ARTIFICIAL INTELLIGENCE AND ADMINISTRATION OF JUSTICE

POLICING AND PREDICTIVE JUSTICE IN ARGENTINA

National AIDP-Team of Argentina

Principal Rapporteur: *Carlos Christian SUEIRO.*

National Team of Argentina: *Nora Alicia CHERÑAVSKY; Marcelo Alfredo RIQUERT; Carlos Christian SUEIRO; Colaboradores del Grupo Nacional; Brenda FLESLER; Santiago Exequiel GAMARRA CALELLO, Sol Noelí JUAN; María Cecilia NEGRI; Gregorio SCHUMACHER*

Abstract:

In Argentina, there is no nationwide legislation that comprehensively defines and regulates artificial intelligence (AI) across the entire country. There are no regulations regarding predictive policing or justice; instead, the legal framework for the use of such technologies stems, in any case, from international agreements. Frequently, these systems are not governed by any specific regulations. This is why there are only a few instances where the state has chosen to implement mechanisms through the deployment of AI. Nevertheless, the federal structure of the country, wherein each province has the autonomy to establish its own rules as long as they do not conflict with the Constitution of the Argentine Republic or federal laws, has enabled the implementation of predictive policing and justice systems through the deployment of AI in certain cities or provinces.

While there is no specific AI legislation in Argentina yet, it is worth mentioning that within the context of the creation of the NATIONAL ARTIFICIAL INTELLIGENCE PLAN in February 2019, the following was stated:

"Artificial intelligence can be defined as a discipline focused on developing computer systems capable of performing tasks that would normally require human intelligence, including visual perception, speech recognition, decision-making, or translation between different languages. AI is transitioning from traditional deterministic computing to addressing non-deterministic problems of increased complexity, enabling the identification of patterns in open and dynamic environments. This allows for the recognition of visual patterns, voice, natural language, and linking data through what is known as machine learning."

Because of the absence of regulations, there is no national approach established, primarily due to a significant political debate that takes into account various options and potential ways to regulate this matter. Nevertheless, it should be mentioned that, in related subjects, Argentine law has often legislated in a manner closely aligned with continental European law.

Therefore, considering the EU's approach of enacting specific legislation applicable to particular sectors within the broad spectrum of AI, it appears that a similar approach may be taken when developing national legislation.

I. <u>Predictive Policing</u>

As a matter of fact, the Argentine Republic lacks an official legal definition for Artificial Intelligence (AI) and its diverse applications, including "predictive policing."

Nevertheless, despite the absence of specific legislation, certain regions have started to implement predictive policing systems. Notable examples in this field are the City of Buenos Aires (CABA), the City of Mendoza, the City of Rosario, and the municipality of Tigre in the Province of Buenos Aires.

At national level, there is a remarkable precedent that, while not directly involving AI, holds significance due to its law enforcement authority and data analysis capabilities. This refers to Decree 1766/11, later amended by Decree 243/17, which established the "Federal Biometric Identification System for Security" (SIBIOS). Its primary objective is to offer a centralized information service related to individual genealogical and biological records. This system aims to facilitate effective and prompt verification in the realm of personal identification and forensic traces, ultimately enhancing the scientific investigation of crimes and supporting preventive security measures.

Concerning the specific application of facial recognition technology, its utilization for fugitive detection was officially authorized in the City of Buenos Aires (CABA) since April 2019, as outlined in Resolution 398/MJYSGC/1957.

The system operates through the Public Integrated Video Surveillance System of CABA and is used exclusively for tasks required by the Public Prosecutor's Office, the Judiciary of the Argentine Republic, the Provincial Judiciary and the Judiciary of the City of Buenos Aires. It is also used for the detection of individuals wanted exclusively by judicial order, registered in the National Rebellion and Capture Consultation System ("CONARC", for its acronym in Spanish). It is important to note that, unless authorized by court order, the inclusion of images and records of individuals not registered in CONARC is strictly prohibited. The system is integrated with all the records included in the National Rebellion and Capture Consultation System Database and with the biometric data consulted from the National Registry of Individuals.

