InFo-Conf 2024

VIII CONFERENCIA NACIONAL DE INFORMÁTICA FORENSE

PROCEEDINGS

DIIT
Departamento de Ingeniería e Investigaciones Tecnológicas

UNIVERSIDAD NACIONAL DE LA MATANZA
UNLaM
1989
REPÚBLICA ARGENTINA

RED UNIF
RED UNIVERSITARIA DE INFORMÁTICA FORENSE

DIIT
Departamento de Ingeniería e Investigaciones Tecnológicas

Autoridades

I. Autoridades del congreso

Prof. Dr. Daniel Martinez	*Rector*
Dr. Fernando Luján Acosta	*Vicerrector*
Mag. Gustavo Duek	*Vicerrector Ejecutivo*
Dr. Ing. Gabriel Blanco	*Decano Dto. de Ingeniería e Investigaciones Tecnológicas*
Mag. Ing. Jorge Eterovic	*Vicedecano Dto. de Ingeniería e Investigaciones Tecnológicas*
Dra. Bettina Donadello	*Secretaria de Investigaciones*
Mag. Ing. Carolina Vicente	*Secretaria Académica*
Mag. Cdora. Mariángeles Vanesa Gallo	*Secretaria Administrativa y de Extensión Universitaria*

II. Dirección del congreso

Mag. Ing. Cintia V. Gioia (DIIT-UNLaM)	*Presidente*

III. Comité Académico

Jorge Eterovic	*Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de la Matanza (DIIT-UNLAM)*
Cintia Gioia	*Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de la Matanza (DIIT-UNLAM)*
Emiliano Zárate	*Departamento de Ingeniería e Investigaciones Tecnológicas de la*

	Universidad Nacional de la Matanza (DIIT-UNLAM)
Marcos Acevedo	*Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de la Matanza (DIIT-UNLAM)*
Ana Di Iorio	*Facultad de Ingeniería de la Universidad FASTA (FI-UFASTA)*
Bruno Constanzo	*Facultad de Ingeniería de la Universidad FASTA (FI-UFASTA)*
Roberto Giordano Lerena	*Facultad de Ingeniería de la Universidad FASTA (FI-UFASTA)*
Miguel Solinas	*Facultad de Ciencias Exactas, Físicas y Naturales de la Universidad Nacional de Córdoba (FCEFYN-UNC)*
Alejandro Ambrosini	*Facultad de Ciencias Exactas, Físicas y Naturales de la Universidad Nacional de Córdoba (FCEFYN-UNC)*
Eduardo Casanovas	*Facultad de Ingeniería, Centro Regional Universitario Córdoba del, Instituto Universitario Aeronáutico, Universidad de la Defensa Nacional (CRUC-IUA - UNDEF)*
Natalia Mira	*Facultad de Ingeniería, Centro Regional Universitario Córdoba del, Instituto Universitario Aeronáutico, Universidad de la Defensa Nacional (CRUC-IUA - UNDEF)*
Sergio Appendino	*Facultad de Ingeniería de la Universidad Católica de Salta (FI-UCASAL)*
Beatriz Parra de Gallo	*Facultad de Ingeniería de la Universidad Católica de Salta (FI-UCASAL)*
Carla Carrillo	*Facultad Regional Delta de la Universidad Tecnológica Nacional (UTN-FRD)*
Lorena Franco	*Facultad Regional Delta de la Universidad Tecnológica Nacional (UTN-FRD)*

Marcelo Cipriano	*Facultad de Ingeniería del Ejército Argentino de la Universidad de la Defensa Nacional (FIE-UNDEF)*
Alberto Cisternas	*Facultad de Ingeniería del Ejército Argentino de la Universidad de la Defensa Nacional (FIE-UNDEF)*
Jorge Kamlofsky	*Universidad Abierta Interamericana (UAI)*
Raúl Romero	*Universidad Abierta Interamericana (UAI)*
Germán Parisi	*Facultad Regional Córdoba de la Universidad Tecnológica Nacional (UTN-FRC)*
Leonardo Ciceri	*Facultad Regional Córdoba de la Universidad Tecnológica Nacional (UTN-FRC)*
Claudia Russo	*Escuela de Tecnología y Escuela de Ciencias Económicas y Jurídicas de la Universidad Nacional del Noroeste de la Provincia de Buenos Aires (ET y ECEyJ - UNNOBA)*

IV. Autoridades de la Red UNIF

Mag. Ing. Cintia V. Gioia (DIIT-UNLaM)	*Presidente*
Ing. Bruno Constanzo (FI-UFASTA)	*Vicepresidente*
Ing. Carla D. Carrillo (UTN-FRD)	*Secretaria*

V. Comité Organizador

Mag. Miriam Barone	*Integrante*
Ing. Maximiliano Guasco	*Integrante*

Mag. Julieta Spinazzola	*Integrante*
Mag. Laila Tassara	*Integrante*
Lic. Yamila Tesolin	*Integrante*
Lic. Natalia Salcovsky	*Integrante*
Marcelo Goncalves	*Integrante*
Ing. Juan Ojeda	*Integrante*

Gioia, Cintia

INFO-CONF 2024: VIII conferencia nacional de informática forense / Cintia Gioia. - 1a ed. - San Justo: Universidad Nacional de La Matanza, 2025.

Libro digital, PDF

Archivo Digital: descarga y online

ISBN 978-631-6611-69-7

1. Nuevas Tecnologías. 2. Ingeniería Informática. I. Título.

CDD 005.1

Autor

Mag. Cintia Gioia

Comité editorial

Responsable de edición

Dra. Bettina Laura Donadello

Editor

Mag. Cecilia Gargano

Diseño

Lic. Yamila Tesolin

PRÓLOGO

En este volumen se presentan las conferencias desarrolladas en el Congreso de informática Forense que tuvo lugar en la Universidad Nacional de La Matanza, organizado por el Departamento de Ingeniería e Investigaciones Tecnológicas en septiembre de 2024, con la colaboración de la Facultad Regional Delta de la Universidad Tecnológica Nacional

Se trata de un evento anual que convoca a referentes de la Informática Forense en temas de sus diversas especialidades, con el objetivo de generar un ámbito para el intercambio de experiencias, difusión e impulso de actividades para promover la integración y cooperación interinstitucional, en el campo de la Informática Forense.

Este libro de actas muestra como en la Conferencia se abordaron las temáticas de Informática Forense y Pericial, Aspectos Legales y Procesales de la Actuación Forense, Ciberseguridad y Ciberdefensa, a través de la disertación de destacados profesionales propios de la Universidad y externos, del ámbito nacional e internacional, con la exposición de artículos presentados, mesas de debate y además un trayecto formativo formado por cursos de capacitación.

El evento estuvo dirigido a profesionales, investigadores, docentes y alumnos de carreras afines a la formación en Informática y Tecnología del Derecho, Criminalistas, Peritos, Operadores del Sistema Judicial, Personal de las Fuerzas de Seguridad y de diversos organismos públicos y privados que se desempeñan en un rol o área afín, como también a profesionales idóneos vinculados con las disciplinas que se abordan.

La Conferencia es impulsada por la Red Universitaria de Informática Forense (Red UNIF), con el objetivo de generar un ámbito para el intercambio de experiencias, difusión e impulso de actividades, profundización del conocimiento a partir del debate, y la generación de lazos de cooperación y acuerdos interinstitucionales que favorezcan la realización de proyectos compartidos.

En cada edición, una de las unidades académicas integrantes de la red de unidades académicas e institutos de investigación universitarios que promueven la integración y cooperación interinstitucional en el campo de la Informática Forense (UNIF), es anfitriona del evento.

Dr. Ing. Gabriel Blanco
Decano

Mag. Ing. Jorge Eterovic
Vice Decano

Ing. Alfredo Vazquez
Prof. Emérito

InFo-Conf 2024
VIII CONFERENCIA NACIONAL DE INFORMÁTICA FORENSE

2024 InFo-Conf
BUENOS AIRES

26 Y 27 SEPTIEMBRE
09:00 A 18:30 HS.

PRESENCIAL Y VIRTUAL

ORGANIZADORES

UNLaM · DIIT Departamento de Ingeniería e Investigaciones Tecnológicas · RED UNIF Red Universitaria de Informática Forense

PROCEEDINGS

Ejes temáticos

- Informática Forense y Pericial
- Aspectos Legales y Procesales
- Ciberseguridad
- Ciberdefensa

https://info-conf2024.unlam.edu.ar

Auspiciantes

CONICET · Programa Nacional de Ciencia y Justicia · Ministerio Público Provincia de Buenos Aires · FRED UTN · RedUNCI · confedi Auspicio Institucional · DDCP Dto. de Derecho y Ciencia Política · InFo-Lab · OCEDIC · COPITEC

Sponsors

CrimL4b Consultora Forense Digital · CIBERPRISMA Alianza por la Ciberseguridad

Agradecemos a las siguientes instituciones que nos acompañaron:

Auspiciantes

Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Programa Nacional de Ciencia y Justicia, Consejo Federal de Decanos de Ingeniería de la República Argentina (CONFEDI), Ministerio Público de la Provincia de Buenos Aires (MPBA), Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab), Observatorio de Cibercrimen y Evidencia Digital en Investigaciones Criminales (OCEDIC), Consejo Profesional de Ingeniería de Telecomunicaciones, Electrónica y Computación (COPITEC), Instituto de Ciencias Forenses de la Universidad Fasta, Red de Universidades con Carreras en Informática (Red UNCI), Colegio de Abogados de La Matanza, Departamento de Derecho y Ciencia Política de la Universidad Nacional de la Matanza, Facultad Regional Delta (FRD.UTN).

Sponsors

Ciberprisma. CrimL4b. RecuperaDatos.com

INDICE

Contenido

Acerca de InFo-Conf y Red UNIF

La **Conferencia Nacional de Informática Forense (InFo-Conf)** es impulsada por la **Red Universitaria de Informática Forense - Red UNIF** y convoca a los mayores referentes de la Informática Forense, la Investigación Criminal Informática, la Ciberseguridad y en general la Tecnología y el Derecho en las ciencias de aplicación forense con el objeto de generar un ámbito para el intercambio de experiencias, difusión e impulso de actividades, profundización del conocimiento a partir del debate y generación de lazos de cooperación y acuerdos interinstitucionales que favorezcan la realización de proyectos compartidos, agregando valor a los esfuerzos individuales.

La primera edición de la InFo-Conf se llevó a cabo en el 2017 con la iniciativa del Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense (InFo-Lab), la Facultad de Ingeniería de la Universidad FASTA y la Red Universitaria de Informática Forense (Red UNIF).

El objetivo de la InFo-Conf es el intercambio de conocimiento y experiencias entre profesionales que abordan los principales desafíos que presenta el campo de la Informática Forense y las distintas disciplinas auxiliares que convergen en ella. Es un espacio multidisciplinario que posibilita profundizar y actualizar el conocimiento a partir del debate y generación de lazos de cooperación, delinear acuerdos interinstitucionales y potenciar el rol de los diferentes actores de la especialidad en la investigación, extensión y actividades académicas y profesionales.

La InFo-Conf se organiza anualmente convocando a las Universidades Nacionales e Internacionales, profesionales, docentes, alumnos y a diferentes organismos e instituciones interesados en las temáticas que se abordan en la misma.

La **Red Universitaria de Informática Forense (Red-UNIF)** es una red de unidades académicas e institutos de investigación universitarios que promueve la integración y cooperación interinstitucional en el campo de la Informática Forense. Surgió en mayo de 2017 como un acuerdo constitutivo conformado por siete universidades públicas y privadas en el marco de la Primera Conferencia Nacional de Informática Forense (Info-Conf) realizada en la ciudad de Mar del Plata.

La Red busca promover la integración y cooperación interinstitucional en el campo de la Informática Forense mediante la contribución, desde la Universidad, a la mejor actuación de los peritos informáticos en particular y de la Justicia en general; el establecimiento de un ámbito universitario permanente de encuentro para el desarrollo conjunto de proyectos de investigación y de tecnología en el campo de la Informática Forense. También impulsa la generación de programas de movilidad,

actualización profesional, docencia de grado y postgrado entre docentes e investigadores en este campo disciplinario y la promoción de publicaciones, actividades y reuniones académicas, científicas, de extensión, de divulgación y de transferencia interinstitucionales.

Autoridades Red UNIF:

- Presidente: Mag. Ing. Cintia V. Gioia (DIIT-UNLaM)
- Vicepresidente: Ing. Bruno Constanzo (FI-UFASTA)

Enlaces de Interés:

- https://info-conf2024.unlam.edu.ar/es/acercade.html
- https://info-conf2024.unlam.edu.ar/es/redunif.html

Edición 2024

La **octava edición de la InFo-Conf (InFo-Conf 2024)** se desarrolló los días 26 y 27 de septiembre de 2024 en la Universidad Nacional de La Matanza, con formato híbrido. Organizada por el **Departamento de Ingeniería e Investigaciones Tecnológicas (DIIT) de la Universidad Nacional de La Matanza**.

Durante las dos jornadas se llevaron a cabo diversas **disertación de profesionales**, presentación de casos de estudio reales, exposición de trabajos de investigación, mesas de debate y el dictado de workshops a cargo de los referentes más destacados de la informática forense, la ciberseguridad, la investigación criminal informática, la tecnología y el derecho en las ciencias de aplicación forense.

Las actividades se desarrollaron de acuerdo a **4 ejes temáticos principales**: Informática Forense y Pericia, Aspectos Legales y Procesales de la Actuación Forense, Ciberseguridad y Ciberdefensa.

Se contó con **disertantes y asistentes a nivel nacional e internacional**.

Estuvo **dirigida** profesionales de carreras afines a la formación en Informática y Tecnología, del Derecho, criminalistas, peritos, operadores del sistema judicial, personal de las fuerzas de seguridad y de diversos organismos públicos y privados que se desempeñan en un rol u área afín, como también profesionales idóneos vinculados a las disciplinas que se abordan. También a nuestra comunidad educativa pudiendo asistir tanto docentes como alumnos interesados en las temáticas que se tratarán en la misma.

A continuación, les presentamos las **ponencias** de ambas jornadas y los **artículos aceptados** en la conferencia.
https://info-conf2024.unlam.edu.ar/

PONENCIAS

Ponencias

Ponencias del JUEVES 26 DE SEPTIEMBRE

Pedro Janices - "Del Caos al Orden"

YouTube https://youtu.be/XXFjOf67UPY?si=B442Y3PucDV6Eie8

Dr. Manuel de Campos - "Investigación de Cibercrimen - Evidencia Digital - Medidas Especiales"

YouTube https://youtu.be/Hsg4KzUSWhs?si=Jz8s3WY8NZmtPx4W

Agente Esp. FBI Alexis Brignoni. "Perito de "Click" o peritos. El Rol del Analista Forense Digital más allá de las herramientas."

YouTube https://youtu.be/CRsa7NtRsEU?si=07C7udROC9JlHXRq

Policía Suecia Eduardo Grutzky - "Proteger a los que protegen".

YouTube https://youtu.be/Gt_048LkACI?si=nJ3V2Js9n4k_lG3h

Ing. Adrián Eduardo Acosta -"Siguiendo las huellas criminales".

YouTube https://youtu.be/9eJHjnPr8Xc?si=mNXzTa_MH0ylxJKM

Dr. Horacio Azzolin - "Criptocrimen en Latinoamérica".

YouTube https://youtu.be/s3ALKJwF4KI?si=845UY4A3KHgQXtfz

Lic. Emiliano Zárate - "El reloj del crimen, cómo las líneas de tiempo transforman la inv. forense digital".

YouTube https://youtu.be/CpnKs5ShKYg?si=5KxSbeb1asnn0fD6

Ing. Emiliano Piscitelli - "Evolución de los ciberdelitos y actores de amenazas en la región".

YouTube https://youtu.be/MUQEgrq1Bc0?si=2SK16fwVtFoGmsMM

Lic. Antonio Maza - "El mindset del analista forense digital".

YouTube https://youtu.be/vyohENQUH3s?si=aZ-yCK9YzJ3tTCmM

Dr. Martín Leguizamón - "Derecho al Olvido: Caso Pompilio y Denegri".

