance immediately in obtaining the digital proof of a crime.

---

[10] Convention on Cybercrime of the Council of Europe; Budapest, Hungary; November 23, 2001. Consulted in: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

III. b.- The role of the UFECI in obtaining digital evidence abroad:

In 2017, the Specialized Unit on Cybercrime (UFECI[11]), in a joint effort with the General Directorate of Regional and International Cooperation (DIGCRI) of the National Public Prosecutor's Office, developed the "Guía de buenas prácticas para obtener evidencia electrónica en el extranjero"[12] (Guide of good practices to obtain electronic evidence abroad).

In its second section, it emphasizes the importance of preserving information in advance of its request, given that due to its volatility it could be altered, damaged or eliminated, either by the different service providers or by its own users. It is also established that the preservation is usually available for a period of ninety (90) days, extendable for a similar period, and that it can be required directly to the company or through the G7 24/7 Network of High Tech Crime, whose point of contact in the country is Dr. Horacio Azzolin, Prosecutor in charge of the UFECI [13].

This network, managed by the United States Department of Justice, provides a procedure that, although it does not replace the formal ones, allows the preservation of digital data found in foreign jurisdictions. The communication is made by the requesting national contact point, with the peer of the State whose cooperation is required, and this way it is also possible to request the closure of a website or report criminal activity online in the United States, when it is affecting the requesting nation.[14]

IV.- New challenges in the criminal process: digital evidence:

Dr. Marcelo A. Riquert points out that the adoption of accusatory codes in the region - referring to Latin American codes - has introduced a situation that he describes

[11] Created by Resolution PGN 3743/15. The UFECI has as its fundamental mission the development of preliminary investigations and assistance to prosecutors in cases in which a computer system has been subject to the crime or has been the means to commit it. At the same time, it was designated as a point of contact for different international cooperation networks such as the Ibero-American Network of International Legal Cooperation, the specialized network of the Ibero-American Association of International Legal Cooperation, among others. Data obtained from its website: https://www.mpf.gob.ar/ufeci/

[12] Unidad Fiscal Especializada en Ciberdelincuencia et. ál; "Guía de buenas prácticas para obtener evidencia electrónica en el extranjero", 2017. Consulted in: https://www.mpf.gob.ar/ufeci/files/2017/01/Guía-de-Buenas-Prácticas-para-Obtener-Evidencia-Electrónica-en-el-Extranjero.pdf

[13] Unidad Fiscal Especializada en Ciberdelincuencia et. ál; Op. Cít. p. 9.

[14] Red G7 24/7. Available in: http://www.oas.org/juridico/spanish/cyb20_network_sp.pdf

as "curious". It is that although there was a tendency to massive transformations of the procedural systems, the provisions related to evidence have remained without major variations with respect to the old inquisitive or mixed digests.[15]

In this sense, it is argued that the reformulation of procedural rules regarding the obtaining of evidence in criminal matters is fundamental, since the existing provisions are applicable only to physical evidence and not to digital evidence, no matter how permissible is the use of analogy in terms of procedure.

In cases in which the proof that is required is electronic, it does not seem as if our procedural code provides us with the answers that are needed, thus generating truly problematic situations.

Marcos Salt gives as an example of this the case of the search of a bank by legitimate order of competent authority, where experts in finding the desired digital information, discover that although through the computer system found they can have access to it, the data is physically stored in another State.

Would it be legitimate to continue with the registration and seizure of the data? Could these be validly incorporated into the criminal process? Would the authority be enabled to proceed to the copying of the data without removing it?[16]

For Dr. Salt, if we applied by analogy the current procedural rules for obtaining physical evidence, we would not be able to find an adequate solution, both in terms of efficiency of the investigation and of the protection of the individual guarantees, especially of the right to privacy.[17]

---

[15] RIQUERT, Marcelo A.; "Convenio sobre Cibercriminalidad de Budapest y el Mercosur Propuestas de derecho penal material y su armonización con la legislación regional sudamericana" in "Informática y delito: Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal" -AIDP / Javier Augusto De Luca and Joaquín Pedro da Rocha. - 1a ed. - Autonomous City of Buenos Aires: Infojus, 2014, p. 170.

[16] SALT, Marcos; "Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos"; 1ª ed., Buenos Aires, Ad-Hoc, 2017, pp. 222-223.

[17] SALT, Marcos; "La relación entre la persecución de delitos informáticos y el Derecho Penal Internacional Delitos informáticos: aspectos de Derecho Penal Internacional", in "Informática y delito: Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal" - AIDP / Javier Augusto De Luca and Joaquín Pedro da Rocha, 1ª ed., Autonomous City of Buenos Aires: Infojus, 2014, p. 239.

Regarding the registration and seizure of computer data, the new National Criminal Procedural Code - law 27.063[18] - provides in Article 144 the power of the judge to stipulate by founded order and at the request of a party, the registration of a computer system or a part of it, or a means of storing computer or electronic data, for the purpose of seizing the components of the system, obtaining a copy or preserving the data or elements of interest for the investigation.

It also expressly stipulates that the limitations established for the seizure of documents apply here, and that regarding the digital evidence seized, there will be applied the rules to open and examine correspondence. However, nothing says about the extension of the order for the case in which the data or the digital evidence sought are stored in another computer system that can be accessed from the one that is the subject of the order.

One of the possible solutions given by the doctrine would be the reform of the procedural codes in the light of Article 19 of the Budapest Convention, empowering the competent authority to register the computer systems, their parts, the digital data stored in them, and data storage devices in its territory, expressly providing the possibility of extending the registration to another computer system when there is sufficient reason to maintain that the data sought is in it, and not in the one that is being registered (only if the second one is also within the national territory, and could be accessed there by means of the initial system).[19] Salt proposes a modification that also includes the possibility of expanding access to data in foreign jurisdictions.[20]

That is to say: one should try, without going so far as to subjugate constitutional guarantees, that the registration and seizure orders are endowed with a certain plasticity, which enables the competent authorities to quickly extend the registration to the other computer system, in which it is thought that the digital evidence is located.

