Julius-Maximilian Universität Würzburg - Summer-School 2018
Abg. Jeremías Brusau

On the incorporation of *Remote Forensic* to federal procedural law

I. Introduction.

We will begin by establishing that no research done only with the evidence envisaged in the Criminal Procedural Code of Argentina would be successful. In fact, it has been written before the age of digitization and hasn't been updated with the emergence of the internet, much less with the tools that emerged most recently: smart devices (from cell phones to homes), *bitcoins*, *apps*, geolocation devices, to name a few examples. In turn, the picture becomes more complicated by considering that both the recently legislated "cibercrimes" as the most traditional ones are committed through digital media.

It is simple to understand the importance of research through computer media in cases of cibercrimes such as grooming. However, Salt gives us a very simple case related to traditional criminal figures: "*A fifteen-year-old student had sent bomb threats to a Washington high school through mails by using the social network Myspace. The police had not been able to resolve the case and judicially requested the use of the CIPAV programme. FBI agents trying to trace the origin of the threats sent by e-mails against a high school in Washington sent the suspect a secret surveillance program designed to surreptitiously monitor and inform a server of Government. "*[1] Thus, the investigation of a conduct that in our law would be subsumiable in the penal type of public intimidation, required the use of modern techniques, unthinkable in the event of a threat made twenty years ago.

It has become a common place to affirm that the exponential development of information and communication technologies has led all aspects of life to be marked by digitization. This phenomenon produces three effects that we want to highlight. First of all, the generation of legal goods worthy of protection. Secondly, the availability of increasingly sophisticated tools for the commission of crimes. Finally, the existence of a new kind of evidence made available to the State for the investigation of criminal offences. In this regard, said Carlos Sueiro that "*In the new digital age, an activity performed by a citizen would hardly not be registered or stored in a server or data center, waiting to be used one day by a state authority or private company when the information about that subject or person is required or demanded. "*[2] However, the lack of specific rules regulating the obtaining of digital evidence results in that either this information will not be incorporated into the penal processes, or it will be by means of proof that do not respond to its specific characteristics. This situation will lead, on the one hand, to a lack of efficiency in the use of the digital evidence, mainly because of the lack of adequate means for obtaining and surveying and the absence of specific forecasts. Regulating Your guard and custody. On the other hand, the analogue application of standards envisaged for other means of testing may negatively impact on the exercise of the right of defense, particularly in the control of the test. In the absence of a legally established procedure, how could the defense object the obtaining of the evidence?

The national state has echoed the problems generated by the lack of specific regulation. Thus, during 2018, it has acceded to the Convention on Cybercrime of Budapest, which required the respective Federal Complex Act, in which they take part the Executive Power and the National Legislature. Within the scope of the Public Prosecutor's Office, by resolution PGN 756/16, the "guide to obtaining, preserving and treating digital evidence" has been approved. The Supreme Court also considered the

[1] Salt, M.; *Nuevos desafíos de la evidencia digital*; Buenos Aires: Ad Hoc, 2017. P. 81.
[2] Sueiro, DC; *Vigilancia electrónica y otros modernos medios de prueba*; Buenos Aires: Hammurabi, 2017. P. 41.

need to incorporate new technologies into criminal investigation in its agreed 30/16, by providing for the creation of the "Directorate of Judicial Assistance in Complex Crimes and Organized Crime". The three instruments mentioned include rules that tend to update the national procedural system and the practice of the courts. But none of them eliminates the need to have a digital proof regulation in the code that establishes the Federal penal rite.

However, although the need for specific regulation on the subject is undeniable, there are voices that rise up against the incorporation of certain means of evidence. They argue that their acceptance would provide the state with a power of such magnitude, that it would allow him meddling in the sphere of rights of its citizens.

In this article we will refer specifically to the *Remote Forensic*, whose incorporation into the Federal Criminal Procedure Code was recently attempted through a failed bill. To do this, we will briefly discuss what it is and what was the proposal addressed at the National Congress, then study what were the constitutional issues that were raised and which ones could be presented and, finally, extract a conclusion concerning the desirability or necessity of incorporating this institute into national legislation.

II. The updating of the criminal procedure legislation. The *Remote Forensic*

It is frequent in the investigations of crimes linked to the organized crime (illicit traffic of narcotic drugs, trafficking of persons, terrorism, money laundering) to proceed to the analysis of computer devices in order to obtain a "bit-a-bit" forensic image of the data there hosted, operation that will be subject to the level of the specific training with which the judicial operator counts. The guide of the Public Prosecutor's Office referenced *ut supra* can be very useful for this process.