YouTube https://youtu.be/7ytwC-FNokQ?si=y0wHsG_8ADY1-n-f

Crio. Maximiliano Méndez - "Investigaciones Cripto, desde el enfoque policial".

https://youtu.be/I8z37YNrv70?si=jzZouhfixNFvlN3Q

Ing. Emiliano Moraña - "Transformando la revisión y el análisis de la evidencia digital mediante la aplicación de nuevas tecnologías".

https://youtu.be/76NnzqAI8Dg?si=Z802HE-HlStY4xpk

Ing. Bruno Constanzo y la Lic. Belén Álvarez - "Guía para la adq., preservación y presentación de la evidencia digital".

YouTube https://youtu.be/5AQ-YUBVmMM?si=op6ABxaDe9CesXc2

Ponencias del VIERNES 27 DE SEPTIEMBRE

Dra. Daniela Dupuy, OCEDIC y UFEDyCI - "Presentación de la Evidencia Digital en el Juicio Oral".

YouTube https://youtu.be/cPyPKw1Sj6w?si=IjvfSHS9hwpdPQe4

Dr. Francisco Pont Verges - "Pericias informáticas, análisis e inteligencia artificial".

YouTube https://youtu.be/OJ5sFm6yjYM?si=ImHx5XAQ9a3j-kAC

Disertación del Comisario Víctor Aquino y del Subof. Escrte. Walter Núñez, Policía Federal Argentina - "Resolución 232/23. Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital para la investigación Criminal".

YouTube https://youtu.be/bhKqplXQ_0w?si=ZZrfO7mZvaU0C3Js

Eduardo Moya Rojas, Poder Judicial Costa Rica - "Caso RAM 911 (relacionado con niños, niñas y adolescentes)".

YouTube https://youtu.be/1kk2Seu8HM4?si=WcG-CVPzX8lbALuT

Ing. Diego Bucci - "Ingeniería Inversa aplicada a Telefonía Celular".

YouTube https://youtu.be/ZuSdmbrEGqs?si=orRC-GDKrREs4RL7

Lic. Matías Noguera Fernández y Juan Pablo Delord - "Desenmascarando la Oscuridad: Técnicas Avanzadas de Investigación en la Dark Web".

YouTube https://youtu.be/_diNmpWoJwA?si=8hSVAKfBLXzkwaHU

Ing. David Alejandro Fuentes - "La Trazabilidad en el Laboratorio de Informática Forense".

YouTube https://youtu.be/AdjbpZICB04?si=LRw9Jf6fjL7_d8uz

Ing. Juan Manuel Beltrán - "El Phishing como puerta de acceso para los Delitos Informáticos".

YouTube https://youtu.be/BzIxnmTAB-0?si=Kk9deWeYLiU_3O33

Braian Arroyo - "Investigaciones a través del prisma de la Ciberinteligencia".

YouTube https://youtu.be/8PS8N5T-8dg?si=0PvgrwpJDWo_1I0b

Panel CONICET

Dr. Willy Pregliasco y Dr. Martin Onetto - "Residuos de Disparo: Machine Learning aplicado al historial de pericias".

Dr. Jorge Gurlekian - "Protocolo sobre pericias de voz".

Dr. Ing. Pablo Negri - "Marco para evaluar la proporcionalidad en el uso de sistemas de reconocimiento facial".

YouTube https://youtu.be/_diNmpWoJwA?si=8hSVAKfBLXzkwaHU

Lic. Patricia Delbono - "Investigación Criminal de las Falsas Acusaciones. El precio oculto de justicia".

YouTube https://youtu.be/MxR4Rxz6sMg?si=jJ3Rg9-HcxBzvvP7

Mg. Lic. Gustavo Sain - "Inteligencia Artificial, Ciberdelito y Derecho".

Dra. Brenda Eldrid - "Algoritmos y Defensa en Juicio. Herramientas para una defensa eficaz".

YouTube https://youtu.be/HXEzWlD-WSk?si=SvEiYG6sERJJoxQG

Mg. Ing. Cintia Gioia, Ing. Bruno Constanzo, Dr. Alan Temiño, Mg. Ing. Gabriel Blanco, Dr. Luis Deuteris - Acto Apertura y Cierre InFo-Conf 2024

YouTube

https://youtu.be/5zvgckY1apY?si=0JeRnhio2DRu3bvc

https://youtu.be/N_nmEQGXvCI?si=SMSCx3GGc6phJJUr

Publicaciones

Papers

Tablero de control para despliegue proporcionado de sistemas de reconocimiento facial en escenarios de vigilancia urbana

Pablo Negri
Instituto de Investigación en Ciencias de la Computación
Departamento de Computación, FCEyN
CONICET- Universidad de Buenos Aires (UBA)
Buenos Aires, Argentina
pnegri@dc.uba.ar

Isabelle Hupert
Joint Research Centre (JRC)
European Commision
Sevilla, España

Emilia Gomez
Joint Research Centre (JRC)
European Commision
Sevilla, España

***Abstract*—El reconocimiento facial (FR por sus siglas en inglés) ha alcanzado una alta madurez técnica. Sin embargo, su uso debe evaluarse cuidadosamente desde una perspectiva ética, especialmente en escenarios sensibles. Este es precisamente el enfoque de este artículo: el uso de FR para la identificación de sujetos específicos en espacios de circulación moderada hasta densa (por ejemplo, espacios públicos, estadios deportivos, estaciones de tren). En particular, es necesario considerar el equilibrio entre la necesidad de proteger la privacidad y los derechos fundamentales de los ciudadanos, así como su seguridad. Las políticas recientes de Inteligencia Artificial (IA), en particular la Ley Europea de IA (AI-Act), proponen que dichas intervenciones de FR sean proporcionadas y se implementen solo cuando sea estrictamente necesario. Sin embargo, hasta la fecha faltan directrices concretas sobre cómo abordar el concepto de intervención proporcional de FR. Este artículo propone un tablero de control para contribuir a evaluar si una intervención de FR es proporcionada o no para un contexto de uso determinado en los escenarios mencionados anteriormente. También identifica las principales variables cuantitativas y cualitativas relevantes para la decisión de intervención de FR (por ejemplo, número de personas en la escena, nivel de daño que las personas buscadas podrían perpetrar, consecuencias para los derechos y libertades individuales) y propone un modelo gráfico 2D que permite equilibrar estas variables en términos de coste ético versus incremento de seguridad. Finalmente, diferentes escenarios de FR inspirados en implementaciones del mundo real validan el modelo propuesto. El tablero de control está concebido como una simple herramienta de apoyo para los tomadores de decisiones cuando se enfrentan al despliegue de un sistema FR.**

***Index Terms*—Reconocimiento Facial, Tablero de Control, Invasión de Privacidad, Uso Proporcional y Etico, Escenarios Reales**

I. Introducción

El reconocimiento facial (FR) es una tecnología biométrica flexible capaz de identificar personas a distancia, incluso sin la cooperación activa de los sujetos fotografiados. En la última década, los sistemas FR se han utilizado para muchos propósitos diferentes, como el control de acceso[18], control de fronteras [7], desbloqueo de dispositivos/máquinas [38], control de asistencia [34], identificación de personas desaparecidas [26] y etiquetado de rostros [3].

Este artículo se centra en la aplicación de la tecnología de reconocimiento facial (FR) más avanzada técnicamente, aunque éticamente controvertida: su uso en tiempo real para identificar sujetos específicos en espacios moderadamente concurridos o muy concurridos (por ejemplo, espacios públicos abiertos, estadios deportivos, estaciones de tren, aeropuertos, centros comerciales) con fines de garantía del cumplimiento del Derecho. Estos escenarios de FR normalmente hacen uso de un sistema multicámara para identificar personas que suponen una amenaza potencial (por ejemplo, ladrones, criminales o terroristas que figuran en los registros policiales) o que están siendo buscadas (por ejemplo, personas desaparecidas o secuestradas) a través de múltiples transmisiones de vídeo. Los productos de software concebidos para este propósito específico están muy extendidos en el mercado [14] y son utilizados por fuerzas de seguridad encargados de hacer cumplir la ley en todo el mundo.

Desde una perspectiva técnica, hoy en día, los sistemas de FR funcionan con éxito incluso en situaciones no controladas, con decenas o cientos de personas en la escena, condiciones de iluminación cambiantes y resoluciones faciales bajas. Los algoritmos de identificación facial de última generación logran métricas de precisión superiores al 95% con una tasa de falsos positivos de 10^{-4} en estos contextos [6], [20]. Por otro lado los sesgos demográficos (por ejemplo, los prejuicios raciales y de género) siguen siendo una importante área de investigación dentro del FR [13], [31], y se están desarrollando algunas medidas de mitigación y además de crear conciencia sobre este asunto y fomentando su investigación [12].

Si bien la solidez algorítmica y la equidad son, sin duda, requisitos clave para el desarrollo de sistemas FR, los aspectos éticos críticos relacionados con las fases de implementación han sido ampliamente subestimados. Incluso suponiendo que un sistema de FR sea casi perfectamente preciso, justo y utilizado por las autoridades con el exclusivo propósito de

Las opiniones expresadas en esta publicación científica son exclusivamente las de los autores y en ningún caso pueden considerarse como una posición oficial de la Comisión Europea.

mejorar la seguridad pública, su uso implica inevitablemente una invasión de la privacidad, ya que los rostros de todas las personas que pasan por una zona designada se procesan para buscar una posible coincidencia con una persona en una lista de vigilancia. En este escenario, es posible que los individuos capturados no deseen estar bajo vigilancia FR y que no estén al tanto de su funcionamiento. También pueden verse afectados otros derechos, como el *derecho a la libertad de expresión, reunión pacífica y asociación, así como a la libertad de circulación*, según [37]. Por lo tanto, la autoridad a cargo del despliegue del sistema debería establecer los mecanismos más estrictos para preservar la privacidad y evaluar cuidadosa-mente el uso de estas tecnologías considerando la relación entre *seguridad y privacidad (o, más ampliamente, derechos fundamentales)*.

Las políticas recientes de inteligencia artificial (IA) que abordan la FR han reconocido la importancia de esta com-pensación. La propuesta de Ley Europea de IA [8] exige un uso *proporcionado* y *estrictamente necesario* de *sistemas de identificación biométrica remota en tiempo real en espacios de acceso público con fines de garantía del cumplimiento del Derecho* y requiere que su despliegue esté sujeto a la autorización previa de una autoridad competente. El Foro Económico Mundial ha demandado *límites responsables al reconocimiento facial* [21] en investigaciones policiales, destacando su *uso necesario y proporcionado*.

La figura. 1 ilustra cuatro alternativas de intervención que podrían ser consideradas por las autoridades cuando se enfrentan a un equilibrio entre seguridad y privacidad. Ninguna intervención podría ser la decisión más adecuada en contextos con necesidades de seguridad muy limitadas o nulas. La intervención de agentes en el lugar, es decir, colocar agentes de policía para patrullar el lugar, podría ser una alternativa cuando las necesidades de seguridad son mayores y no es posible instalar cámaras. La vigilancia con CCTV puede ser una solución adecuada si hay cámaras disponibles en el lugar y la supervisión humana en tiempo real de la transmisión de vídeos se considera suficiente para garantizar el nivel de seguridad requerido. Finalmente, la intervención de reconocimiento facial haría uso adicional de un sistema FR para analizar automáticamente vídeos en busca de rostros en una lista de vigilancia y enviar alarmas de identificación a los cuerpos de seguridad. Esta es la solución que más invade la privacidad, aunque podría ser necesaria en caso de amenazas graves a la seguridad.

Hasta donde sabemos, no se han desarrollado pautas con-cretas sobre cómo abordar el concepto de uso proporcionado en implementaciones de FR. Las autoridades se beneficiarían de ellas para formalizar, visualizar y orientar su decisión sobre si el despliegue de un sistema FR es proporcionado o no en una situación determinada. Este artículo propone un tablero de control 2D para esta evaluación. En primer lugar, se identifican las principales variables cuantitativas y cualitativas relevantes para la decisión de despliegue de FR (por ejemplo, el número de personas en la escena, la escala de la amenaza, las consecuencias sobre los derechos y libertades individuales).

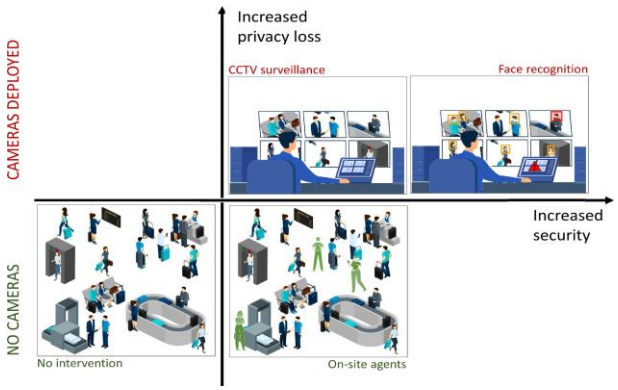


Fig. 1. Diferentes tipos de intervenciones que pueden considerarse en un escenario de aplicación de la ley. (Fuente: capturas tomadas de [9], [10]).

A continuación, se propone un modelo 2D que permite pon-derar estas variables en términos de coste ético (incluida la privacidad y los derechos fundamentales relacionados) frente a incremento en seguridad. El tablero de control está diseñado para ayudar a los tomadores de decisiones que se enfrentan a la elección de implementar un sistema FR o no. Por último, el modelo se aplica a diferentes escenarios de reconocimiento facial inspirados en implementaciones del mundo real, con fines de validación del marco propuesto.

Este trabajo es una versión extendida del paper presentado en el Congreso IEEE FG 2024 [25].

II. Contexto

A. *La perspectiva de la sociedad*

Las personas utilizan el reconocimiento facial en su vida cotidiana. Por ejemplo, FR se utiliza comúnmente para des-bloquear dispositivos como teléfonos inteligentes, acceder a cuentas bancarias electrónicas, pasar controles en aeropuertos o etiquetar a amigos en redes sociales. Sin embargo, cuando se trata de escenarios menos conocidos y que no se utilizan a diario, incluido el uso a gran escala de FR por parte de las autoridades encargadas de hacer cumplir la ley con fines de seguridad, que es el tema central de este documento, los estudios revelan reticencia y desconfianza más profundas ante su uso.

Seng et al. [33] analizaron la percepción de las personas sobre la FR en 35 escenarios diferentes, que van desde el desbloqueo de dispositivos hasta transacciones financieras, marketing personalizado, control de asistencia y vigilancia en eventos públicos. Mostraron 35 escenarios de FR a 314 participantes en forma de viñetas y formularon preguntas relacionadas con la utilidad, el nivel de comodidad y las preocupaciones sobre la privacidad. Sus resultados confirman que las percepciones de la RF dependen en gran medida del contexto especifico en el que se aplica. Los participantes se sienten más cómodos en escenarios en los que confían en las entidades que recopilan su información facial y donde esta

información se almacena en sus dispositivos personales, lo que les da una sensación de control sobre sus datos confidenciales. Otro hallazgo clave de este estudio, también planteado en [14], es que los usuarios que no encuentran un beneficio claro en el uso de FR en un escenario determinado tienden a considerar la tecnología como una invasión de la privacidad. De hecho, de los 35 escenarios, solo dos de ellos se relacionan con el uso a gran escala del reconocimiento facial en eventos públicos. Se diferencian en un aspecto: mientras que el objetivo del primero se deja abierto ("FR se utiliza para rastrear a las personas que asisten a un evento público"), el segundo especifica que el propósito es "garantizar la seguridad pública y la aplicación de la ley". Los participantes encontraron que el segundo escenario era más útil e informaron que se sentían más cómodos en comparación con el que no indicaba el propósito de la vigilancia del FR. Esto concuerda con la *teoría del contrato social* [24], que establece que la privacidad individual a menudo debe sacrificarse por un bien mayor, como la seguridad nacional.