More recently, the City of Buenos Aires established the general regulation of the "Comprehensive Public Security System" by virtue of the local law No. 6339 (published in the Official Gazette of the City of Buenos Aires dated 11/19/2020),

Book VII is focused on the "Comprehensive Public Video Surveillance System". It includes Section 474, which opens Title I, and regulates the utilization of video surveillance systems by the Executive Branch for recording images in public locations. It later addresses Sections 485 and 486, outlining the specific procedures for handling these images and the framework of protections for citizens' fundamental rights and public freedoms. This framework must be consistently upheld throughout the various phases of image recording and usage, as set forth in Section 475.

The utilization of the comprehensive video surveillance system is bound by the principles of proportionality and reasonableness, whether in its procedural or minimal intervention forms, as stipulated in Section 476). Section 489 designates the Ministry of Justice and Security as the governing body overseeing the "Public Comprehensive Video Surveillance System." It holds the responsibility for safeguarding the acquired images and managing their subsequent utilization, including rendering them obsolete or ensuring their destruction.

Regarding the regulatory references to "video surveillance systems," Section 480 states that they are understood to encompass any technical analogical means and, in general, any system that enables the recordings outlined in this Book. This also includes the Facial Recognition System for Fugitives (SRFP), which aims at identifying and recognizing individuals who are fugitives from the law based

on real-time analysis of video images. It also covers the Preventive System, which aims at identifying predefined patterns in live video images using analytical methods to prevent actions related to potential criminal activities, as well as the Forensic System, which aims at performing searches for predefined patterns using video images stored by urban surveillance camera devices.

Video Surveillance System in the City of Buenos Aires

The primary function of the comprehensive facial recognition system is to identify fugitives or individuals with arrest warrants. When a match is found, it sends an alert to law enforcement agencies, facilitating their apprehension and subsequent transfer to judicial authorities.

The existing facial recognition system, powered by artificial intelligence, is integrated into the Comprehensive Public Video Surveillance System[1]. It can rapidly identify the faces of individuals who are accused or have outstanding arrest warrants in less than half a second.

"This capability is made possible through a database provided by the Co.Na.R.C. (National Rebellion and Capture Consultation System), which maintains a database of images of criminals and operates under the jurisdiction of the Ministry of Justice of Argentina.[2]"

This electronic surveillance system operates through AI-assisted facial recognition, processing real-time images from 300 of the 6963 cameras installed by the government of the city of Buenos Aires in streets and subway stations[3].

To prevent widespread electronic surveillance of citizens in the City of Buenos Aires (CABA), the system exclusively identifies individuals present in the Co.Na.R.C. *(National Rebellion and Capture Consultation System)* database.

Public officials responsible for the system are bound by confidentiality, and any unauthorized data or image insertion, data disclosure, or illegitimate access to this system is considered a crime under Section 157 *bis* of the Criminal Code.

The electronic surveillance system utilizing AI-assisted facial recognition is complemented by:

1.- The Electronic License Plate Recognition System.

2. The Comprehensive Public Video Surveillance System.

3.- the *Mi Argentina App*[4].

---

[1] Cfr. SUEIRO CARLOS CHRISTIAN. "*Vigilancia electrónica y otros modernos medios de prueba*". Prólogos de Marcelo A. Riquert y Marcos G. Salt, 2ª Edición, Editorial Hammurabi, Buenos Aires 2019.

[2] GALLO DANIEL. "Seven fugitives have already been apprehended with the facial recognition system in Buenos Aires," published in the newspaper La Nación on April 25, 2019.

[3] See GALLO DANIEL. *"A facial recognition system to apprehend fugitives will be used for the first time"* as reported in the La Nación newspaper on April 24, 2019.

[4] The Mi Argentina application aims at modernizing the digital portability of essential documents for citizens, including: 1.- National Identity Document (DNI), 2.- Passport, 3.- CUIL Certificate (Unique Identification Code for Workers), 4.- Certificate of Disability, 5.- Transplant Credential y 6.- Driver's Licenses
Through the application, these documents can be displayed during police checks, even without the need for internet connectivity.
For more information, please visit the official website of the Argentine National Government www.argentina.gob.ar/aplicaciones-moviles.

The system was enhanced in 2020 in response to the COVID-19 pandemic. In addition to facial recognition cameras, it has been equipped with the capability for infrared temperature detection.[5].

Thermal cameras, combined with Artificial Intelligence (AI) software, can measure the body temperature of up to 20 people simultaneously, without physical contact, and with an error margin of less than 0.3 degrees Celsius.