The structure of the organizations dedicated to these crimes makes it impossible to advance in an investigation without using digital evidence. Indeed, the estrangement of the chiefs or organizers with respect to the "scene of the crime", coupled with the selectivity with which the police forces operate, practically guarantees the impunity to the upper tables of the organizations, unless the state has the ability to unravel the internal links that set them up. And, in the age of encrypted communications capable of disappearing in seconds, the digital test is the only way to acquire efficiency on investigations.

However, the exponential growth of the functionality of computer devices has an unequal impact on the tension between state power and the activities of criminal organizations. While they can immediately make use of new technologies in their illicit activities, the latter cannot use means of evidence involving a relevant interference in the rights of people without a law that enables it[3]. Therefore, the constant technological advance also requires a constant revision of the legislation.

In this context appears the proposal of reform of the Penal Procedural Code approved by law 27,063, as soon as it impulses the incorporation of electronic surveillance techniques as a mean of proof in the criminal process. This from the Institutes of acoustic surveillance, surveillance of electronic communications, remote surveillance on computer equipment, surveillance through image capture and surveillance devices through tracking and localization devices. In particular, it is the remote surveillance on computer equipment which occupies our attention, being the one that unleashed the biggest objections and, in turn, one of the most effective in criminal investigations.

[3] Cfr., Bruzzone, G.A., "La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal", en AA.VV.; *La justicia penal hoy. De su crisis a la búsqueda de soluciones*; Buenos Aires, Di Plácido, 2000. P. 247.

Remote monitoring of computer equipment consists of the installation of malicious programs, known as *Remote Forensic Software,* in a computer device. These programs produce surreptitiously the sending of data from that device to another, managed by the judicial police or other body in charge of the task. According to Salt's brilliant enumeration, the use of this technique allows:
"-Search for information stored in computer media. (...)
-Record and preserve data Traffic on communications (...) In this function, it is allowed to secure data that even in a raid often is not obtained since the computers do not store the data of communication.
-The program can record access keys to remote servers or encrypt files contained in the system and send them remotely to the authority that is in charge of the measure. (...)
-Record information that is processed through the computer but is not permanently recorded on the hard drive (...)
-Activate surveillance mechanisms such as webcams or microphones. (...)
-Identify the author of an Internet communication that would have been made with techniques specially designed to mask the IP address from which the communication occurs. "[4]
As we see, the techniques of *Remote Forensic* allow access to the data that is normally obtained after the expertise of the devices, without physical access to them. But they also make it possible to obtain another kind of information that so far is inaccessible to researchers.
Professor Sueiro offers an example of the usefulness of this method of research, explaining that "*Aware that once the Internet session has started on the Deep Network (Deep Web) It is impossible to identify the electronic device that was connected and that is browsing, as well as to see the contents of its conversations or files that it exchanges, and in turn because many of its documents, files, photos, recordings or videos are found encrypted; is that security forces, often resort to stealth installation of spyware on electronic equipment, in order to know their encryption passwords and see in advance which documentation you want to exchange before connecting to the deep network (Deep Web). "*[5]
Originally, within the framework of the Program "Justice 2020" of the Ministry of Justice and Human Rights[6], a standard was presented which established: "*The non-ostensible use of software that allows or facilitates remote access of computers, computer systems, databases or massive computer data storage instruments may be authorized. The judge shall require the Prosecutor to specify the data or computer files to be obtained with the measure and the manner in which it shall be collected; the identification of the software through which the control of the information is executed, the individualization of the computers, electronic devices, computer systems, databases, or instruments of mass storage of computer data that shall be subject to surveillance; and the estimated length of the measure. The Prosecutor shall request the judge to extend the registration measure if warned that the data sought they are stored on another computer device that is accessed from the originally authorized system."*
As we see, the text of the article clearly points to the incorporation of the Institute we have been dealing with, but with some limitations on its application. Firstly, it is established that the data or computer files that are sought should be clarified, thus avoiding the use of this tool for a "fishing excursion". This rule seeks to ensure that the *Remote Forensic* constitutes a measure taken in an

[4] Salt, M.; idem appointment 1. P. 71-72.
[5] Sueiro, DC; idem quotation 2. P. 115.
[6] Cfr. www.justicia2020.com.ar. Date of last entry: July 18, 2018.