Además del beneficio percibido en el uso de FR con fines de seguridad pública, estudios recientes han analizado la confianza de los ciudadanos en las fuerzas del orden como entidades responsables de los despliegues de FR. Una encuesta con 4109 adultos realizada por el Instituto Ada Lovelace [15] y otra con 2291 participantes por la Universidad de Monash [2] mostró que, aunque la gente tiene ciertos miedos y no hay apoyo incondicional a la policía, están abiertos al uso de la tecnología con fines de aplicación de la ley siempre que exista un beneficio público demostrable, así como regulaciones y salvaguardas de privacidad en la gestión de datos biométricos. Sin embargo, se ha descubierto que la percepción pública del uso de FR con fines policiales está estrechamente relacionada con el entorno cultural. Un estudio sobre las actitudes del público hacia la identificación de rostros en la justicia penal en los EE. UU., China, el Reino Unido y Australia [30] encontró que los encuestados estadounidenses aceptan más el seguimiento de los ciudadanos, aunque confían menos en la policía que la gente del Reino Unido y Australia. Esto ilustra la necesidad de tener en cuenta la perspectiva cultural en las decisiones relacionadas con el despliegue de FR por parte de los organismos públicos. También es importante entrelazar la cultura y la educación. Como se destaca en [14], aspectos relevantes como el desconocimiento de estos sistemas por parte de los ciudadanos (por ejemplo, sus principios de funcionamiento, limitaciones y aplicaciones) están estrechamente relacionados con la aceptación de esta tecnología.

B. La perspectiva de la seguridad

Las políticas globales recientes se refieren al uso *proporcionado* de tecnologías FR. Esta sección incluye dos ejemplos relevantes. La Ley Europea de IA [8], cuyo objetivo es el desarrollo, la implementación y el uso confiable y seguro de sistemas de IA. La Ley de IA adopta un enfoque basado en el riesgo, según el cual los sistemas de IA están sujetos a diferentes requisitos en función de su nivel de riesgo, que está vinculado a su contexto de uso y depende de la manera en que el sistema puede afectar a los derechos fundamentales.

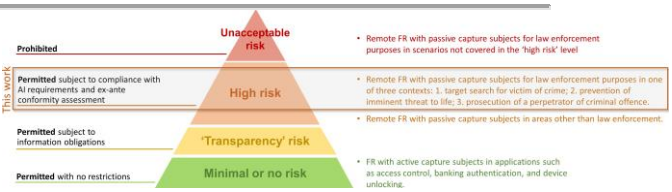


Fig. 2. Ilustración de los cuatro niveles de riesgo propuestos por la Ley de IA con las correspondientes aplicaciones de reconocimiento facial. Este documento se centra en el uso de alto riesgo de FR con fines policiales (resaltado en naranja).

La propuesta de la Comisión Europea define cuatro niveles de riesgo: (1) riesgo prohibido o inaceptable; (2) riesgo alto, en el que los sistemas de IA están sujetos a un conjunto de requisitos que incluyen, por ejemplo, la implementación de medidas de mitigación de riesgos, niveles adecuados de precisión, solidez, ciberseguridad, gobernanza de datos, documentación técnica y estrategias de supervisión humana; (3) riesgo de transparencia, que implica únicamente obligaciones de información; (4) riesgo mínimo, en el que los sistemas de IA están permitidos sin restricciones. Hupont et al. [14] analizan el panorama de las aplicaciones de procesamiento facial, vinculándolas con diferentes niveles de riesgo, como en la propuesta de la Ley de IA. En términos de FR (fig. 2), el estudio identifica como aplicaciones de bajo riesgo aquellas destinadas a verificar la identidad de una persona siempre que esta tenga un papel activo. Esto incluye aplicaciones de control de acceso, autenticación bancaria o desbloqueo de dispositivos. En el otro lado de la dimensión de riesgo, el estudio considera escenarios de FR en los que los sujetos tienen un rol pasivo (denominados escenarios remotos), que están vinculados a un riesgo alto e inaceptable según el contexto.

La propuesta presta especial atención a los sistemas de *IA para la identificación biométrica remota en tiempo real de personas físicas en espacios de acceso público con fines de garantía del cumplimiento del Derecho*, que incluyen los escenarios abordados en este documento. La reglamentación europea se analiza en la sección VI. Otra iniciativa relevante a nivel internacional es liderada por el Foro Económico Mundial (FEM) que recientemente desarrolló un marco de políticas compuesto por un conjunto de principios para el uso de FR en la aplicación de la ley [21]. La propuesta identifica el *uso necesario y proporcionado* como uno de los principios a seguir, que está relacionado con el equilibrio entre amenazas a la seguridad y derechos fundamentales. Afirma que *la decisión de utilizar tecnología de reconocimiento facial siempre debe estar guiada por el objetivo de lograr un equilibrio justo entre permitir a los organismos encargados de hacer cumplir la ley implementar las últimas tecnologías, que hayan demostrado ser precisas y seguras, para salvaguardar a los individuos y a la sociedad contra las amenazas a la seguridad y la necesidad de proteger los derechos humanos de las personas. Como principio general, se considera que el reconocimiento facial está vinculado a una causa y necesidad, ya que de lo contrario socavaría los derechos humanos y fundamentales.*

Este principio también se refiere a la necesidad de documentar y justificar la implementación del FR, especificando los delitos o investigaciones para los que su uso es aceptable y/o lícito, y limitando tanto la recopilación de imágenes de espacios públicos como el período de tiempo en que se lleva a cabo. En particular, se llama a considerar alternativas al uso del FR y a garantizar que su uso sea apropiado, limitado y exclusivamente relacionado con fines de investigación.

Aunque no son iniciativas políticas, en esta sección se incluyen los esfuerzos realizados por algunas empresas privadas, instituciones de investigación y organizaciones del sector público de todo el mundo para construir principios y directrices éticos para la IA. Aún no hay consenso sobre los elementos constitutivos reales de la ética de la IA, pero el análisis exhaustivo de 84 principios y directrices éticas de la IA realizado por Jobin et al. [16] encuentra que está surgiendo un acuerdo global en torno a los siguientes principios clave: transparencia, equidad, no maleficencia, responsabilidad, privacidad, beneficencia, libertad y autonomía, y confianza. Por lo tanto, estos principios se aplican a los sistemas de reconocimiento facial y, de hecho, están alineados tanto con las políticas FR específicas antes mencionadas como con las preocupaciones de los ciudadanos.

III. Ejemplos de Modelos de Intervención

Los tableros de control bidimensionales (2D) se han utilizado ampliamente como herramientas simples pero sólidas para la asignación de recursos y las decisiones de intervención política en diferentes campos, desde la meteorología [36], [39], economía [23] y medicina [1], [27]. En general, estos marcos comparan costes versus beneficios para evaluar la conveniencia de un proyecto, una decisión o cualquier otro tipo de intervención. Aunque las palabras *coste* y *beneficio* pueden parecer puramente económicas, cabe señalar que la compensación entre estos dos términos no tiene por qué ser necesariamente monetaria. Por ejemplo, el coste de implementar o no una intervención también puede ser ético (por ejemplo, perder un derecho fundamental, como el de la privacidad) o médico (por ejemplo, contraer una enfermedad). A continuación, se describen algunos marcos 2D de otros campos que han inspirado este artículo.

Wilks propone un marco de costes/pérdidas económicas para la predicción meteorológica, concebido para quienes toman decisiones [39]. Por un lado, este marco tiene en cuenta el coste C de implementar medidas (es decir, intervenir) para protegerse de los efectos de una posible condición climática severa y la probabilidad prevista p de que tal evento ocurra. Por otro lado, la ocurrencia de eventos climáticos adversos sin esta intervención resultaría en pérdidas por daños L. La intervención se considera económicamente viable cuando la relación coste/pérdida está por debajo de la probabilidad de ocurrencia del evento climático adverso, es decir, cuando $C/L < p$. Por lo tanto, este marco transforma un pronóstico meteorológico en una decisión de GO/NO-GO. También relacionado con el clima, Keith propone en [17] un modelo de intervención de desviación de vuelo en caso de amenazas climáticas severas. La intervención, basada en un pronóstico desfavorable, implica cargar combustible adicional para llegar a un aeropuerto alternativo. Si no se toman medidas de protección y se produce el evento, el vuelo deberá regresar al aeropuerto de salida, con el consiguiente gasto extra de combustible y retrasos.

El campo de la medicina utiliza desde hace tiempo el análisis coste-efectividad (ACE) para decidir si intervenir ante una amenaza para la salud. Se evalúan decisiones como la asignación de recursos adicionales de atención médica [32] o la vacunación de la población (por ejemplo, contra el coronavirus [19]). Black [5] propone un enfoque visual del ACE en Medicina mediante el uso de un plano 2D, en el que el eje x representa la efectividad (E) y el eje y representa el costo (C). Define una función lineal con pendiente $K > 0$, que representa la relación entre el coste y la efectividad, y divide el espacio en dos regiones. Una estrategia de intervención se considera rentable si proporciona más efectividad que costes. Geométricamente hablando, esto implica que el punto en el plano 2D que representa la intervención se encuentra en la parte inferior del espacio donde $E > \frac{C}{K}$. Se pueden evaluar dos estrategias de intervención alternativas, I_1 y I_2, en términos de su distancia a la línea con pendiente K, para decidir cuál es más rentable. Es importante resaltar que, en el caso de la medicina, el coste es económico, pero los beneficios son puramente sanitarios (por ejemplo, el coste por contagio de COVID-19 evitado).

Este artículo define *intervención* como la decisión de desplegar un sistema FR con fines de aplicación de la ley como acción protectora en caso de amenaza pública inminente. Si bien la mayoría de los artículos se centran en analizar y mejorar la precisión y el rendimiento de los modelos FR, la evaluación de las intervenciones del mundo real no ha sido desarrollada. Como se ha visto anteriormente, muchos factores pueden afectar a esta decisión. Al igual que una amenaza climática severa, los sospechosos de la lista de vigilancia FR pueden causar distintos niveles de pérdida, daños y perjuicios que afectan a la sociedad desde una perspectiva económica y de vida humana. Sin embargo, si bien el clima severo no se puede detener, un sospechoso en la lista de vigilancia sí se podría. Otro factor a considerar es el contexto específico en el que se llevaría a cabo la intervención (por ejemplo, en un espacio interior o abierto, más o menos concurrido). Además, la implementación de FR conlleva un coste ético en términos de derechos fundamentales relacionados con la privacidad [37]. Esto representa una compensación entre preocupaciones éticas y necesidades de seguridad, como se muestra en la Fig. 3.

IV. Tablero de Control

El paradigma de coste/pérdida se utiliza como base para proponer un tablero de control gráfico 2D que permita evaluar el uso proporcionado y adecuado de FR en contextos relevantes. Tiene en cuenta factores clave, como el tipo de escenario de vigilancia, el riesgo para la seguridad, y las preocupaciones sobre la privacidad de los ciudadanos, y pretende ayudar a las autoridades a tomar una decisión sobre una intervención.

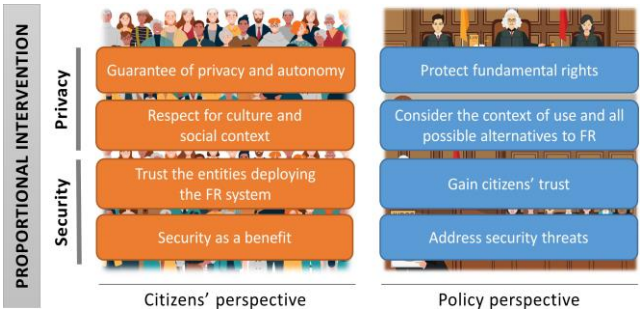


Fig. 3. Elementos clave que debe sopesar una decisión de intervención de reconocimiento facial, según las necesidades ciudadanas y políticas.

El marco de decisión consta de dos elementos: un plano 2D estático con las variables *pérdida de privacidad (privacy loss)* frente a *riesgo potencial en seguridad (security harm)* y una función dinámica s_i definida por los detalles de implementación.

A. Plano 2D proporcional

Nuestro tablero de control se basa en un plano cartesiano 2D que modela el uso proporcionado de una intervención FR. El eje *y* tiene en cuenta el coste ético de la implementación, relacionado con la privacidad y posibles violaciones de los derechos fundamentales, y se asocia con una pérdida de confianza de los ciudadanos en las autoridades. El eje *x* representa el riesgo potencial de daño de la amenaza a la seguridad, es decir, el daño potencialmente causado por no identificar y detener al individuo en la lista de vigilancia (por ejemplo, la amenaza de no capturar a un criminal o rescatar a una persona desaparecida). Cabe señalar que la dimensión económica no se considera de forma intencionada en nuestro marco, ya que el enfoque se centra exclusivamente en los aspectos éticos de las intervenciones de RF.

Dado que el coste ético está fuertemente impulsado por la invasión de la privacidad, la dimensión del eje y se ha denominado *pérdida de privacidad*. Su valor *p* se formaliza como dependiente principalmente de dos variables:

- *d* – la densidad de personas (por ejemplo, personas/hora) que circulan por el lugar de despliegue y, por lo tanto, están sujetas a FR. Cuanto mayor sea la densidad de personas bajo vigilancia de FR, mayor será la pérdida general de privacidad.
- *c* – el coste ético vinculado al lugar de implementación, que podría considerarse de manera diferente dependiendo de sus características (por ejemplo, espacio público abierto, espacio interior, infraestructura critica), la intensidad de la vigilancia (por ejemplo, número de cámaras existentes, área cubierta) y el contexto cultural (por ejemplo, beneficio percibido por la sociedad en el país de despliegue).

La dimensión del eje *x* se ha denominado daño potencial, lo que representa el valor del daño *h*, que podría mitigarse mediante una implementación de FR en el sitio *i*. Cubre tanto el daño potencial material como el daño humano con diferentes niveles, desde daño físico hasta vidas humanas, y depende de los valores de *d* y *l*, donde *l* representa el nivel de daño que potencialmente podría implicar o causar la(s) persona(s) buscada(s).

La tabla I proporciona algunos ejemplos de escenarios y cómo pueden vincularse a diferentes valores de p y h, respectivamente.

Cabe señalar que, aunque las dimensiones del marco se conciben como continuas, se proporcionan valores conceptuales (p_n para Privacy Loss y h_m para Security Harm) ya que su valor numérico concreto podría necesitar adaptarse al contexto particular de despliegue, incluidas, por ejemplo, consideraciones culturales.

Pérdida de privacidad		
Priv	Var	Descripción
p_1	d+ c+	FR desplegado en un espacio público abierto con una densidad de flujo de personas moderada (de decenas a cientos de personas por hora), es decir, calles, plazas, barrios, etc.
p_2	d++ c++	FR desplegado en un espacio interior con una densidad de flujo de personas moderada (pasan cientos de personas por hora) y con acceso restringido. Por ejemplo: aeropuertos o estadios a los que se puede entrar con entrada, como un partido de fútbol o un concierto musical.
p_3	d+++ c+++	El FR se despliega en una infraestructura crítica con una alta densidad de flujo de personas (circulación de cientos a miles de personas por hora). Este escenario podría ser, por ejemplo, un centro comercial, una estación de tren, autobús o metro.
Daño potencial		
Harm	Var	Description
h_1	l++	Cuestiones de seguridad que involucran vidas humanas, como asesinatos, secuestros o personas desaparecidas.
h_2	l+++	Cuestiones de seguridad relacionadas con ataques terroristas que ponen en riesgo muchas vidas humanas.

TABLE I
EJEMPLOS DE DIFERENTES NIVELES DE *Pérdida de Privacidad p* Y *Daño Potencial h*. EL SIGNO '+' INDICA EL NIVEL DE PREOCUPACIÓN DE LA VARIABLE.

En el caso del valor de *Pérdida de privacidad* p_n, el índice *n* aumenta con el nivel de invasión de la privacidad. Su valor más bajo, p_1, representa un escenario en el que un grupo de tamaño pequeño a mediano de personas es monitoreado por el sistema FR en espacios abiertos. En el segundo nivel de privacidad, p_2, se consideran escenarios que involucran un mayor flujo de personas, pero esta vez en espacios interiores, como estadios, aeropuertos o conciertos. En este tipo de lugares es habitual que las autoridades implementen medidas de seguridad en la entrada, como pedir el DNI o las entradas. Recientemente se han producido graves incidentes de seguridad en estos casos, lo que ha despertado la conciencia y el miedo en la población.