Legal Framework:

At national level in Argentina, there are no specific legal regulations governing AI-based predictive policing surveillance systems.

Discussions regarding the protection of rights such as equality and non-discrimination are in their early stages and have only recently started to gain attention. It has been only three years since the first works on this topic began to be published in legal books and journals.[6]

The procedural criminal legislation in the Argentine Republic, including the Code of Criminal Procedure (Law No. 23984), the Federal Code of Criminal Procedure (Law No. 27063 as amended by Law No. 27482), and the Codes of Criminal Procedures of the provinces of the Argentine Republic, has not incorporated the use of predictive policing. Therefore, there is no specific framework for ensuring reliability, impartiality, and effectiveness in the use of such technology.

The lack of specific regulations regarding the application of this and other potential predictive policing systems raises numerous concerns. There is no established mechanism for controlling the data used, and transparency measures are insufficient to determine, for example, whether other state databases are being employed in conjunction with these systems.

In the supranational context in 2019, the OECD and its member countries, including Argentina, formally endorsed a series of general recommendations on Artificial Intelligence (AI) and agreed to adhere to international standards that ensure *"the design of AI systems makes them robust, secure, impartial, and reliable."*[7].

Furthermore, the Legislature of the City of Buenos Aires passed Law 6339 in October 2019, amending Law 5688, which regulates the use of the Comprehensive Public Security System, including the use of Facial Recognition System.

Nonetheless, there is currently no extensive and genuinely democratic debate on the topic, and the utilization of the surveillance system in the City of Buenos Aires is not without its share of criticism.

You can also refer to a news article in the newspaper LA NACIÓN titled *"Mi Argentina App: Todo lo que tenés que saber"*, dated February 12, 2019 and retrieved on Monday, April 29, 2019.

[5] Cfr. SUEIRO CARLOS CHRISTIAN *"Vigilancia electrónica asistida por inteligencia artificial (IA)"*. 1ª Edición, Editorial Hammurabi, Buenos Aires, 2020.

[6] AA.VV. RIQUERT MARCELO A. (Dirección) – SUEIRO CARLOS CHRISTIAN (Coordinación) *"Sistema Penal e Informática"* Nº, 1, 2, 3, y 4, 1ª Edición, Editorial Hammurabi, Buenos Aires, 2018, 2019, 2020 y 2021; as well as in the work of DANESI CECILIA C. (Dirección). *Inteligencia artificial, tecnologías emergentes y derecho. Reflexiones interdisciplinarias.* 1ª Edición, Editorial Hammurabi, Buenos Aires, 2020.

[7] https://www.oecd.org/centrodemexico/medios/cuarentaydospaisesadoptanlosprincipiosdelaocdesobreinteligenciaartificial.htm

Most of these criticisms revolve around various flaws or inaccuracies in facial recognition, which have hindered the system's deployment due to issues with the Comprehensive Facial Recognition System in the City of Buenos Aires (CABA).

Opposition to the Facial Recognition System is exemplified by the case of the Association for Civil Rights (ADC). Upon the system's implementation, the ADC initiated a declaratory action of unconstitutionality against the Government of the City of Buenos Aires. They argued that "*facial recognition, when used for police surveillance purposes, becomes an excessive technology that, in addition to lacking proper legal foundations, significantly infringes upon the constitutional rights and guarantees of all individuals living in the city.*" [8].

The system was also criticized by other civil society organizations, such as the Argentine Observatory of Information Rights (ODIA)[9]. The United Nations Special Rapporteur on the Right to Privacy, Joseph Cannataci, also expressed concerns. During his visit to Argentina, he questioned the "*proportionality of deploying technology with significant privacy implications to search a database of 46,000 individuals, which includes minors and individuals with minor offenses, and is not consistently updated and rigorously verified for accuracy*." [10]

The Office of the Ombudsman, an oversight body invited to audit the system, also provided comments and recommendations on its implementation.[11]

In terms of jurisprudence, the resolution of the 1st Instance Court in Administrative and Tax Matters No. 23, Secretariat No. 45, of the City of Buenos Aires, dated May 20, 2020, in the case *"Argentine Observatory of Information Rights O.D.I.A. v. GCBA on Access to Information"* is noteworthy. This case originated from a lawsuit filed by the Argentine Observatory of Information Rights against the Government of the City of Buenos Aires regarding a request for access to public information related to Resolution 398/MJYSGC/2019, which approved the implementation of the Facial Recognition System for Fugitives in the City. Along with the lawsuit, the plaintiff submitted a request for access to public information to the GCBA.