---

[18] This law was approved by the National Congress but its entry into force was suspended by an executive decree.

[19] DUPUY, Daniela; "Desafíos procesales en la investigación de delitos informáticos" in "Informática y delito: Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal" -AIDP / Javier Augusto De Luca and Joaquín Pedro da Rocha. - 1a ed. - Autonomous City of Buenos Aires: Infojus, 2014, pp. 145-146.

[20] SALT, Marcos; "Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos"; 1ª ed., Buenos Aires, Ad-Hoc, 2017, pp. 307-308.

## V.- Conclusion:

Science and technology progress minute by minute in leaps and bounds, interfering for better or for worse in every aspect of the life of man and society, thus existing a physical reality, and a virtual reality.

With the same agility, individuals acting from cyber-criminality improve their knowledge and techniques in such a way that they manage to consummate their crimes with ever greater impunity, leaving their victims in a state of great vulnerability.

This lack of protection does not take place only because of the lack of sophisticated digital tools that function as defensive barriers for individuals, but also because of the gap between the advances of Law and those of scientific and technical activity, as if there were two worlds that do not manage to converge in a fluid and enriching dialogue.

It seems that, especially in the Argentinian criminal procedure, the Law is always several hundred meters behind technological advances, where particularly in terms of means of evidence in the digital field, its shortcomings are evident.

The lack of adequate procedural regulation in the matter means that the rules for obtaining physical evidence must be applied by analogy - based on the principle of evidentiary freedom - a circumstance that harms both the efficiency of the investigation and the protection of the guarantees of the accused, fundamentally, the right to privacy.

Many times, the negligence of the judicial operators even reaches the point of making it impossible to achieve the real truth through the criminal process, since digital evidence is in many cases indispensable, both for the prosecution of cybercrimes and traditional crimes.

The only possible way to shorten the gap is to achieve the constant training of legislators and judicial operators, who acting in conjunction with specialists of the technical sciences, must adapt the existing procedural structures, always striving to strengthen the bonds of international cooperation in the matter, otherwise it would not be possible to face this type of crime, whose deployment no longer recognizes borders.

VI.- Bibliography and sources:


- Argentinian Chamber of Deputies, Parliamentary Secretariat, Parliamentary Information Directorate, 34th Meeting - 25th Ordinary Session, October 11, 2006. Written transcription consulted in: http://www1.hcdn.gov.ar/sesionesxml/mltsearchfull.asp#8
- DUPUY, Daniela; "Desafíos procesales en la investigación de delitos informáticos" in "Informática y delito: Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal" -AIDP / Javier Augusto De Luca and Joaquín Pedro da Rocha. - 1a ed. - Autonomous City of Buenos Aires: Infojus, 2014.
- NAGER, Horacio Santiago. "Protección Penal de la Privacidad en la <<sociedad de la información>>. Análisis de la ley 26.388 y algunas consideraciones preliminares en torno al Anteproyecto de Código Penal de la Nación". Consulted in: http://www.pensamientopenal.com.ar/doctrina/41420-proteccion-penal-privacidad-sociedad-informacion-analisis-ley-26388-y-algunas
- RIQUERT, Marcelo A.; "Convenio sobre Cibercriminalidad de Budapest y el Mercosur Propuestas de derecho penal material y su armonización con la legislación regional sudamericana" in "Informática y delito: Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal" -AIDP / Javier Augusto De Luca and Joaquín Pedro da Rocha. - 1a ed. - Autonomous City of Buenos Aires: Infojus, 2014.
- SALT, Marcos. "Informática y Delito" in "Revista Jurídica del Centro de Estudiantes", September, 1997. Consulted in: https://derechopenalinformatico.blogspot.com/search/label/DI%20Derecho%20Penal
- SALT, Marcos; "La relación entre la persecución de delitos informáticos y el Derecho Penal Internacional Delitos informáticos: aspectos de Derecho Penal Internacional", in "Informática y delito: Reunión preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal" -AIDP / Javier Augusto De Luca and Joaquín Pedro da Rocha, 1ª ed., Autonomous City of Buenos Aires: Infojus, 2014.

❖ SALT, Marcos; “Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos”; 1ª ed., Buenos Aires, Ad-Hoc, 2017.

❖ Unidad Fiscal Especializada en Ciberdelincuencia, Dirección General de Cooperación Regional e Internacional del Ministerio Público Fiscal de la Nación; “Guía de buenas prácticas para obtener evidencia electrónica en el extranjero”, 2017. Consulted in: https://www.mpf.gob.ar/ufeci/files/2017/01/Guía-de-Buenas-Prácticas-para-Obtener-Evidencia-Electrónica-en-el-Extranjero.pdf

- Laws and conventions:

❖ Law Nº 26388. Consulted in: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm.

❖ Law Nº 26.904. Consulted in: http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm

❖ Law Nº 27.411. Consulted in: http://servicios.infoleg.gob.ar/infolegInternet/anexos/300000-304999/304798/norma.htm

❖ Law Nº 27.436. Consulted in: http://servicios.infoleg.gob.ar/infolegInternet/anexos/305000-309999/309201/norma.htm

❖ Convention on Cybercrime of the Council of Europe; Budapest, Hungary; November 23, 2001. Consulted in: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

❖ Website of the UFECI (Unidad Fiscal Especializada en Ciberdelincuencia). Consulted in: https://www.mpf.gob.ar/ufeci/