El nivel de pérdida de privacidad más alto considerado, p_3, está directamente asociado con la intervención de FR en las llamadas *infraestructuras críticas*, que incluyen estaciones

de autobús, metro o tren con una circulación de personas muy elevada [11]. En estos escenarios también se han producido recientemente graves incidentes de seguridad. En estos contextos, cientos o incluso millones de personas podrían estar caminando frente al sistema FR todos los días, sin darse cuenta de que sus rostros se comparan con los de una lista de vigilancia. En cuanto a la *Pérdida de Privacidad*, se definen dos niveles para el *Daño Potencial* h_m, donde el índice m aumenta con la gravedad del daño que una persona de la lista de vigilancia podría perpetrar. La tabla I describe los dos niveles propuestos de *daño potencial* h_1 y h_2, que están vinculados a vidas humanas y distinguen entre asesinatos/secuestros/personas desaparecidas y ataques terroristas, respectivamente. Tenga en cuenta que, en el caso de los secuestros, las personas que se buscan pueden ser los secuestradores o la persona secuestrada (o ambos). La razón de estos niveles de daño es que la búsqueda de sospechosos de secuestro, asesinatos y ataques terroristas puede ser suficiente para justificar una intervención de FR.

La prevención de cualquiera de estos eventos, especialmente cuando existe una alta probabilidad de que aparezca la(s) persona(s) buscada(s), puede considerarse una justificación para el despliegue como acción protectora. Tener en cuenta que los problemas de seguridad que implican daños materiales, como robos o daños a la propiedad, se consideran en este estudio como un uso no proporcional de FR.

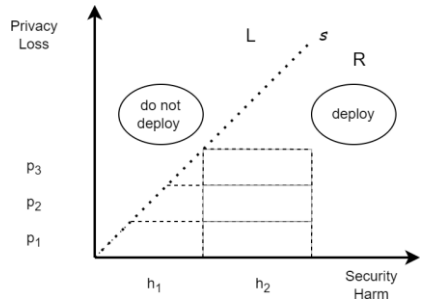


Fig. 4. Se propone un plano 2D proporcional para la evaluación de la intervención FR y la función dinámica s que divide el plano en áreas de implementación y no implementación.

De forma similar a la visualización 2D de costo/efectividad propuesta en [5] para la evaluación de intervenciones médicas, la Fig. 4 muestra nuestro plano 2D dividido en dos regiones por la función de identidad s. En la región R, el valor de pérdida de privacidad, p, está por debajo del de daño potencial h, y, por lo tanto, el uso y la implementación de FR pueden considerarse proporcionales. En la región L, la pérdida de privacidad está por encima del daño potencial y, en principio, la implementación de FR no es proporcionada.

La figura 4 también divide el espacio 2D discretizado en regiones o bloques rectangulares según los valores definidos de perdida de privacidad (p_n) y daño potencial (h_m) en la Tabla I. La relación entre la altura y la anchura (H/W) de los bloques impulsa el análisis gráfico de la compensación entre la pérdida de privacidad y el daño a la seguridad, propuesta en este documento, que se ilustra con más detalle en las siguientes secciones. Las autoridades que se enfrentan a esta infinidad de escenarios y tienen la responsabilidad de autorizar una intervención de FR se beneficiarían de un marco de decisión que les ayude a sopesar todas estas variables para garantizar la seguridad ciudadana. El plano 2D proporcional tiene en cuenta todas esas variables complejas y ofrece una representación gráfica e intuitiva en 2D para tomar la decisión de intervenir.

B. *The dynamic implementation function*

La Fig. 4 muestra la función de línea de identidad s que divide el plano 2D en regiones de *despliegue* vs *no – despliegue*. En la práctica, el tablero de control propuesto utiliza una nueva función de implementación dinámica, s_i, que depende de las siguientes variables:

- w – probabilidad de que los individuos de la lista de vigilancia puedan aparecer en el escenario i. Esta información podría ser proporcionada, por ejemplo, por autoridades o agencias de inteligencia basándose en investigaciones previas.
- r – fiabilidad del sistema FR, por ejemplo, en términos de falsos positivos/negativos, tasa de identificación de falsos positivos (FPIR) y problemas de sesgo demográfico. Por ejemplo, un falso positivo podría suponer la detención de una persona equivocada y la consiguiente desconfianza en las autoridades.
- t – período de tiempo en el que se implementa el sistema (por ejemplo, 24 horas, 7 días) durante un período de tiempo limitado durante un evento).

Por lo tanto, la función dinámica relaciona el conocimiento *a priori* sobre el o los individuos de la lista de vigilancia en la variable w, la especificación sobre el despliegue en la variable t y los detalles del sistema FR en la variable r. Esta función se define mediante la siguiente ecuación:

$$s_i(h) = w \cdot h^r - t \qquad (1)$$

w es una variable de probabilidad definida en el rango de (0, 1), y consta de los siguientes eventos: 0.0 (no ocurre), 0.1 (muy poco probable), 0.3 (es poco probable), 0.5 (puede ocurrir), 0.75 (probable) y 1.0 (muy probable). La variable r también se define en el rango (0, 1) y puede asociarse con la puntuación F1 del sistema FR. Finalmente, la variable t toma los valores discretos [0, 0,25, 0,5], que representan un despliegue de FR durante un período de menos de una semana, un par de semanas y más de un mes, respectivamente.

La figura 5 muestra diferentes funciones dinámicas con diferentes valores de variables. Las funciones dinámicas s1 y s_2 tienen los siguientes valores: $r = 1$, $t = 0$ y $w = 0,75$ y $w = 0,5$, respectivamente. La función s_3 tiene estos valores: $r = 1$, $w = 0,5$ y $t = 0,25$, la misma pendiente que s_2 con un desplazamiento hacia la derecha. La preocupación por la pérdida de privacidad aumenta debido al despliegue más prolongado del sistema FR. Finalmente, s_4 se define por r = 0, 75, w = 0, 5 y t = 0.

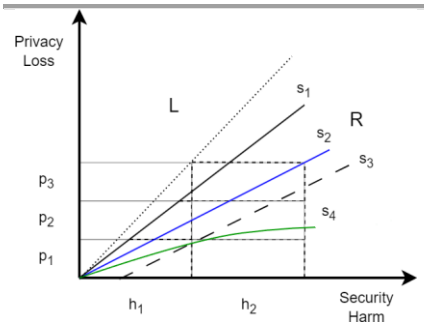


Fig. 5. Ejemplos de funciones dinámicas para diferentes variables.

Por simplicidad, en los siguientes ejemplos proporcionados en este artículo, se utilizarán las variables $r = 1$ y $t = 0$, para trabajar con rectas sin desplazamiento.

C. Desplegar o No Desplegar

Tanto el plano 2D proporcional (sección IV-A) como la función dinámica (sección IV-B) determinan el marco para abordar la decisión de intervención en un caso de aplicación de la ley concreto. Por lo tanto, la ubicación de la intervención y los individuos de la lista de vigilancia indican las coordenadas (h_m, p_n) del bloque correspondiente en la cuadrícula del plano 2D, como se muestra en la figura Fig. 4. Las variables específicas de este caso y el sistema FR dan forma a la función dinámica, que dividirá el plano en una región de despliegue y una región de no despliegue. Sin embargo, en lugar de centrarse en la totalidad del plano R, el análisis se realiza a nivel de bloque.

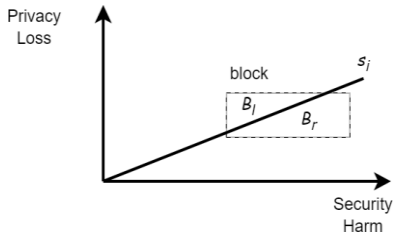


Fig. 6. Análisis de bloques basado en las superficies B_l y B_r en la posición (h_m, p_n).

La Fig. 6 muestra el procedimiento gráfico de toma de decisiones. La función dinámica s_i divide el bloque B en dos áreas, B_l y B_r. Entonces, la regla marco 2D define que la intervención FR en el sitio i es proporcional si y solo si $B_r > B_l$.

Ahora, podemos volver a la Fig. 5 para evaluar la decisión proporcional en función de las diferentes funciones de implementación dinámica. Tomemos el bloque (p_3, h_2). La implementación de FR con la función s_1 determina una decisión de intervención, es decir, $B_r > B_l$, mientras que la función s_2 no. Como sabemos, la diferencia entre ambas funciones es la probabilidad de aparición w. Un valor bajo de w en este alto nivel de pérdida de privacidad descarta la decisión de implementación.

Tomando ahora el bloque (p_1, h_1), la función de implementación dinámica s_2 determina una decisión de intervención, pero las funciones s_3 y s_4 no. Esta vez, la diferencia para s_3 es un tiempo de implementación más largo y, para s_4, un rendimiento de puntuación F1 más bajo del algoritmo FR.

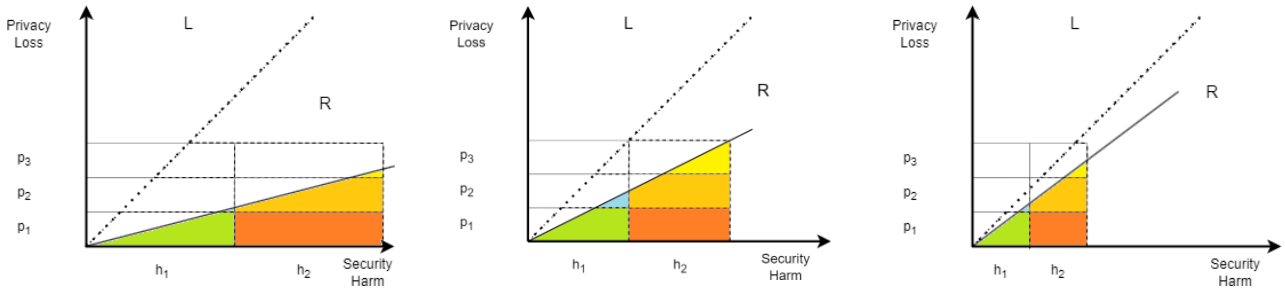
D. Contexto Cultural

Como se mencionó anteriormente, la percepción pública de las aplicaciones de procesamiento facial en una amplia gama de escenarios relacionados con el bien social está fuertemente condicionada por los antecedentes culturales [14], [30].

La Fig. 7 ilustra cómo se usaría el plano 2D para impulsar una decisión de intervención FR en diferentes contextos culturales. En la figura, la decisión de intervención o no intervención se basa en el análisis de las áreas B_l y B_r, y muestra la relevancia de la relación alto/ancho (H/W) del bloque. Gráficamente, el despliegue de FR se permitiría cuando el área rellena con color en un bloque sea mayor que el área sin color, es decir, cuando $B_r > B_l$. La Fig. 7 muestra ejemplos de diferentes relaciones H/W que representan diferentes perspectivas de la sociedad sobre los sistemas FR y la pérdida de privacidad. En los tres ejemplos, los bloques (p_1, h_1), (p_1, h_2) y (p_2, h_2) cumplen la condición $B_r > B_l$, mientras que los bloques (p_2 ,h_1) y (p_3, h_2) no la siguen. Se eligen valores de w que conducen a un comportamiento de intervención similar, mientras que la relación H/W cambia, con $r = 1$ (lo que significa un rendimiento perfecto de FR) y $t = 0$ (lo que implica que el sistema FR se implementará durante un corto tiempo).

El primer ejemplo (fig. 7-izquierda), con $H/W = \frac{3}{13}$, que representa un contexto con altas preocupaciones de seguridad, valida una intervención en el bloque (h_2, p_2) incluso con una baja probabilidad de aparición del sujeto $w = 0.25$, como lo muestra la función dinámica correspondiente (s_i). Este contexto refleja una sociedad tolerante con los sistemas FR y una preocupación moderada por la pérdida de privacidad. El segundo contexto moderado (fig. 7-centro) tiene una relación de $H/W = \frac{3}{9}$. La intervención de FR en el bloque (h_2, p_2) se consideraría proporcional cuando la probabilidad de aparición sea $w = 0,5$, que representa un valor razonable para implementar un sistema FR. El último ejemplo (fig. 7—izquierda), donde $H/W = \frac{3}{5}$, representa un contexto de política más conservador en términos de pérdida de privacidad. En este caso, la implementación de FR en el bloque (h_2, p_2) solo valdría la pena con una probabilidad muy alta de aparición de un individuo en la lista de vigilancia. Esto significaría una función dinámica s_i con $w = 0,75$.

Estos ejemplos demuestran cómo las diferencias culturales pueden influir en la decisión de intervenir o no con FR, así como la importancia de que los responsables de las políticas aborden adecuadamente la compensación entre la pérdida de privacidad y el daño potencial. Algunos países y sus ciudadanos podrían estar más dispuestos que otros a sacrificar parte de su privacidad a cambio de mayor seguridad.



$s_i@w = 0.25$ en contexto tolerante $s_i@w = 0.50$ en contexto moderado $s_i@w = 0.75$ en contexto conservador

Fig. 7. ilustración gráfica de cómo se utilizaría el plano 2D propuesto para evaluar una intervención FR en sitios i con diferentes funciones dinámicas s_i asociadas y relación H/W.

V. Ejemplos prácticos

En la siguiente sección, se aplica el tablero de control 2D para evaluar diferentes tipos de intervenciones de FR inspiradas en tres escenarios de aplicación de la ley del mundo real.

1) Metropolitan Police Service Live Facial Recognition Trials: En 2020, el Servicio de Policía Metropolitana de Londres presento´ un informe sobre el despliegue del reconocimiento facial entre agosto de 2016 y febrero de 2019 [22]. El informe detalla diez despliegues en espacios públicos y un conjunto de métricas de interés para una evaluación completa, que incluyen: duración, promedio de oportunidades de reconocimiento, tamaño de la lista de vigilancia, número de falsas alarmas, número de personas involucradas por un oficial de policía y número de acciones/arrestos. Nos centraremos en dos de estos ensayos, que utilizaron la misma versión de software del algoritmo FR y equipo similar (cámara de vigilancia). En primer lugar, la prueba *Stratford Westfield, 28 de junio de 2018* se refiere a un despliegue urbano durante 6 horas. La lista de vigilancia tenía 486 personas *buscadas* elegidas por área geográfica (proximidad a Westfield Stratford). El despliegue produjo 5 alertas sobre 10.000 personas detectadas y evaluadas. Vale la pena mencionar aquí que las alertas FR (una coincidencia por encima de un umbral) siguen un proceso de adjudicación por parte del operador. Un operador es un agente cualificado que ha recibido una formación avanzada sobre el sistema de reconocimiento facial y sus funciones. Por lo tanto, solo una de estas alertas resultó en la intervención de un agente, pero no se llevó a cabo ninguna acción/arresto. En segundo lugar, el despliegue callejero de prueba *Romford, febrero de 2019* consistió en una vigilancia de 6:45 horas, en la que se detectaron 10 100 peatones, con una lista de vigilancia de 1996 personas, incluidas personas buscadas por delitos violentos y filtradas por área geográfica. El despliegue arrojó 13 resultados positivos, que en 3 ocasiones dieron lugar a una detención.

En nuestro marco, este escenario de *pérdida de privacidad* puede considerarse como p_1, dado que se implementa en un espacio público abierto con una densidad de flujo de personas moderada, como se define en la Tabla I. Las variables que definen la función de implementación dinámica s_{met} son: $t = 0$ (tiempo limitado), $r = 0,85$ (obtenidas de estadísticas detalladas de rendimiento en el informe, como falsas alarmas e identificaciones positivas en cada ensayo) y probabilidad $w = 0,3$ (es poco probable que ocurra), que es un valor moderado, ya que la lista de vigilancia se filtra por área geográfica (individuos que viven en el vecindario vigilado). Falta información sobre el nivel de daño asociado a las personas de la lista de vigilancia. Esto permitiría a las autoridades determinar el nivel de daño a la seguridad y, por tanto, su proporcionalidad, según nuestro modelo. En la figura 8 se representa este escenario, con los bloques (p_1, h_1) y (p_1, h_2) coloreados bajo la función dinámica $s_{met}(h)$. En este valor de w, ambas áreas bajo $s_met(h)$ indican una recomendación de intervención, pero solo si el daño a la seguridad causado por las personas en la lista de vigilancia corresponde a h_1 y niveles h_2.