According to the judge's assessment, there were no responses to the following questions: 1.- What are the security and reliability protocols for capturing facial images 2.- Audit of data deletion 3.- Identification of individuals not included in the CONARC and National Criminal Record databases. 4.- Detection of the percentage of false positives., 5.- Determination of the agents receiving confidential information.

[8] See https://adc.org.ar/2019/11/06/el-reconocimiento-facial-para-vigilancia-no-pertenece-a-nuestro-espacio-publico/
[9] https://odia.legal/
[10] See https://www.cels.org.ar/web/2020/10/la-legislatura-portena-debe-rechazar-el-uso-de-la-tecnologia-de-reconocimiento-facial-para-la-vigilancia-del-espacio-publico/
[11] https://defensoria.org.ar/noticias/avanza-el-proyecto-para-modificar-el-sistema-de-seguridad/

II. Predictive Justice

As regards the legislation of the Argentine Republic, there is currently no legal definition of "Predictive Justice"

Nevertheless, two operational systems designed for "Predictive Justice" are currently in use. One is a government-developed system by the Public Prosecutor's Office of the City of Buenos Aires, known as *"Prometea"*, while the other is a private system called *"Sherlock Legal"*, owned by Albremática S.A., owner of the digital publisher ElDial.com.

Prometea

"Prometea is an AI created in Argentina, within the framework of the Public Prosecutor's Office of the City of Buenos Aires. The system was designed and implemented with the aim of optimizing the justice system, exponentially speeding up judicial processes for the benefit of citizens."[12]

By standardizing routine procedures and automating repetitive tasks, combined with its substantial capacity for processing and cross-referencing extensive interconnected databases, this system has successfully resolved 52% of the less complex cases that have been filed with the Deputy General Prosecutor's Office for Contentious Administrative and Tax Matters of the City of Buenos Aires.[13].

It is contended that from a technical standpoint, this artificial intelligence system can accomplish something beyond the capacity of any human operator within the administration of justice system. It can read, predict, draft, and resolve a judicial case in approximately 20 seconds, achieving an accuracy rate of 96%"[14]. Additionally, the AI possesses the capability to translate opinions, writings, or appeals into three languages: English, French, and Portuguese.

Prometea has the following distinctive features:

1.- It is an artificial intelligence system that operates under human supervision.

2.- It utilizes an integrated screen model, eliminating the need to switch between windows to search for information[15]. This simplifies the interface, making it more user-friendly and efficient.

3.- It can be operated by individuals who may have difficulties with typing due to disabilities, whether those difficulties are temporary or permanent.

[12] CORVALÁN JUAN GUSTAVO. *"Estados eficientes. La productividad del sector público"*, AA.VV. Algoritmolandia. Inteligencia Artificial para una integración predictiva e inclusiva de América Latina.1 Edición, Integración & Comercio # 44, Julio 2018, Editorial Planeta, Buenos Aires 2018, Pág 260.

[13] See CORVALÁN JUAN GUSTAVO. *"Estados eficientes. La productividad del sector público"*, AA.VV. Algoritmolandia. Inteligencia Artificial para una integración predictiva e inclusiva de América Latina.1 Edición, Integración & Comercio # 44, Julio 2018, Editorial Planeta, Buenos Aires 2018, Pág 261.

[14] See CORVALÁN JUAN GUSTAVO. *"Estados eficientes. La productividad del sector público"*, AA.VV. Algoritmolandia. Inteligencia Artificial para una integración predictiva e inclusiva de América Latina.1 Edición, Integración & Comercio # 44, Julio 2018, Editorial Planeta, Buenos Aires 2018, Pág 261.

[15] See CORVALÁN JUAN GUSTAVO. *"Estados eficientes. La productividad del sector público"*, AA.VV. Algoritmolandia. Inteligencia Artificial para una integración predictiva e inclusiva de América Latina.1 Edición, Integración & Comercio # 44, Julio 2018, Editorial Planeta, Buenos Aires 2018, Pág 262/ 263.