ongoing investigation where there is already other evidence that indicates that in a device or computer system there is data necessary to achieve the purposes of the instruction.
It also adds the standard to the need to specify the way in which recruitment will be made. That is to say that the Prosecutor must indicate the *software* that will be used and the methodology that will be applied to place it on the appropriate device or system. In general, this operation is done by sending an email to the device carrier so that it downloads a file containing the malicious program. However, it can also be installed directly via a mobile device. This information must be explicit in the order of the Prosecutor.
It is also required the individualization of the device or system that will be the subject of the measure, clearing that if it's needed to extend it to a different object, a new order must be requested. Indeed, organizations that use more sophisticated technology often deposit the information they generate into encrypted databases, which means that the access must be done in two steps. First, ensure access to the device from which the user is connected that has already been individualized, in order to locate the database of the data and the decryption key. Secondly you can try accessing the database.
Finally, the rule requires the Prosecutor to estimate the length of the measure. While a limit is not established there, article 175 ter orders that the measure could be taken for a maximum of one month, extendable to a total of three months. This is the shortest period of time between which it enables the procedural standard for electronic surveillance measures.
Subsequently, the Senators Urtubey and Guastavino presented in the Congress a bill that retook the proposals, and that in its Article 175 septies foresaw remote surveillance of computer equipment by saying, "*The non-ostensible use of software allowing or facilitating remote access to the content of computers, electronic devices, computer systems, databases or mass storage instruments may be authorised. "* This standard was supplemented by Article 175 quater, which envisaged a maximum duration of one month, extendable without time limit, according to the principles of necessity, reasonability and proportionality.
When comparing both texts, it appears at first sight that the second lacks the precisions established by the first and that, as we pointed out, they clearly aim to prevent the state from taking advantage of this tool to carry out "fishing excursions" outside of a specific investigation. It is clear that the application of the general principles and the proportionality test will in each case require robust judicial control, taking into account the rights at stake. However, the formal requirements provided for the Prosecutor's request made it possible for the judicial authorities to have real control.
We understand that the lack of specific training on the part of the judicial operators in matters of cybercrime produces that both the identification of the cases in which one can go to the digital evidence as well as the way to obtain it and to protect it is turned extremely difficult. And it is clear that those who do not know how to operate a system cannot control it efficiently. It has been shown that the low rate of judicial complaints in the field of cybercriminality is explained in part because of "*The belief that criminal investigation will not have an effective resolution for lack of training of judicial officers and appropriate resources. "*[7] In this context, the requirement of the authorities requesting the production of evidence through *Remote Forensic* revealing the method by which the

[7] Sain, G.; Dificultades del proceso judicial en la investigación de delitos relacionados con dispositivos informáticos", en Sain, G. Azzolin, H.; *Delitos* Informáticos; Buenos Aires: B de F, 2018. P. 69

information will be obtained and identifying the software to be used constitutes a real guarantee that the necessary judicial control will be produced on the measure.
However, despite the advantages that we pointed out in the incorporation of this evidence into the procedural norm, it generated a great resistance, especially in the organizations dedicated to the protection of human rights. This due to the fact that his treatment was not given in Congress, withdrawing from the bill the respective articles, and suspending his discussion indefinitely. In the next section we will explain the constitutional objections that were raised and those which could be presented in connection with the *Remote Forensic*.

III. Privacy, intimacy and electronic surveillance

As soon as it was disseminated that the reform of the Criminal Procedure Code would be treated in Congress, different voices were raised against the incorporation of electronic surveillance techniques as evidence. This is the case of the Civil Rights Association (ADC), which disclosed the document "Spy reform. Comments to the regulation of new surveillance techniques in the reform project "[8]. Particularly In relation to Surveillance on electronic devices, it indicated that "*The project omits to consider essential issues for a legitimate exercise of that faculty. Who would be responsible for carrying out such activities? What would be the software used? Would the software be purchased as a packaged solution to companies specialized or developed by the same state? Would audits-ideally independent-be carried out to be sure that the software does only what was determined in the order authorized by the judge? What kind of control mechanisms would be put in place for proper accountability of the use of the software and the operations carried out with it? Of the limited description provided by the layout of the project, it is not clear what type of software will be used specifically, or how it will be implemented. "*[9]
In addition, a coalition of NGOs made public a document in which it expressed concern that "*The state advances on the possibility of intervening in the intimate jurisdiction of those who are the subject of a criminal investigation without a debate as to the form and scope that these measures must have in order to conform to a due respect of the constitutional guarantees of the accused. "*[10]
As a result, at the time of the debate on the bill on the premises of the Senate, the articles relating to electronic surveillance measures were withdrawn. However, there were interventions that referred to these institutes. That is the case of Kunath, who expressed himself in the following terms: "*The truth is that I am glad to hear the changes that have been made to the opinion of majority, but I can not understand how they dared to carry out a maneuver so crude wanting to run over highly personal rights of all Argentines in a debate that lasted, in the Committee on Justice and Criminal Matters, thirty-two minutes. I repeat: Thirty two minutes to get an opinion of a project that, if you took it as it was, it would allowed to spy and persecute not only those who think differently-we have been spectators of that many Argentines-but also-why not say-to the commercial competitors of the CEOs who govern us today. "*[11]