2) Arrest of Terrorist Suspect in London: Un miembro del ejército británico de 21 años, convertido en presunto terrorista y espía en enero de 2023, fue enviado a la prisión de HMP Wandsworth. Se escapó de la prisión la mañana del miércoles 6 de septiembre y fue recapturado el sábado 9 de septiembre. La búsqueda, que duró cuatro días, se coordinó en el Centro de Operaciones contra el Terrorismo (CTOC) de West Brompton, en el centro de Londres [35]. La sala de situación del centro tenía acceso a tecnología de espionaje *de vanguardia*, incluido el reconocimiento facial, una red de cámaras CCTV y datos de seguimiento telefónico. Este caso representa un escenario real con un individuo en la lista de vigilancia del sistema FR. La información técnica sobre la implementación del sistema FR no está disponible. Sin embargo, este tipo de búsqueda implica el uso de FR en escenarios con diferentes pérdidas de privacidad: p_1, p_2 y p_3.

Si bien el nivel de daño no se puede definir exactamente, los cargos contra el individuo involucran la seguridad nacional y, por tanto, se le puede asignar h_2. También se pueden estimar otras variables del marco 2D para dibujar la función de implementación dinámica s_{run}. El parámetro de tiempo fue inferior a una semana, es decir, $t = 0$. La variable r se puede considerar igual a $r = 0.9$. Finalmente, si se considera que el despliegue de FR se realiza en lugares donde el público informó haber visto al sospechoso, la probabilidad de aparición es $w = 0,75$ (probable que ocurra). Además, los escenarios que involucran p_3 normalmente corresponden a

aquellos lugares donde un fugitivo puede aparecer y escapar en el metro, los trenes o las llanuras. En este caso, la implementación se podría considerar dentro del área de uso proporcionado, si está asociada a un alto potencial de daño, que debe tenerse en cuenta con respecto a un umbral máximo de privacidad. La Fig. 8 muestra los bloques (p_1, h_2), (p_2, h_2) y (p_3, h_2) coloreados bajo la función dinámica que valida la recomendación de *Intervención*.

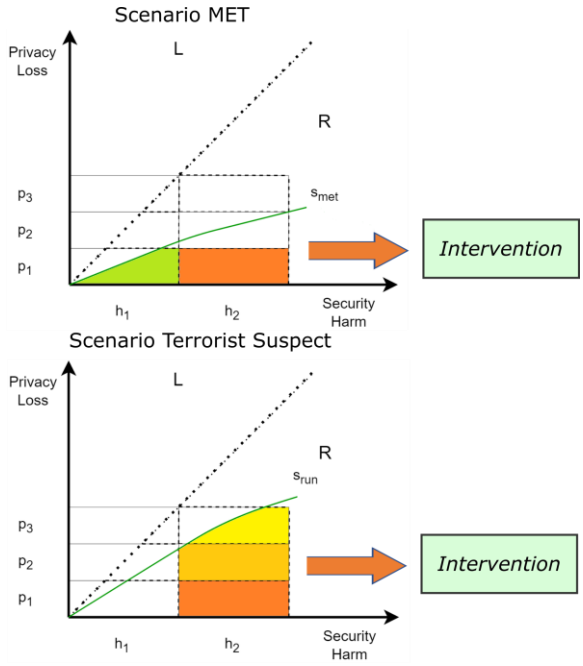


Fig. 8. Tablero en la práctica.

3) Brøndby IF's STADIUM: Brøndby IF es un club de fútbol profesional de la Superliga danesa [29]. En el verano de 2019, Panasonic instaló *FacePRO*, un sistema de reconocimiento facial en el estadio de Brøndby IF. Las personas que hayan sido sorprendidas infringiendo las normas del estadio tienen prohibido regresar a los partidos y están registradas en una lista de vigilancia. El Brøndby IF tiene una asistencia media a los partidos en casa de unas 14.000 personas y, en promedio, hay unas 100 personas registradas en la lista de seguimiento. Para el marco gráfico 2D, este escenario correspondería a un nivel de privacidad p_2, dado que se implementa en un espacio interior, como se especifica en la Tabla I. La variable tiempo es $t = 0$, porque el despliegue corresponde a un período corto (el tiempo del partido). La probabilidad de aparición tiene un valor relativamente alto, es decir, $\omega = 0,5$, porque es probable que los aficionados estén presentes en el partido. La tecnología en el modelo FR se basa en [40] y el punto de evaluación del informe de evaluación oficial del Instituto Nacional de Estándares y Tecnología (NIST) indica $r = 0,95$. Sin embargo, cuando el nivel de daño potencial causado por los aficionados de la lista de vigilancia no se puede determinar mediante la Tabla 2.1, ya que los sujetos están prohibidos por comportamiento violento y no por delitos graves. Nuestro marco gráfico 2D no coloca el escenario en el plano *Intervención-No Intervención*, lo que significa que no se recomienda la implementación de FR. Por tanto, se pueden vislumbrar otros tipos de intervenciones en la Fig. 1.

VI. CUMPLIMIENTO DE REGULACIONES INTERNACIONALES

La Ley de Inteligencia Artificial (IA) de la Unión Europea se publicó en el Diario Oficial el 12 de julio de 2024 [8] Esta ley representa la primera regulación horizontal vinculante a nivel mundial sobre IA y establece un marco unificado para la utilización y provisión de sistemas de IA dentro de la Unión Europea (UE). Proporciona un sistema de clasificación para los sistemas de IA, con requisitos y obligaciones diferenciados fundado en un enfoque basado en riesgos potenciales. Consecuentemente, aquellos sistemas de IA que presenten un nivel de riesgo inaceptable reciben un prohibición tácita en su uso. Por otro lado, un amplio abanico de categorías de sistemas de IA de *alto riesgo*, que podrían potencialmente ser la causa de daños significativos a las personas en términos de salud, seguridad o derechos fundamentales, serían permitido su uso pero solo sujeto a un conjunto de requisitos y obligaciones. Aquellos sistemas de IA que solo presenten un *riesgo mínimo* para las personas no estarán sujetos a obligaciones adicionales. Finalmente, aquellos sistemas de IA que presenten riesgos limitados, pero sean cerrados, estarán sujetos a requisitos de información y transparencia.

Esta sección analiza el marco de implementación propuesto, que aborda la mayoría de las preocupaciones suscitadas por la Ley de IA.

A. Contexto de la Ley de IA

La Ley de IA establece una postura definitiva sobre el despliegue de sistemas de IA en la vigilancia urbana y enfatiza que su utilización para la identificación biométrica remota en tiempo real de personas en lugares de acceso público con fines de aplicación de la ley es particularmente invasiva para los derechos y libertades de las personas interesadas. Esto puede tener un impacto significativo en la vida privada de una proporción considerable de la población, generando una sensación de vigilancia constante e indirectamente disuadiendo el ejercicio de los derechos fundamentales, incluida la libertad de reunión.

Por tanto, debe prohibirse el uso de dichos sistemas con fines policiales. Sin embargo, existen importantes excepciones y pautas para escenarios especiales:

- Despliegue proporcionado: existen situaciones enumeradas exhaustivamente y definidas de forma estricta, en las que el uso es estrictamente necesario para lograr un interés público sustancial, cuya importancia supera los riesgos.
- Alcance limitado: el sistema biométrico debe emplearse únicamente con el fin de confirmar la identidad del individuo cuya identidad se busca específicamente. El despliegue de dichos sistemas debe

limitarse a lo estrictamente necesario en cuanto al período de tiempo, así como al ámbito geográfico y personal.

- Autorización: el despliegue de un sistema de identificación biométrica remota debe estar supeditado a la emisión previa de una autorización expresa y específica por parte de una autoridad judicial o de una autoridad administrativa independiente de un Estado miembro cuya decisión sea vinculante. En principio, dicha autorización debe obtenerse antes de utilizar un sistema de inteligencia artificial para identificar a una persona o personas.
- Evaluación de riesgos: La utilización del sistema en cuestión debe autorizarse exclusivamente en los casos en que la autoridad policial pertinente haya realizado una evaluación de impacto sobre los derechos fundamentales y haya registrado el sistema en la base de datos, de acuerdo con lo establecido en el reglamento de la Ley de IA.

B. Aplicaciones de IA permitidas

El Capítulo II desarrolla las prácticas prohibidas de IA en el artículo 5 para varias aplicaciones de dichos sistemas.

En lo que respecta a la implementación de sistemas de identificación biométrica remota en tiempo real, se observarán las siguientes excepciones a su uso en el punto *h*, siempre que dicho uso se considere estrictamente necesario para el cumplimiento de uno o más de los siguientes objetivos:

i la búsqueda selectiva de víctimas específicas de secuestro, trata de seres humanos o explotación sexual de seres humanos, así como la búsqueda de personas desaparecidas;

ii la prevención de una amenaza específica, sustancial e inminente a la vida o la seguridad física de personas físicas o una amenaza genuina, presente o genuina y previsible de un ataque terrorista;

iii la localización o identificación de una persona sospechosa de haber cometido un delito penal, con el fin de llevar a cabo una investigación o enjuiciamiento penal o ejecutar una sanción penal por los delitos mencionados en el anexo II y punibles en el Estado miembro de que se trate, que conlleven una pena privativa de libertad o una orden de prisión preventiva por un período máximo de al menos cuatro años.

El punto 2 de este artículo establece que la utilización de dichos sistemas tendrá en cuenta los siguientes elementos:

a la naturaleza de la situación que da lugar al posible uso, en particular la gravedad, probabilidad y magnitud del daño que se causaría si el sistema no se utilizara;

b las consecuencias del uso del sistema para los derechos y libertades de todas las personas interesadas, en particular la gravedad, probabilidad y escala de esas consecuencias.

C. Ley IA dentro del tablero de control

Las secciones anteriores han proporcionado una descripción general de los principios que rigen el uso de sistemas de identificación biométrica en tiempo real. Sostenemos que nuestro tablero de control abarca la mayoría de los conceptos principales relacionados con el proceso de toma de decisiones en torno al despliegue de dichos sistemas.

- Alcance: se consideran los conceptos de tiempo y situaciones en eq.refeq:si, teniendo en cuenta el período de tiempo del despliegue y la probabilidad de que el sujeto pueda estar presente en ese lugar.
- Escala: se evalúa el nivel de daño y los costes éticos del plano bidimensional y del espacio discretizado.

Este tablero de control satisface la necesidad de las autoridades de evaluar el impacto del uso del sistema biométrico. Además, sintetiza una evaluación más detallada de la situación específica realizada por las fuerzas de seguridad, que podría servir de base para una decisión de la autoridad judicial sobre la autorización o prohibición del despliegue del sistema FR.

VII. Conclusiones y trabajo futuro

Se propuso un marco gráfico 2D para evaluar el uso proporcional de sistemas FR en escenarios del mundo real, basado en un modelo de coste ético frente al beneficio de la seguridad. Las dos dimensiones consideran variables de estudios y políticas recientes sobre reconocimiento facial y preocupaciones relacionadas con la privacidad de los ciudadanos. Hasta donde sabemos, este es el primer marco que aborda el problema de la intervención en FR, lo que podría tener un alto impacto en los tomadores de decisiones y conducir a nuevas investigaciones que consideren el principio de proporcionalidad en FR. Se espera que también contribuya a un debate abierto, en línea con regulaciones mundiales como la Ley Europea de IA [AIact] sobre el uso proporcional y estrictamente necesario de la tecnología FR.

Nuestro marco, sin embargo, tiene algunas limitaciones. En su implementación práctica se ha utilizado un enfoque lineal simple con una amplia discretización del plano 2D en grandes bloques de intervención. Este modelo se puede mejorar incorporando en su diseño a las partes interesadas directamente involucradas en el despliegue de FR (por ejemplo, ciudadanos, tomadores de decisiones, etc.). Para abordar esto, en el futuro se puede incluir el desarrollo de simulaciones de diferentes escenarios de FR y la realización de una encuesta de usuarios a gran escala para comprender cuáles de ellos se consideran información proporcional y relacionada con la cultura. Esto nos permitirá generar un modelo matemático más detallado aprovechando la naturaleza continua de las variables, como la relación H/W. De hecho, el marco necesita identificar las diferentes preferencias culturales y éticas de los países o regiones del mundo. En el futuro, también se debería comprobar la usabilidad y la utilidad del marco con los responsables de la formulación de políticas y las autoridades, y aplicar ese tipo de marco a otras situaciones de toma de decisiones.

References

[1] J. P. Anderson, J. Bush, M. Chen, and D. Dolenc. Policy space areas and properties of benefit-cost/utility analysis. *Jama*, 255(6):794–795, 1986.

[2] M. Andrejevic, R. Fordyce, L. Li, and V. Trott. *Australian attitudes to facial recognition: a national survey*. Clayton Victoria Australia: Monash University, 2020.
[3] S. Balakrishnan, S. Chaudhuri, and V. Narasayya. Autotag'n search my photos: leveraging the social graph for photo tagging. In *Proceedings of the 24th International Conference on World Wide Web*, pages 163–166, 2015.
[4] G. Barquero, C. Fernández, and I. Hupont. Long-term face tracking for crowded video-surveillance scenarios. In *2020 IEEE International Joint Conference on Biometrics (IJCB)*, pages 1–8. IEEE, 2020.
[5] W. C. Black. The CE plane: a graphic representation of cost-effectiveness. *Medical decision making*, 10(3):212–214, 1990.
[6] F. Boutros, N. Damer, F. Kirchbuchner, and A. Kuijper. Elasticface: Elastic margin loss for deep face recognition. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 1578–1587, 2022.
[7] L. R. Carlos-Roca, I. Hupont, and C. Fernández. Facial recognition application for border control. In *2018 International Joint Conference on Neural Networks (IJCNN)*, pages 1–7, 2018.
[8] European Commission. Regulation (EU) 2024/1689 of the European Parliament and The Council. Available: http://data.europa.eu/eli/reg/2024/1689/oj, 2024. [Online; accessed September 27, 2024].
[9] Freepic. Monitoring screens. https://bit.ly/3LsxdSd. [Online; accessed September 27, 2024].
[10] Frepic. Airport passengers. https://bit.ly/3EHDsOn. [Online; accessed September 27, 2024].
[11] D. Gritzalis, M. Theocharidou, and G. Stergiopoulos. Critical infrastructure security and resilience. *Springer International Publishing*, 10:978–3, 2019.
[12] P. Grother, M. Ngan, and K. Hanaoka. *Face recognition vendor test(FRVT): Part 3, demographic effects*. National Institute of Standards and Technology (NIST), 2019.
[13] I. Hupont and C. Fernández. Demogpairs: Quantifying the impact of demographic imbalance in deep face recognition. In *2019 14th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2019)*, pages 1–7. IEEE, 2019.
[14] I. Hupont, S. Tolan, H. Gunes, and E. Gómez. The landscape of facial processing applications in the context of the european ai act and the development of trustworthy systems. *Scientific Reports*, 12(1):10688, 2022.
[15] A. L. Institute. Beyond face value: Public attitudes to facial recognition technology. https://bit.ly/44ZLRr4, 2020-07-24 2019. [Online; accessed September 27, 2024].
[16] A. Jobin, M. Ienca, and E. Vayena. The global landscape of ai ethics guidelines. *Nature Machine Intelligence*, 1(9):389–399, 2019.
[17] R. Keith. Optimization of value of aerodrome forecasts. *Weather and Forecasting*, 18(5):808–824, 2003.
[18] H. Lee, S.-H. Park, J.-H. Yoo, S.-H. Jung, and J.-H. Huh. Face recognition at a distance for a stand-alone access control system. *Sensors*, 20(3):785, 2020.
[19] R. Li, H. Liu, C. K. Fairley, Z. Zou, L. Xie, X. Li, M. Shen, Y. Li, and L. Zhang. Cost-effectiveness analysis of bnt162b2 covid-19 booster vaccination in the united states. *International Journal of Infectious Diseases*, 119:87–94, 2022.
[20] F. Liu, M. Kim, A. Jain, and X. Liu. Controllable and guided face synthesis for unconstrained face recognition. In *European Conference on Computer Vision*, pages 701–719. Springer, 2022.
[21] S. Louradour and L. Madzou. A policy framework for responsible limits on facial recognition, use case: Law enforcement investigations. In *World Economic Forum*, 2021.
[22] Metropolitan Police Service. Metropolitan Police Service Live Facial Recognition Trials. Available: https://bit.ly/3vjXe0N, 2020. online.
[23] E. J. Mishan and E. Quah. *Cost-benefit analysis*. Routledge, 2020.
[24] A. D. Moore. *Privacy, Security and accountability: ethics, law and policy*. Rowman & Littlefield, 2015.
[25] P. Negri, I. Hupont and E. Gomez. A Framework for Assessing Proportionate Intervention with Face Recognition Systems in Real-Life Scenarios *IEEE 18th International Conference on Automatic Face and Gesture Recognition (FG)*, Istanbul, Turkiye, pp. 01–09, 2024.
[26] P. Negri, S. Cumani, and A. Bottino. Tackling age-invariant face recognition with non-linear plda and pairwise svm. *IEEE Access*, 9:40649–40664, 2021.
[27] P. J. Neumann, G. D. Sanders, L. B. Russell, J. E. Siegel, and T. G. Ganiats. *Cost-effectiveness in health and medicine*. Oxford University Press, 2016.
[28] A. Oksanen, M. Kaakinen, J. Minkkinen, P. Räsänen, B. Enjolras, and K. Steen-Johnsen. Perceived societal fear and cyberhate after the november 2015 paris terrorist attacks. *Terrorism and Political Violence*, 32(5):1047–1066, 2020.
[29] Panasonic. Peace of mind on match day: facial recognition solution at the football stadium. Available: https://bit.ly/47lWnKr, 2019. online.
[30] K. L. Ritchie, C. Cartledge, B. Growns, A. Yan, Y. Wang, K. Guo, R. S. Kramer, G. Edmond, K. A. Martire, M. San Roque, et al. Public attitudes towards the use of automatic facial recognition technology in criminal justice systems around the world. *PloS one*, 16(10):e0258241, 2021.
[31] J. P. Robinson, G. Livitz, Y. Henon, C. Qin, Y. Fu, and S. Timoner. Face recognition: too bias, or not too bias? In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, pages 0–1, 2020.
[32] L. B. Russell, M. R. Gold, J. E. Siegel, N. Daniels, and M. C. Weinstein. The role of cost-effectiveness analysis in health and medicine. *Jama*, 276(14):1172–1177, 1996.
[33] S. Seng, M. N. Al-Ameen, and M. Wright. A first look into users' perceptions of facial recognition in the physical world. *Computers & Security*, 105:102227, 2021.
[34] T. Sutabri, A. K. Pamungkur, and R. E. Saragih. Automatic attendance system for university student using face recognition based on deep learning. *International Journal of Machine Learning and Computing*, 9(5):668–674, 2019.
[35] The Guardian. Surveillance centre hailed as critical in capture of escaped terror suspect. Available: https://bit.ly/3TNZuaR, 2023. online.
[36] J. C. Thompson. On the operational deficiences in categorical weather forecasts. *Bulletin of the American Meteorological Society*, 33(6):223 – 226, 1952.
[37] United Nations High Commissioner for Human Rights. The right to privacy in the digital age. Available: https://bit.ly/48bNzbP, 2021. online.
[38] Z. Wang, Z. Cheng, H. Huang, X. Zhou, and Y. Liu. Design and implementation of vehicle unlocking system based on face recognition. In *34rd youth academic annual conference of chinese association of automation (YAC)*, pages 121–126. IEEE, 2019.
[39] D. Wilks. A skill score based on economic value for probability forecasts. *Meteorological Applications*, 8(2):209–219, 2001.
[40] L. Xiong, J. Karlekar, J. Zhao, Y. Cheng, Y. Xu, J. Feng, S. Pranata, and S. Shen. A Good Practice Towards Top Performance of Face Recognition: Transferred Deep Feature Fusion, 2018.