Thanks to the use of *"intelligence in the interface"*[16] users can interact simply by speaking through its voice recognition system.

Sherlock Legal

In early 2016, prompted by the Argentine private sector, the publisher ElDial.com introduced an AI-assisted program known as *"Sherlock Legal"*.

The legal aid *"Sherlock Legal"* is built on the basis of the jurisprudence database owned by the publisher and incorporates natural language processing (NLP) supported by AI, enabling automated knowledge extraction from legal texts.

The natural language processing (NLP) software employed by "Sherlock Legal" stems from IBM's Watson Legal due to a strategic partnership between Albremática S.A., the owner of ElDial.com, and IBM for the creation of this intelligent legal assistant. Consequently, AI-supported software *like IBM's Watson Legal can access and analyze ElDial.com's online legal library.*[17].

The intelligent legal assistant "Sherlock Legal" with AI-assisted NLP software can accomplish the following: 1.- Categorization of legal texts; 2.- Grouping of texts according to their content; 3.- Extraction of information from the text, distinguishing valuable data within unstructured text; 4.- Identification by extracting names of natural and legal persons; 5.- Identification of relationships and links between the identified subjects; 6.- Emotional and sentimental analysis through the use of grammar, semiotics, and psychology.

The Argentine-origin "Sherlock Legal" is quite similar to intelligent legal assistants like "Kleos" designed by the Anglo-Dutch firm Wolters Kluwer and "Legal One" from Editorial La Ley, under the Anglo-Canadian transnational corporation Thomson Reuters.

Both the AI-assisted systems *Prometea* and *Sherlock Legal* are not designed for risk assessment or for making judicial decisions.

Both systems were designed to streamline the handling of cases in the Public Prosecutor's Office of the Judiciary of the City of Buenos Aires (CABA) by automating the preparation of documents, opinions, requests, and appeals.

In the case of *Sherlock Legal*, its primary purpose is to enhance efficiency and provide dynamic solutions to lawyers by autonomously extracting information from cases and offering AI-assisted support in crafting legal submissions.

When developing the AI-assisted program for collaboration with the Public Prosecutor's Office of the City of Buenos Aires, *Prometea*, the following principles were established:

---

[16] See CORVALÁN JUAN GUSTAVO. *"Estados eficientes. La productividad del sector público"*, AA.VV. Algoritmolandia. Inteligencia Artificial para una integración predictiva e inclusiva de América Latina.1 Edición, Integración & Comercio # 44, Julio 2018, Editorial Planeta, Buenos Aires 2018, Pág 262/263.

[17] Cfr. GRANERO HORACIO R. *"La inteligencia artificial aplicada al Derecho y el dilema de los algoritmos inteligentes"*, artículo publicado en la obra de RIQUERT MARCELO A. (Director), SUEIRO CARLOS CHRISTIAN (Coordinador) "*Sistema Penal e Informática*" Nº3, 1ª Edición, Editorial Hammurabi, Buenos Aires, 2020.

1. Algorithmic transparency: refers to the requirement that the system should offer a clear and comprehensible explanation of the criteria it employs to arrive at a particular conclusion, recommendation, or outcome.

2. Algorithmic traceability: entails that the system must be capable of elucidating the technical operations employed from the initiation to the culmination of the process.

The book *"Prometea"* outlines the design of the algorithm's conversational assistant, emphasizing the incorporation of a white-box or algorithmic transparency system in its development[18]. Nevertheless, Prometea has not undergone any external certification or audit.

The same principles apply to the AI-assisted program from the private sector, Sherlock Legal, owned by Albremática S.A.

It is stated that a white-box or algorithmic transparency system has been utilized, but as of now, there has been no external audit.

Legal framework and soft law

There are no local regulations that govern the use of AI-based systems for predictive justice.

There is no legislation addressing the reliability, impartiality, equality, and adaptability of AI in this context.

III. Law of evidence

[18] AAVV. PROMETEA. Inteligencia artificial para transformar organizaciones públicas. 1ª Edición, Universidasd de Rosario, DPI Cuántico, IMODEV Improving Public Policies in a Digital World, Editorial Astrea, Buenos Aires, 2019, Pág 60.