[8] Available in https://adcdigital.org.ar/portfolio_tag/reforma-espia/. Last entry: July 18, 2018.
[9] See the referenced document in the preceding note, P. 8-9.
[10] "Reform of the procedural Code extends the powers of the state to monitor" available in https://www.cels.org.ar/web/2018/04/la-reforma-del-codigo-penal-amplia-las-facultades-del-estado-para-vigilar/. Last entry: July 18, 2018.
[11] Verbatim version of the 1st special session of the period 136 °, dated April 25th, 2018, of the Senate of the nation.

It is clear from the above that there is widespread consensus that the measures of *Remote Forensic* imply a limitation of rights, but little precision as to what assets are affected and to what extent they are. The national doctrine has entered to the treatment of the question from the distinction, introduced by Carlos Nino and traditional in our literature, between the right to intimacy and the right to personal autonomy or privacy. According to him, the right to intimacy protects people's claim that the actions they make discreetly and reserved remain outside the knowledge of third parties, whether the State or a particular. Instead, the right to privacy refers to the possibility of performing any behavior that does not affect third parties, and is linked to the free development of the personality. From there derives the right to self-determination of the personality, that is, the possibility that assists everyone to design their own plan of life consciousness, cultivating the values that it considers appropriate on the basis of the free choice, without interference from the state or from any other person.

While the distinction between intimacy and privacy does not emerge clearly of International human rights instruments and compared legislation, in our system, it has been interpreted that the constitutional right of privacy arises from the first sentence of article 19 of the National Constitution. Instead, the right to intimacy arises from article 18, as it consecrates the inviolability of the domicile and of the private papers and epistolary correspondence.

It has been recognized as a special area of the right to intimacy the "right to self-determination of information" or "informatic freedom". In the words of Pizzolo, "*This right owes its conceptualization to the jurisprudence of the German Federal Constitutional Court, which in its famous judgement on the "Census law" developed the notion of the right to informatic self-determination as: "The faculty of the individual, derived from the idea of self-determination, to basically decide for itself when and within what limits it is necessary to reveal situations relating to one's own life. "*[12] In our constitutional system, this right arises from the clause of the implicit rights, but also from the general protection of the intimacy and of the specific guarantee that has been prepared for its protection: the *Habeas data*.

The access to the information contained in an electronic device or database through the surreptitious installation of a software implies, then, an affectation to the right to the privacy of the people, specifically to their informative self-determination. It deprives those who generated the information that is intended to be obtained in the process of the right to keep it secret, and it is revealed in the context of a criminal process.

However, the truth is that, unlike personal autonomy, the right to intimacy has limits. In fact, the inviolability of the domicile may be put aside before a search warrant issued by the competent judge, telephone communications may be intervened if the forms provided for in the procedural rules are complied with, the correspondence can be opened. So, if the state is allowed to enter people's homes, why should not it be enabled to access to their electronic devices?

The truth is that the *Remote Forensic* technic has particular characteristics, which take it away from other measures involving an intrusion of the state into the intimate sphere of people. So, unlike of the search, the remote access to electronic devices is done in a surreptitious way, without giving notice to the person or the people who use them. In this regard it approaches telephone interventions, but with a scope that is not limited to interactions with other people, but comes to the most intimate information, that which is not revealed to any human being, but for its protection is

[12] Pizzolo, C.; *National Constitution commented, agreed and annotated with the international treaties with constitutional hierarchy and the jurisprudence of the international control bodies*; Mendoza: Legal editions of which, 2002. P. 495.