Residuos de Disparo: Machine Learning aplicado a pericias históricas

Martín A. Onetto
Sección Física Forense,
Centro Atómico Bariloche, CNEA)
San Carlos de Bariloche, Argentina
martinonetto93@gmail.com

Rodolfo G. Pregliasco
Sección Física Forense
Centro Atómico Bariloche, CNEA
San Carlos de Bariloche, Argentina
w.pregliasco@gmail.com

***Resumen*—La búsqueda de residuos de disparo mediante micrioscopía electrónica de barrido SEM/EDX ha sido un estándar de trabajo en el área forense desde hace décadas. Sin embargo, el criterio para determinar que una muestra es compatible con el disparo de un arma de fuego prácticamente no ha cambiado desde su conformación original, el cual está determinado por la presencia o ausencia de al menos una partícula con composición de PbBaSb. Este criterio tiene la desventaja de ser estricto y exclusivo, ya que ninguna otra composición es considerada relevante, y además, excluye aquellas partículas producto de municiones que no poseen Sb en su composición. En este trabajo ahondaremos en la búsqueda de otras composiciones que brinden información similar a la de las partículas PbBaSb a partir de los análisis forenses de muestras recolectadas de manos en causas judiciales. Para ello, construimos una base de datos de más de 3000 muestras gracias a la colaboración de los laboratorios forenses nacionales de Rosario, Chaco y Tucumán. Utilizando herramientas estadísticas y de inteligencia artificial, encontramos que la presencia de partículas con composiciones CuPbBa y CuZnPbBa están muy correlacionadas con la presencia de partículas PbBaSb. Estas nuevas composiciones podrán emplearse para generar criterios complementarios para el análisis de muestras y eventualmente ampliar los resultados de la técnica para municiones sin Sb.**

***Index Terms*—GSR, Machine Learning, Estadística Bayesiana, MySql, Forense**

I. Introducción

La detonación de un arma es un evento termodinámico extremo de alta presión y temperatura. La deflagración de la carga explosiva genera gases que salen proyectados a 2000 °C arrastrando partículas metálicas que rápidamente se enfrían y se depositan en las proximidades del tirador cuando realiza un disparo. A estas partículas se las conoce como residuos de disparo, o GSR por su nombre en inglés *GunShot Residue* [1]. La búsqueda de GSR se realiza tomando muestras de manos con cintas de carbono adhesivas montadas en portamuestras de aluminio cilíndricos de 12.7 mm de diámetro, comúnmente denominados stubs (Fig. 1).

El procedimiento de toma de muestra de GSR depende del país y región. Es habitual que se realicen 50 toques del stub sobre la superficie de interés (en general las manos de sospechosos) o hasta que la cinta de carbono pierda adherencia [2]. Al llegar al laboratorio las muestras se analizan con un microscopio electrónico de barrido (SEM) acoplado con un espectrómetro de rayos X (EDX) e integrado con un software de búsqueda automática de partículas metálicas. El resultado del análisis consiste en una caracterización elemental de todas las partículas metálicas en la muestra.

Figura 1. Stub de aluminio 12 mm de diámetro con cinta de carbono de doble adherencia. El mismo esta´ depositado en un recipiente listo para hacer una toma de muestra de GSR y mantenerlo preservado después de la toma.

El último protocolo para el análisis de residuos de disparo fue publicado en 2020 [3]. Las definiciones de partículas vigentes y que usaremos en este manuscrito son:

- *partículas características*: aquellas cuya composición elemental raramente tienen un origen distinto que GSR.
- *partículas consistentes*: aquellas cuya composición elemental se encuentra en los GSR y aparecen en otros contextos no relacionados con las armas de fuego.
- *partículas ambientales* o *comúnmente asociadas*: aquellas metálicas frecuentes en el ambiente.

En este protocolo las partículas clasificadas como características son solamente aquellas que están compuestas elementalmente por combinaciones Pb-Ba-Sb, a pesar de que no todas las municiones producen estos residuos [4]. Las partículas clasificadas como consistentes poseen Pb-Ba, Pb-Sb, Sb-Ba, Ba-Al, y Ba-Ca-Si. Finalmente, las partículas ambientales son aquellas que no tienen combinaciones de estos elementos y pueden poseer individualmente alguno de los elementos Pb, Ba y Sb.

Las mediciones de las muestras son luego interpretadas por un perito en un informe pericial. Si en una muestra se detecta al menos una partícula característica se concluye que la muestra es compatible con residuos de disparo de un arma

de fuego. En ese caso no necesariamente la persona de la cual se tomó la muestra ejecutó un disparo. Estas partículas pueden tener otro origen: ser resultado de la transferencia de alguna superficie contaminada o haber estado en la proximidad de un disparo. Las consecuencias jurídicas de este tipo de pericia deben ser evaluadas junto con el resto de la evidencia en la causa.

El aporte de las pericias de GSR en el ámbito judicial depende estrictamente del nivel de certeza que tenga la asociación entre la muestra y el contexto en el que se disparó un arma. Por esta razón el estudio de fuentes alternativas de partículas consistentes y características, como de los procesos de transferencia, ha sido indispensable desde los orígenes de la técnica hasta la actualidad (G. M. Wolten [5]–[7]). Se ha encontrado que en algunos talleres de frenos de autos, los trabajadores presentaban ocasionalmente la presencia de partículas con los elementos Pb-Ba-Sb y morfología irregular [8].También es importante conocer cuál es la aparición de las partículas de GSR en la población general. N. Lucas y colaboradores hicieron un relevamiento en Australia de la incidencia de partículas metálicas en la población, eligiendo 289 personas con diversas ocupaciones [9]. Encontraron en 11 personas partículas consistentes y sólo una persona con una partícula característica, que curiosamente no poseía un arma y no estuvo en contacto con una.

Hay varias maneras de que lleguen partículas características al cuerpo sin haber disparado un arma. La más directa es estar presente a corta distancia de un tirador. Los gases despedidos depositan partículas metálicas en las proximidades de quien dispara [10]. También queda una gran cantidad de partículas en el arma que potencialmente puede contaminar cualquier superficie con la que entre en contacto. Se han hecho estudios sobre la presencia de GSR en los asientos traseros de patrulleros y comisarías, por ejemplo R. Berk reportó la detección de partículas características en el 20 % de las muestras provenientes de las comisarías de Chicago [11]
. Otra forma de transferencia es el contacto con las manos de un tirador, J. French estableció diferentes escenarios de contaminación y encontró que basta un apretón de manos para que se transfieran partículas características [6], [7].
Desde la introducción de la técnica de SEM/EDX no han cambiado las categorías de partículas asociadas a GSR ni la interpretación de los resultados de los análisis. Sigue siendo la detección de partículas con elementos Pb-Ba-Sb el criterio principal para asociar una muestra con la detonación de un arma de fuego. Pensamos que esto no agota toda la información que puede extraerse de una muestra. Uno de los propósitos de esta tesis consiste en desarrollar herramientas estadísticas para extender las categorías actuales y su significancia.
El análisis de una muestra de GSR se basa en la detección de estas partículas. Los informes periciales interpretan estos resultados y sólo afirman la compatibilidad de una muestra con la detonación de un arma de fuego cuando se han encontrado partículas características en la muestra, mientras que el resto de la información es excluida. Esto nos convoca a preguntarnos: ¿Qué información útil hay en la población de partículas registradas como ambientales? ¿Qué otros elementos están asociados a las partículas consistentes? y ¿Hay información útil en esos datos sin utilizar? Para responder estas preguntas debemos salir de las categorías de partículas establecidas e indagar en otras combinaciones de elementos presentes en las muestras y partículas de las bases de datos.

II. Muestras de laboratorios forenses

Accedimos a la información de los análisis de las muestras de causas judiciales realizando convenios con tres servicios forenses del país: Organismo de Investigaciones del Ministerio Público de Acusación de la provincia de Santa Fe (LQDR) que cuenta con un microscopio de barrido *Zeiss Evo LS 15* con un espectrómetro de rayos X *XMax* de *Oxford instruments*, Centro Integral de Microscopía (CIME) de la Universidad Nacional de Tucumán que cuentan con *Zeiss SUPRA 55VP* acoplado con un detector de rayos X *PentaFet* de *Oxford Instruments* e Instituto de Medicina y Ciencias Forenses (IMCiF) que depende del poder judicial de la provincia de Chaco, que en su laboratorio trabajan con un microscopio *Zeiss Evo LS 15* con un espectrómetro de rayos *X XMax* de *Oxford Instruments*. En cada caso la información compartida fue anonimizada y eliminamos cualquier dato sensible de la causa en cuestión. Resumimos esta información en la Tabla I.

Servicio	Lugar	SEM	EDS	Número de muestras
LQFR	Santa Fé	*Evo LS 15*	XMax	1117
CIME	Tucumán	*SUPRA 55VP*	*PentaFe*	1191
IMCiF	Chaco	*Evo LS 15*	*XMax*	831

Tabla I
DESCRIPCIÓN DE LOS SERVICIOS FORENSES CON LOS QUE DESARROLLAMOS LA BASE DE DATOS.

Los tres servicios trabajan con el mismo sistema automático de búsqueda de GSR, el *INCAEnergy* de *Oxford Instruments*. Las variables morfológicas y elementales de cada partícula medidas por el sistema las mostramos en la Tabla II. En la Figura 2 vemos una imagen del resultado de análisis de una partícula característica utilizando este sistema.

Variable	Descripción	Unidades
Area	área	μm^2
Breadth	ancho	μm
CentreX	posición en X	píxeles
CentreY	posición en Y	píxeles
Direction:	ángulo entre X e Y	-
ECD:	diámetro circular equivalente	μm
Length:	largo	μm
AspectRatio:	relación entre ancho y largo	-
Perimeter	perímetro	μm
Shape:	medida de circularidad	-
AC	concentración atómica	%
Wt	concentración en masa	%

Tabla II
VARIABLES REGISTRADAS POR EL *INCAEnergy* AL ANALIZAR PARTÍCULAS

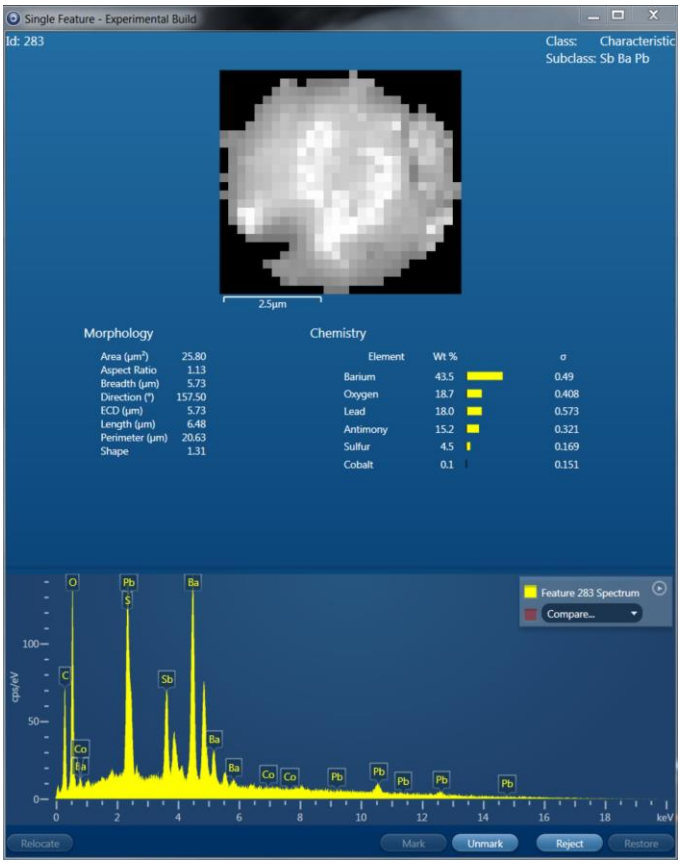


Figura 2. Partícula característica de GSR detectada por electrones retrodispersados por el sistema automático de barrido INCA Energy de *Oxford Instruments*. Los resultados del análisis presentan información morfológica de la partículas y de los elementos presentes en ella.

III. BILBLIOTECA DE SOFTWARE GsrDB

Una vez concluido el análisis de una muestra, las mediciones de cada partícula son almacenadas en un archivo. Este sólo es accedido a través del software propietario *INCAEnergy* en la computadora del microscopio, que no permite hacer comparaciones entre muestras. Estas limitaciones impiden hacer un seguimiento del servicio a largo plazo, dificultando su gestión. Por estos motivos diseñamos el sistema GsrDB [12] que toma los archivos procesados por el microscopio y los incorpora en una única base de datos relacional *MySQL*.