To date, there hasn't been an extensive discussion regarding issues of equality or the right to non-discrimination in relation to the utilization of AI-based systems. Certain authors and organizations are endeavoring to kickstart this dialogue. As an illustration, you can examine the content of the book "Prometea," which states: "Prometea: Artificial Intelligence to Transform Public Organizations" contends that this system showcases remarkable outcomes by streamlining processes, minimizing errors, and expediting document development, which profoundly influences the effectiveness of rights overall, especially the principles of equality and legal certainty. This is attributed to the substantial presence of jurisprudential precedents. It is contended that a 96% probability of substantial case similarity, coupled with the use of the same response, serves to safeguard the mentioned principles.
Nonetheless, as previously noted, these findings lack external scrutiny, particularly concerning the broader issue of whether the equal and expedited treatment of all cases eliminates the potential for discrimination and the adoption of underlying legal-ideological stances that may ultimately perpetuate social inequalities.
Its creators have aimed at preventing this problem and state that, for the development of Prometea, they have established the principles of: 1. Algorithmic Transparency: this means that the system should provide an understandable explanation of the criteria it relies on to reach a specific conclusion, suggestion, or outcome; 2. Algorithmic Traceability: the system should have the capability to elucidate the technical procedures employed from the commencement to the conclusion of the process; 3. Non-discrimination Algorithm: this entails ensuring that AI systems do not process information or data with biases or distinctions based on factors such as race, color, sex, language, religion, socio-economic status, political opinion, and other factors.

To date, digital evidence is not specifically provided for in the federal codes of criminal procedures of the Argentine Republic.[19] This is considered a pending matter, especially taking into account the incorporation of the Budapest Convention on Cybercrime into the local legal framework on November 22, 2017, through Law No. 27411. It is constitutionally and traditionally required to adapt the criminal procedural system to the requirements of the second section of this convention.

From a historical perspective, it is reasonable and logical to understand that the initial Code of Criminal Procedure of the Argentine Republic did not address this matter.

The first Code of Criminal Procedure of the Argentine Republic known as the *Code of Criminal Procedure* (Law 2372)[20], enacted on October 4, 1888, and in force until 1991, followed an inquisitorial system of adjudication.

For most of its period of validity, information technology and communication technologies (ICT) had not even been developed, making it materially unfeasible to foresee this type of evidence.

Similarly, the second *Code of Criminal Procedure of the Argentine Republic* (Law No. 23984)[21], which has been in effect since 1991, did not incorporate provisions for the admission of electronic evidence.

The reason for not including digital evidence in the title of means of proof at the time of its enactment, promulgation, and enforcement was that information and communication technologies (ICTs) were just beginning to emerge in the 1990s. It was only in 1996, following the arrival of the *Internet* in our country, that the first bills related to the incorporation of criminal offenses related to cybercrime into the Criminal Code of the Argentine Republic began to be discussed.

So far, we have relied on the regulatory criteria of the scope of evidence and the truthfulness or seriousness of evidence of this nature or acquired through AI. Such evidence has been accepted, and its probative value depends on the examination by experts who provide it with authenticity and credibility. To put it differently, this kind of evidence is admitted just like any other, following the principles of evidentiary freedom and rational evaluation.

The new Federal Code of Criminal Procedure (Law No. 27063, amended by Law No. 27482) has not included any particular regulations concerning the specific methods for acquiring digital evidence stored on diverse electronic devices or computer equipment, and this issue remains pending to date. It only provides a very general reference to data seizure in Section 151[22].

Most provinces in the Argentine Republic (each with its own code of criminal procedure) have not yet adapted their criminal procedural legislation to the requirements of the Budapest Convention on

[19] In the Argentine Republic, there are currently two Federal Codes of Criminal Procedure in force.

[20] Code of Criminal Procedure, Law 2372. Enacted on October 4, 1988, and promulgated as of January 1, 1989.

[21] Code of Criminal Procedure of the Argentine Republic. Law 23,984. Enacted on August 21, 1991, and promulgated on September 4, 1991

[22] Section 151 – *CPPF (Federal Code of Criminal Procedure, for its acronym in Spanish) "The judge may, at the request of a party and by means of a well-founded order, order the search of a computer system or a part thereof, or of a data storage medium for computer or electronic data, to seize the components of the system, obtain a copy, or preserve data or elements of interest for the investigation, under the conditions set forth in Section 136."*

The same limitations established for the seizure of documents will apply.