dumped in the digital world. But, to appreciate on all its magnitude the affectation of rights implied, it is necessary to consider that in the digital age, people dump an unimaginable amount of information on the network through their computer devices. The *Remote Forensic* allows access to much more than would be achieved with a raid on the residence of the imputed: contacts, endless listings of communications by different means, passwords of social network accounts, banking services, intimate diaries and digital agendas, artistic and scientific production, among many others. However, recognition of such a degree of intimacy does not imply that the use of this tool should be ruled out. As Sueiro rightly points out, in the digital age all our habits and customs are captured by cameras, sensors, geolocation systems and even through our own movements in the network[13]. Today there are programs dedicated to monitoring our movements for commercial purposes, programs that record personal information in databases of which we do not have any information. We understand that reasonable legislation will authorize the State to access this information on the basis of a strict proportionality examination, taking into account the particularities of the measure.
In the same vein, Salt said that "*Legal habilitation must be highly restrictive in response to the danger generated by individual guarantees, only for crimes of special severity previously determined with a numerus clausus (e.g., terrorist organizations or associations linked to drug trafficking offenses), in response to special situations such as the challenges of organized crime or imminent dangers to the safety or physical integrity of persons, under special conditions to ensure their use when It is absolutely necessary in accordance with proportionality criteria which take particular account of the importance of State interference authorized and with special controls on the form of implementation of the measure and on the incorporation to the process of the data obtained. "*[14]
In similar terms, when referring to the use of surreptitious recordings by the State, Ipohorski has said that "*it has been held that in the face of interference in the private life of persons, for the purpose of investigating a crime, a court order is necessary that authorizes it, not enough the order of the Prosecutor or the intervention of an administrative authority. "*[15]
Thus, in the case of an extremely burdensome measure for the right of intimacy of people but which can prove enormously effective in the fight against the most serious forms of organized crime, we understand that the task of the legislator must be rigorously define the limits within which their use is legitimate. Thus, taking some of the figures mentioned above, a closed catalogue of crimes, a temporary limit and the requirement of the Prosecutor to provide technical details could be fixed. As for the protection of personal information obtained, beyond what may be useful for the process, we understand that it would be appropriate to foresee its destruction in a peremptory term, existing in the case of non-compliance with the specific guarantee of *Habeas data*.

IV. Conclusion

Our analysis began by pointing out the importance of providing the state with new tools for the development of criminal investigations within the framework of the digital age. It is undeniable that criminal organizations make use of increasingly sophisticated technology both to plan and commit illicit acts and to ensure their impunity. Meanwhile, Argentina at the federal level has a criminal procedural code dating from the analogue era, when no one imagined the importance of a

[13] Cfr. Sueiro, D.C.; idem quotation 2. P. 76 and ss.
[14] Salt, M.; idem appointment 1. P. 182.
[15] Ipohorski, J.; "El derecho a la intimidad", In Gargarella, R. Guidi, S. (Dirs)*;* Comentarios de la Constitución de la Nación Argentina; Buenos Aires: La Ley, 2016. T. II. P. 506-507

disembodied entity as a computer data could have for the outcome of a criminal process. This led to the identification of the *Remote Forensic* as an extremely effective research tool, which allows us to obtain unique information regarding the test measures so far available in our system, but which has at the same time been recognized as potentially dangerous for the human rights. From there, we evaluated the particularities of this research measure, concluding that it is a particularly intrusive institute when compared with the search or the telephone intervention. Finally, we join the readings that advocate a restrictive regulation of the use of these tools, but without prohibiting the state the possibility of their use in criminal investigations.

We want to make it clear that it is not a question of the state renouncing morality in order to achieve greater effectiveness in its criminal policy. On the contrary, the temptation to move away from the legal framework in investigations of extremely serious acts, for example, of international terrorist networks operating in the region, is greater when the necessary tools are banned in an unreasonable form. Depending on this, what we propose is the regulation of cases where it is legitimate to go to the *Remote Forensic.*

To conclude, we want to retake a quote from Professor Pérez Barbera, who has pointed out that "*It is clear that, in a democratic and also technocratic society, proper regulation of the use of technology is necessary when it affects or can affect the individual. It is certainly not a question of thinking about the problem from a posture of aversion to technological advancement (...).”*[16]

[16] Pérez Barberá, G.; “La prueba como información y la “autodeterminación informacional” como derecho fundamental del imputado”, en Falcone, A. *et al.*; *Autores detrás del autor*; Buenos Aires: Ad Hoc, 2018. P. 647 y ss.