III-A. Arquitectura

La base de datos que creamos tiene la misma estructura que los archivos del *INCAEnergy*, pero con una capa adicional que indexa y facilita la navegación entre las muestras. En la Figura 3 presentamos la arquitectura con los objetos que participan en la base de datos. La información de cada análisis está almacenada en un archivo en el microscopio con extensión *.mdb*, donde se detalla la configuración del microscopio y las mediciones de las partículas detectadas. Los archivos *.mdb* se descomponen en 'Areas' que representan los stubs introducidos en el microscopio. Estos están indexados por un 'AreaID' y tienen asociados campos de barrido de la muestra, indexados por 'FieldID'. Estos campos son las regiones delimitadas de la muestra que son navegadas por el INCAEnergy en la etapa de descubrimiento, donde se detectan las partículas. Cada una de estas partículas (llamadas 'Features' en la base de datos) tiene asociada mediciones que se usan para la clasificación en: características, consistentes o ambientales, acorde a lo que indica la normativa [3]. Para mayor detalle sobre la estructura de la base datos consultar [12].

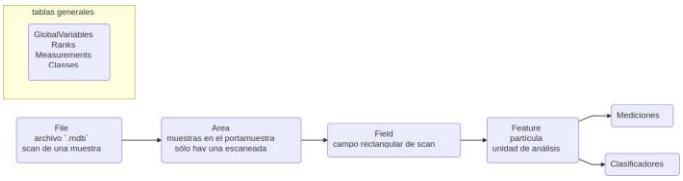


Figura 3. Estructura de objetos que conforman las entradas de la base de datos. La arquitectura de la información es a partir de archivos (Files), muestras o stubs (Areas), campos analizados (Fields), partículas detectadas (Features) y, mediciones y clasificaciones sobre cada una de ellas. A su vez, la información de los parámetros de configuración del barrido esta´ almacenada en los archivos en tablas (GlobalVariables, Ranks, Measurements, Classes).

IV. ELEMENTOS RELEVANTES EN LAS BASES DE DATOS

Empezaremos por comparar las elementos presentes en las muestras de cada base de datos, distinguiendo aquellas en donde se encontraron partículas características y en donde no. Denominamos en el texto como:

- MC: muestras en donde se encontraron partículas características (PbBaSb)
- $\overline{MC}$: muestras en donde no se encontraron partículas características.

Queremos determinar qué información adicional de las muestras MC puede utilizarse para identificarlas, además de la presencia de las partículas características. Por esta razón, eliminamos del registro todas estas partículas, es decir, aquellas que contienen simultáneamente Pb, Ba y Sb. De esta manera, el resultado de una pericia para todas las muestras seria negativo.

Realizado este filtro, analizamos la cantidad de veces que aparece cada elemento químico en las bases de datos de cada servicio y comparamos las frecuencias observadas para las muestras MC y $\overline{MC}$. Los detalles técnicos de la comparación estadística entre los histogramas pueden verse en el Apéndice. En la Figura 4 presentamos las frecuencias de todos los elementos químicos para los dos tipos de muestra en los tres servicios estudiados. Los valores positivos en la comparación representan el nivel de significancia estadística (relevancia) que posee la presencia de ese elemento en las muestras MC y, de igual manera, los negativos representan este aspecto para las muestras $\overline{MC}$.

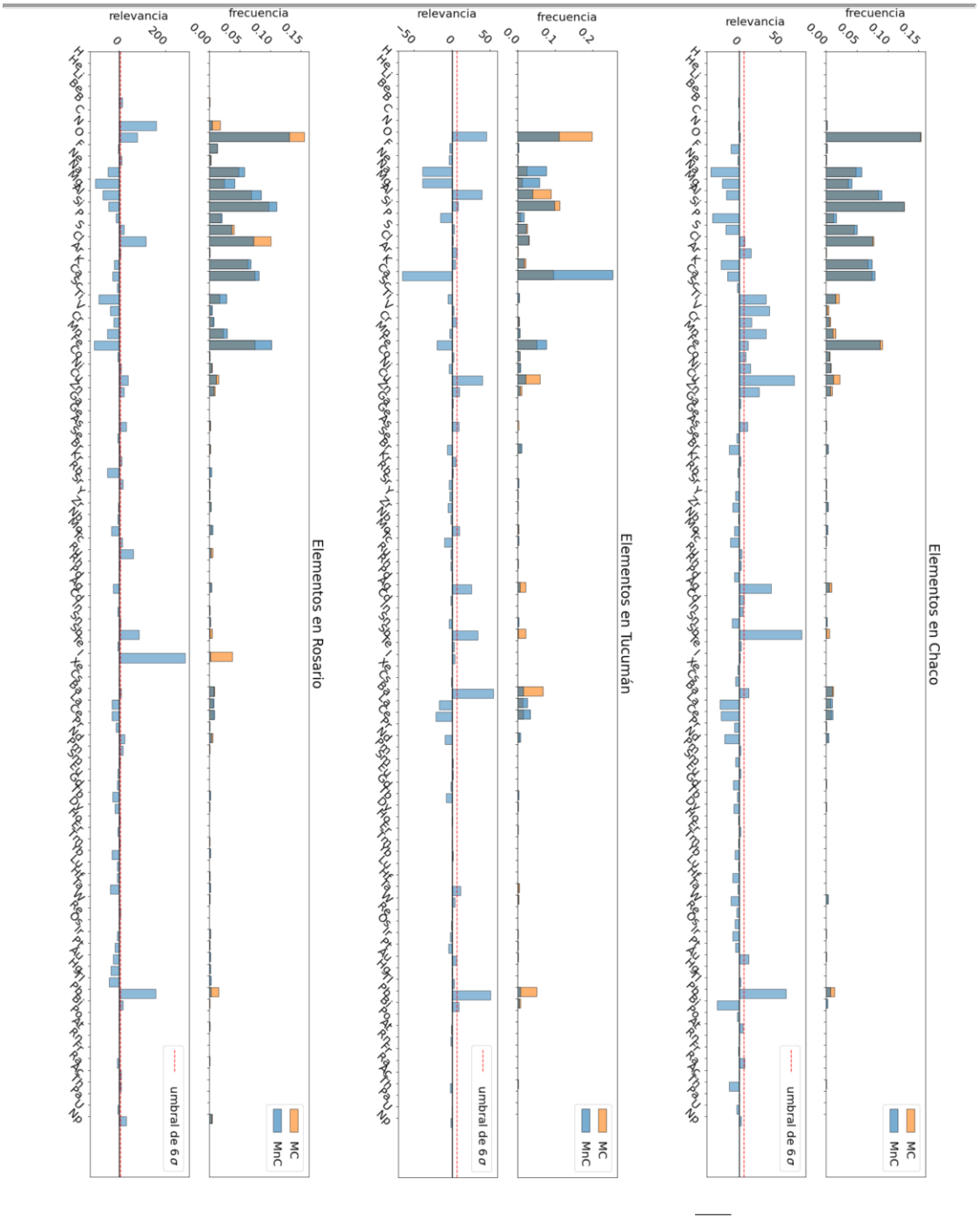


Figura 4. Histogramas de la frecuencia de aparición de cada elemento químico en las muestras MC y *MC* para los servicios de IMCiF, CIME y LQFR. La relevancia para cada elemento corresponde a la diferencia estadística entre los dos tipos de muestras en unidades de dispersión, ver [sec:appendiceA]Apéndice A.

Existe una asimetría en este ejercicio, nos interesa buscar información para identificar una muestra como MC a partir de los elementos presentes en ellas. Por otro lado, carece de sentido clasificar una muestra como $\overline{MC}$ por presentar algún elemento específico dado que sabemos que estas muestras no son identificadas por algún criterio concreto, sino simplemente por el hecho de no ser MC. Por esta razón nos vamos a concentrar solamente en los elementos estadísticamente significativos en las muestras MC, es decir los que presentan una discrepancia estadística positiva. Tomando un umbral de 6σ para la selección de los elementos (ver [sec:appendiceA]Apéndice A) determinamos los elementos relevantes comunes a las tres bases de datos, estos son Cu, Zn, Sb, Ba y Pb (Tabla III). Notamos que estos elementos son los que componen el encamisado de las puntas de las municiones, Cu y Zn, y también los principales elementos que conforman a los fulminantes, Sb, Ba y Pb.

Elemento	Nombre	Z	Fuente
Cu	Cobre	29	Encamisado y vaina
Zn	Zinc	30	Encamisado y vaina
Sb	Antimonio	51	Fulminante
Ba	Bario	56	Fulminante
Pb	Plomo	82	Fulminante y punta

Tabla III
TABLA DE LOS ELEMENTOS ELEGIDOS SEGÚN LA DISCREPANCIA ESTADSTICA QUE POSEEN CUANDO SE COMPARA SU OCURRENCIA EN LA POBLACIÓN DE MUESTRAS MC CON $\overline{MC}$.

V. NUEVAS COMBINACIONES RELEVANTES

A partir de los elementos elegidos (Cu, Zn, Sb, Ba y Pb) armamos las 27 combinaciones elementales posibles para las partículas. Estas combinaciones son aquellas que presentan hasta 4 elementos y que no son partículas características tradicionales, por lo que no pueden contener Pb, Ba y Sb simultáneamente.

Luego, extraemos de la base de datos el número de partículas detectadas que posee cada combinación elemental definida. Para el análisis de estas partículas filtramos la base de datos para mejorar la discriminación entre las dos poblaciones MC y $\overline{MC}$. En el caso de la población de MC nos quedamos con aquellas muestras con más de 2 partículas características, y en la población $\overline{MC}$ descartaremos aquellas muestras que no contenían partículas con la combinaciones de elementos obtenidas. Este procesamiento hace que la distancia estadística entre las poblaciones de muestra sea más grande y nos ayude a encontrar mejores criterios para diferenciarlas. Los dos conjuntos de datos resultaron en un población MC de 598 muestras y otra $\overline{MC}$ de 2518 muestras.

En la Figura 5 presentamos la ocurrencia promedio de cada combinación de elementos en las muestras MC y $\overline{MC}$ de la base de datos filtrada. Allí vemos que todas las combinaciones propuestas son detectadas con más frecuencia en las muestras MC. Esta observación es consistente con nuestra elección de elementos químicos (Tabla III) y sugiere que la presencia de estas partículas puede resultar útil para la clasificación de muestras.

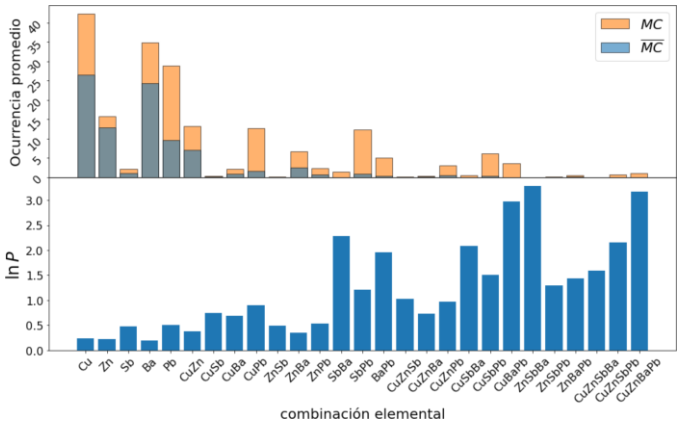


Figura 5. Ocurrencia y relevancia, cuantificada como $\ln\left(\frac{P(c_i \mid MC)}{P(c_i \mid \overline{MC})}\right)$, de las combinaciones definidas por los elementos que distinguen a las muestras MC y $\overline{MC}$ de la base de datos unificada.

Una forma de cuantificar la relevancia de estas composiciones es comparar la probabilidad de que una muestra sea MC dado que hemos observado una combinación de elementos c_i, con la probabilidad de que sea $\overline{MC}$ utilizando la misma información. El cálculo de esta probabilidad lo hacemos con el Teorema de Bayes:

$$\ln P \equiv \ln\left(\frac{P(MC \mid c_i)}{P(\overline{MC} \mid c_i)}\right) = \ln\left(\frac{P(c_i \mid MC)}{P(c_i \mid \overline{MC})}\right) + \ln\left(\frac{\pi_{MC}}{\pi_{\overline{MC}}}\right) \quad (1)$$

donde notamos $\ln P$ a la discriminación estadística. o relevancia, y c_i corresponde a la composición i dentro de las 27 posibles.

En la Figura 5 representamos el resultado del cálculo de la Ec. (1) para las combinaciones propuestas. Allí notamos que las tres combinaciones más relevantes son Zn-Sb-Ba, Cu-Zn-Ba-Pb y Cu-Ba-Pb. Estas poseen elementos del encamisado, fulminante y vaina de la munición. Creemos que estas combinaciones aportan información adicional comparado con las partículas características tradicionales compuestas por Pb, Ba y Sb. Sin embargo, para que estas combinaciones elementales sean útiles en la práctica forense es fundamental que sean abundantes en la población de muestras MC. En la Tabla IV presentamos la frecuencia de ocurrencia de estas tres partículas en las muestras MC y $\overline{MC}$.

Combinación	MC [%]	$\overline{MC}$ [%]	$\ln P$
Zn-Sb-Ba	3.2	.1	1.8
Cu-Zn-Ba-Pb	33.9	1.4	1.7
Cu-Ba-Pb	67.9	3.5	1.5
Alguna de las anteriores	75.3	4.4	1.4

Tabla IV
FRECUENCIA DE OCURRENCIA Y NIVEL DE RELEVANCIA $\ln P$, DEFINIDO EN LA EC. (1). DE LAS PARTÍCULAS CON LAS COMBINACIONES ELEMENTALES ZN-SB-BA, CU-ZN-BA-PB Y CU-BA-PB EN LAS MUESTRAS MC Y $\overline{MC}$.

En la Tabla IV observamos que la partícula con mayor relevancia es Zn-Sb-Ba con $\ln P = 1{,}8$. Esto significa que al

encontrar al menos una de estas partículas es $e^{1,8} \sim 6$ veces más probable que haya partículas características en la muestra a que no las haya. Sin embargo, vemos también que sólo un 3 % de muestras MC contiene esas partículas. Por otro lado, las partículas Cu-Ba-Pb tienen una relevancia similar a las anteriores, pero aparecen en la mayor parte de las muestras MC. Concluimos que la combinación Cu-Ba-Pb está muy correlacionada con la presencia de las partículas características que en una gran cantidad de casos su detección puede ser de utilidad para re-evaluar el resultado del análisis de una muestra.

La presencia de partículas con combinaciones Zn-Sb-Ba, Cu-Zn-Ba-Pb o Cu-Ba-Pb sugieren que la muestra es de tipo MC. Es tentador establecer un criterio rígido a partir de ellas como el criterio definido por la presencia o ausencia de partículas caracter´ısticas. Este criterio presenta un 25 % de falsos negativos y un 5 % de falsos positivos lo cual es un resultado útil en la práctica. Por ejemplo, puede usarse como criterio para evaluar cómo proceder si se hizo un barrido y no se encontraron partículas características, pero sí muchas consistentes. La detección de alguna de las combinaciones elementales Zn-Sb-Ba, Cu-Zn-Ba-Pb o Cu-Ba-Pb invita a hacer un nuevo barrido con más detalle, por ejemplo un tamaño de píxel más chico. Para entender qué tan útil es este criterio comparado a otros posibles necesitamos herramientas adicionales que desarrollaremos a continuación.

VI. MÉTRICAS PARA LA EVALUACIÓN DE UN CLASIFICADOR

Si bien un resultado como el descrito en el final de la sección anterior es útil, se puede mejorar haciendo uso simultáneo de todas las otras combinaciones de elementos encontradas. Individualmente pueden ser relevantes, pero todas en su conjunto serán más efectivas.

En esta sección vamos a utilizar sistemas de clasificación que requieren como entrada la base de datos utilizada. Buscaremos una regla estadística que maximice la diferencia entre las dos categorías de muestras, MC y $\overline{MC}$. Las reglas estadísticas se diferencian de las reglas rígidas en que no tienen una condición estricta para definir la clasificación. Con "reglas estadísticas" no queremos decir que la evaluación ante una misma entrada será diferente cada vez, sino que el resultado será un número entre 0 y 1, que representa la probabilidad que formula el clasificador de que la muestra sea MC. En ese sentido la "rigidez" de los sistemas de clasificación estadísticos aparece en la determinación de un umbral de probabilidad a partir del cual se defina una clase o la otra.

Los sistemas de clasificación estadístico están diseñados para encontrar la máxima separación entre las clases según la información que le brindemos de cada una. Para evaluar el rendimiento de los sistemas al clasificar las muestras contamos con las métricas que mencionamos en los capítulos anteriores. Estas son: los falsos positivos (FP), falsos negativos (FN), verdaderos positivos (VP) y verdaderos negativos (VN).