The examination of the objects, documents, or the results of intercepted communications will be carried out under the responsibility of the requesting party. Once the components of the system are seized or a copy of the data is obtained, the rules for opening and examining correspondence will apply.

The return of components that are unrelated to the case will be ordered, and copies of the data will be destroyed. The interested party may appeal to the judge to obtain the return of the components or the destruction of the data."

Cybercrime (2001), which, as mentioned, was incorporated into our legal system through Law No. 27411 on November 22, 2017.

These tools are often in the possession of security forces such as: 1. - the Federal Police of Argentina (PFA), National Gendarmerie of Argentina (GNA), Argentine Naval Prefecture (PNA), Airport Security Police (PSA), and the Police of the City of Buenos Aires (PCABA).

They are also commonly used by the Public Prosecutor's Offices of the Argentine Republic, City of Buenos Aires, and various provinces, including Buenos Aires, Cordoba, Corrientes, Neuquen, Mendoza, Rio Negro, Santa Fe, San Juan, San Luis, and Tucuman.

The flagship forensic program used at national level for smartphones and tablets forensic analysis is the UFED program.

The name UFED stands for Universal Forensic Extraction Device.

The UFED program, developed by Cellebrite, like any forensic program, performs three basic steps:

1. - Preservation: This step involves reviewing and generating forensic images of the evidence to enable analysis. Cutting-edge technology is employed for the duplication process to ensure both the integrity of the evidence and the necessary chain of custody. Creating a forensic image involves generating a *"bit-by-bit"* copy of the entire disk, enabling the retrieval of all information, including deleted data, from the hard drive.

This technique is known as Mirror Image, a bit-by-bit copy of an electronic storage medium. The image includes the spaces occupied by files and deleted areas, including hidden partitions.

2. – Analysis: this is the process of applying scientific and analytical techniques to the duplicated media by means of forensic processing to find evidence of certain behaviors. Searches for character strings, specific actions of the user(s) such as the use of USB devices (brand, model), searching for specific files, recovering and identifying emails, recovering the last visited sites, recovering Internet browser cache, among others, can be performed.

3.- Presentation: it involves collecting all the information obtained from the analysis to create a report and presentation for lawyers, the generation of an expert report, and its proper interpretation without using technical jargon.

The UFED forensic program allows the retrieval of the following data from any mobile device:

1.- Recovery of deleted files;

2.- Verification of file signatures;

3.- The ability to search, filter, and organize files according to different criteria for a clearer case view;

4.- Temporal reconstruction;

5.- Recovery of partitions;

6.- Support for *log* analysis;

7.- Internet analysis toolkit;

8.- Creating the image in Raw or Split format;

9.- Facilitating information retrieval in the stack space (Data Carving);

10.- Detection of information in the spaces between partitions;

11.- Instant messaging data (WhatsApp, Telegram, WeChat, Snapchat);

12.- Social media chat data (Facebook, Instagram, LinkedIn, TikTok, Kwai, VK);

13.- Information from the SIM card;

14.- Data saved in the calendar;

15.- Data of connections with other devices through synchronization.

Thus, the prevailing doctrine in the field of forensic computing highly recommends the use of the UFED program for examining smartphones, particularly smartphones. *UFED* is a forensic tool that enables the comprehensive analysis of the content stored on a wide range of cell phones, including models from various manufacturers available in the international market. This includes smartphones of Chinese origin like Huawei, OPPO, and Xiaomi. UFED is considered a valuable resource for conducting forensic examinations of mobile devices.[23]

Conclusion:

In Argentina, there is no nationwide regulation that provides specific definitions and limitations for the use of AI-based systems. This means that each jurisdiction in Argentina can implement its own system of predictive policing and justice, as long as it doesn't contradict national legislation and respects basic rights and guarantees.

It is indeed necessary for lawmakers to regulate this issue as soon as possible. The creation of a concrete legal framework is essential to protect the security and privacy of citizens while also enabling security agencies and the judiciary to carry out their tasks more effectively.

23 See PICCIRILLI, DARIO A. *"La Forensia como Herramienta en la Pericia Informática"*, Revista Latinoamericana de Ingeniería de Software, Buenos Aires, 2013, 1(6): 237-240, ISSN 2314-2642; Págs. 238/239.