Una forma común de visualizarlas es a través de lo que se conoce como matriz de confusión [13].

$$\text{Matriz de confusión} = \begin{array}{|c|c|}\hline \text{VN} & \text{FP} \\ \hline \text{FN} & \text{VP} \\ \hline \end{array} \qquad (2)$$

La matriz de confusión brinda mucha información sobre el rendimiento del sistema, pero es preferible condensarla en otras métricas concisas. Aquí tomaremos las métricas llamadas y precisión y sensibilidad definidas por [1]:

$$\text{precisión} = \frac{VP}{VP+FP} \qquad \text{sensibilidad} = \frac{VP}{VP+FN} \qquad (3)$$

Para ganar un poco de intuición sobre ellas, podemos pensar que una manera de obtener precisión perfecta es hacer sólo una predicción positiva y estar seguros de que es correcta. En ese caso no tendremos ningún falso positivo y, por lo tanto, $\text{precisión} = \frac{1}{1+0} = 100\%$. La métrica nos da un resultado perfecto, pero es un clasificador poco útil en la práctica dado que ignoramos todas las otras instancias positivas de los datos. Para complementar esta métrica utilizamos la sensibilidad que corresponde, como indica en la Ec. (3), a la relación que hay entre clasificaciones positivas correctas entre todas las positivas en el conjunto de datos. En general dependerá del problema cuál de las dos métricas es más importante maximizar.

Si utilizamos como sistema de clasificación la presencia de alguna de las combinaciones Zn-Sb-Ba, Cu-Zn-Ba-Pb o Cu-Ba-Pb obtenemos una matriz de confusión:

Matriz de confusión (ZnSbBa, CuZnBaPb o CuBaPb) =

2406	112
148	450

Luego, los resultados de las métricas de precisión y sensibilidad son:

$$\text{precisión} = 80\,\% \qquad \text{sensibilidad} = 75\% \qquad (4)$$

Nos interesa construir un clasificador que en la instancia de no encontrar partículas características, pero sí muchas consistentes, nos guíe en la decisión de analizar con más detenimiento la muestra o no. En general, en esta situación es usual que los operadores re-examinen la muestra, por lo que un criterio útil en la práctica será aquel que cuando una muestra se clasifique como $\overline{MC}$ podamos descartar la muestra con seguridad. Buscaremos otros criterios incorporando información de otras combinaciones de elementos para aumentar la sensibilidad, respecto al criterio anterior sin perder mucha precisión.

VII. ENTRENAMIENTO DE UN CLASIFICADOR ESTADÍSTICO

Para generar un criterio de clasificación utilizaremos métodos de aprendizaje estadístico también conocido como *Machine Learning*. Las técnicas de clasificación de Machine Learning las dividimos en dos tipos: unas que plantean una

[1] Comúnmente llamadas *precicion* y *recall*

función de discriminación con un umbral bien definido y otras formadas por ensambles de clasificadores pobres [14].

Entre las primeras técnicas se encuentra el método de LDA, el cual consiste en ajustar cada categoría de datos con una distribución gaussiana multivariada y determina el umbral de clasificación con los puntos de equiprobabilidad entre estas distribuciones. Estos puntos definen hyperplanos en el espacio de entrada que, si la dimensión es baja, son de fácil interpretación. Por otro lado, si la dimensión es alta, las direcciones en donde el clasificador cambia de predicción resultan poco intuitivas.

Las técnicas de ensamble trabajan bajo la premisa de que un conjunto de muchos clasificadores independientes tiene un gran rendimiento [15]. Estos clasificadores no son necesariamente muy efectivos individualmente, pero sí cuando son promediados entre sí. Uno de los métodos de ensamble más usados es el Random Forest que utiliza como clasificadores árboles de decisión[2] [16]. Cada árbol trabaja articulando porciones de datos de forma aleatoria y un subconjunto de variables para la clasificación. Una vez ajustado cada árbol, el promedio de la clasificación de todos ellos da el resultado final del método. La estructura de los métodos de ensamble hace que no podamos interpretar la razón de una clasificación. Sin embargo, existen herramientas que permiten determinar qué variables son las más relevantes, una muy utilizada en la literatura es el *feature importance*. Esta métrica toma valores en el intervalo $(0, 1)$ y es más grande cuanto más relevante sea la variable para discernir entre las categorías de los datos.

VII-A. Procesamiento de los datos y ajuste

Los algoritmos de aprendizaje estadístico tienen como propósito identificar patrones en un conjunto de datos para luego funcionar como clasificadores de datos nuevos. Este concepto se conoce como *generalización*, y corresponde a la capacidad del sistema clasificar correctamente datos que no fueron parte de su conjunto de entrenamiento.

Para poder estimar la capacidad de un sistema de clasificación de generalizar, o bien estimar el error del sistema para nuevos datos, utilizamos el procedimiento estandarizado que comienza con la partición *train-test*. El sistema es entrenado con el 80 % de los datos y una vez que se selecciona el mejor modelo, se evalúan las métricas de interés sobre la partición de test (el 20 % restante de los datos). Los resultados obtenidos sobre la partición de test son la estimación final del rendimiento y el error de generalización del sistema.

Una vez divididos los datos, el procedimiento continua mediante la realización del ajuste del sistema. Al tratarse de sistemas de muchos grados de libertad, es decir muy maleables, es fundamental evaluar la posibilidad de que haya un sobre-ajuste. Una manera de hacerlo es a través de una validación cruzada que consiste en los siguiente: definimos 5 conjuntos disjuntos de datos que preservan las proporciones de cada categoría establecida, elegimos uno de los 5 conjuntos definidos, lo apartamos y entrenamos con los 4 restantes. Luego, evaluamos las métricas de interés y el error de clasificación sobre el conjunto apartado y repetimos el proceso. Al realizar el entrenamiento y luego la evaluación con cada uno de los subconjuntos planteados obtenemos 5 métricas y errores. La inspección de estos resultados son los que indican si el sistema está sobre-ajustando los datos o no y, a su vez, indican que´ tan bueno es el modelo en generalizar para datos con los que no fue entrenado. Las métricas resultantes de la evaluación sobre estos 5 conjuntos apartados en la validación cruzada son los que utilizamos para seleccionar el mejor modelo.

Los datos de entrada que utilizaremos son listas de 27 variables divididas en dos categorías MC y $\overline{MC}$. Las variables contienen información del número de partículas con las combinaciones elementales presentadas en Sec. V por muestra. Esta información la transformamos según la expresión $\ln(1 + n_i)$ donde n_i es el número de partículas con la combinación de elementos i. Esta transformación es conveniente porque acentúa las diferencias cuando se tiene una pequeña cantidad de partículas, que es en general nuestro caso. Le sumamos 1 al argumento del logaritmo para evitar la singularidad cuando no hay partículas de alguna categoría. El procesamiento de los datos y el entrenamiento lo realizamos con la librería de Python 3.7 *sklearn- 0.24.1* [17].

VIII. Resultados

Aquí presentamos los resultados del entrenamiento de los modelos LDA y Random Forest sobre la base de datos. En la elección del mejor modelo sobre cada algoritmo buscamos como prioridad maximizar la sensibilidad manteniendo la precisión por arriba del 75 %. En la Tabla V presentamos los promedios de las métricas sensibilidad y precisión obtenidos tras la validación cruzada sobre ambos modelos:

Criterio	Sensibilidad	Precisión
Presencia de ZnSbBa, CuZnBaPb o CuBaPb	75 %	80 %
LDA	86 %	76 %
Random Forest	90 %	76 %

Tabla V

Comparación de resultados de criterios de clasificación. La presencia de la combinación CuPbBa es la alternativa simple de clasificación de muestras. Luego, los modelos LDA y Random Forest son criterios estadísticos que utilizan todas las composiciones descriptas en la base de datos.

A partir de estos resultados elegimos como mejor modelo al Random Forest [3]. Para acercarnos a una interpretación de qué combinaciones elementales son las más relevantes en su entrenamiento, calculamos el *feature importance* de cada variable y mostramos las primeras 5 en la Figura 6. Allí vemos que, al igual que en nuestro análisis de frecuencias al comienzo del capítulo, las combinaciones elementales Cu-Ba-Pb y Cu-Zn-Ba-Pb son relevantes en la discriminación de las muestras. Sin embargo, no aparece la combinación Zn-Sb-Ba, lo cual es

[2]Los árboles de decisión son equivalentes a diagramas de flujo en donde cada nodo impone una condición binaria que divide a los datos en dos ramas. Esta condición busca separar la población de tal manera que cada rama quede tenga sólo una categoría de datos.

[3]Los parámetros óptimos implementados en la implementación del Random Forest fueron: "criterio de división": gini, 'max depth': 15, 'max features': 27, 'número de estimadores': 600 .

interesante, dado que remarca que la poca ocurrencia de Zn-Sb-Ba en la muestra resulta poco práctica para la clasificación.

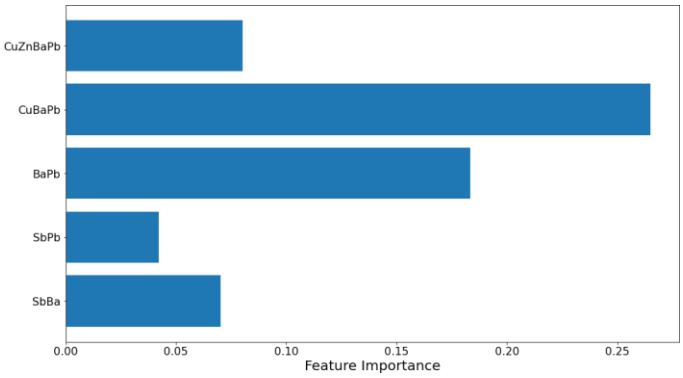


Figura 6. *Feature importance* de las composiciones seleccionadas a partir del entrenamiento del Random Forest.

Habiendo elegido nuestro mejor modelo evaluamos el rendimiento del mismo en la partición de test, para ver su capacidad de generalizar. Los resultados para las métricas precisión y sensibilidad son:

$$\text{precisión}_{\text{test}} = 75\ \% \qquad \text{sensibilidad}_{\text{test}} = 91\ \% \qquad (5)$$

lo cual coincide con nuestra estimación realizada durante el entrenamiento y tiene una alta tasa de reconocimiento de muestras positivas como queríamos. Este resultado nos dice que nuestro modelo es capaz de clasificar correctamente muestras con las que no fue entrenado.

IX. CONCLUSIONES

Hacen falta criterios complementarios de clasificación de muestras los cuales son necesarios para poder desarrollar la técnica de residuos de disparo en mayor profundidad. Esto se debe a que no es siempre posible la detección de partículas características en las muestras, incluso cuando se han tomado de las manos de un tirador. Algunas razones son: que las municiones no poseían Sb, que no se depositaron en la piel, que se perdieron por tomarse la muestra pasado mucho tiempo del disparo, porque en el proceso de barrido y estudio de la muestra no fue posible hallarlas. En este capítulo encontramos que el resultado del barrido y los espectros de las partículas encontradas también poseen información del origen de la muestra, más allá de las partículas características. Sin embargo, en los protocolos actuales esta información no es relevante en un informe pericial.

Con el fin de encontrar nueva información que pueda discriminar entre las muestras donde sí se hallan partículas características y donde no, ahondamos en los elementos químicos presentes en las partículas que distinguen a estos dos tipos de muestras (Tabla III). Las combinaciones elementales resultantes fueron 27 y encontramos que estadísticamente algunas de ellas tienen un gran poder discriminatorio. Las combinaciones Zn-Sb-Ba, Cu-Zn-Ba-Pb o Cu.Ba-Pb resultaron ser las que en su conjunto presentaban una manera simple de distinguir entre los dos tipos de muestras, MC y $\overline{MC}$. Y a diferencia de la composición de las partículas características, todas estas composiciones poseen elementos tanto del encamisado, como de los fulminantes. Esto es fundamental al intentar determinar si la muestra provino de un hecho donde hubo un disparo de arma de fuego. A su vez, dos de estas combinaciones no poseen Sb, el cual en algunas municiones de bajo calibre está ausente, haciendo en ese caso imposible la producción y detección de partículas características. Creemos que estas nuevas partículas cobran especial importancia en esos casos.

A partir de la presencia o ausencia de partículas con elementos Zn-Sb-Ba, Cu-Zn-Ba-Pb o Cu-Ba-Pb planteamos un criterio complementario que puede ser utilizado para determinar si es conveniente analizar una muestra con más detenimiento si, en el resultado de un primer barrido, no se encontraron partículas características. Este criterio identificó el 75% de las muestras MC sin hacer uso de la presencia de partículas características. Por lo que como criterio complementario puede colaborar en qué decisión tomar cuando sólo se hallan partículas consistentes en una muestra.

Por otro lado, creemos que es relevante extraer más información de las muestras y que los resultados de una pericia no estén determinados exclusivamente por la presencia o ausencia de alguna combinación de elementos. Las correlaciones entre partículas con ciertos elementos químicos, así como las cantidades relativas de ciertas partículas respecto a otras, son factores relevantes que pueden explotarse para desarrollar un criterio de clasificación. Para esto acudimos a sistemas de aprendizaje estadísticos diseñados para establecer una probabilidad de categoría de muestra según la información de todas las partículas relevantes presentes. El algoritmo de *Random Forest* resultó ser el mejor modelo para clasificar las muestras obteniendo una sensibilidad del 90 % e identificó que las partículas más relevantes en la clasificación son las que contienen Cu-Ba-Pb. Lo cual indica nuevamente que esta composición tiene mayor relevancia respecto de las otras, e incluso podríamos llamar “quasi-característica”.

El análisis presentado en este trabajo tiene puntos en común con la historia de las técnicas de detección de residuos de disparo. Los elementos propuestos para reconocer el disparo de arma fueron desde un principio aquellos que constituyen a las municiones. Luego, las combinaciones elementales relevantes fueron determinadas al estudiar los espectros químicos de las partículas presentes en muestras de tiradores. Aquí nuestro acercamiento sigue esos mismos pasos, considera los elementos químicos presentes en las municiones, que fueron identificados por la clasificación de las muestras, e incorpora otras composiciones elementales. Utilizando nuestras metodologías encontramos nueva información que es relevante para la técnica. Creemos que la incorporación de estas nuevas combinaciones elementales extienden las categorías de partículas hoy planteadas, ambientales, consistentes y características de residuos de disparo.

X. APÉNDICE

Nos interesa poder comparar cuantitativamente las distribuciones que originan dos poblaciones de datos A y B a partir de histogramas de observaciones, en el caso donde tenemos los mismos bines para ambos histogramas. Definimos un número de observaciones N para la población A y M para la población B.

Para cada bin del histograma tenemos una distribución binomial:

$$n \sim Bin(N,\ p) \qquad m \sim Bin(M,\ q) \tag{6}$$

donde p es la probabilidad de ese bin para la población A y q para la población B.

Basándonos en los trabajos de Katz [18] y Koopman [19], podemos tomar para cada bin la aproximación:

$$s = \log \frac{n/N}{m/M} \sim \mathcal{N}\ (\mu, \sigma^2) \tag{7}$$

donde

$$\mu = \ln (p/q)$$
$$\sigma^2 = \frac{1/p-1}{N} + \frac{1/q}{M} \tag{8}$$

Por lo que podemos modelar y cuantificar la diferencia entre las poblaciones para cada bin con una variable aleatoria gaussiana, parametrizada por μ y σ^2. En el caso de tener muchos bines y que cada uno de estos acumule poca probabilidad podemos aproximar $\sigma^2 \approx \frac{1}{n} + \frac{1}{m}$. Usando el teorema de Bayes podemos hacer inferencia sobre μ, escribimos:

$$P(\mu|s, \sigma^2) \propto P(s|\mu, \sigma^2) = \mathcal{N}\ (\mu, \sigma^2) \tag{9}$$

Este método nos permite cuantificar la discrepancia por bin de las observaciones que hacemos. Al nivel de discrepancia μ lo vamos a medir en unidades de dispersión σ. El nivel de discrepancia en ese caso nos cuantifica la probabilidad de que provengan de diferente distribución.

Para ver con más detalle cómo funciona esta comparación mostramos un ejemplo sintético, usando como base dos distribuciones normales con mismo centro y diferente dispersión. La población A tendrá una dispersión de 1,0 y la B en 1,2. Tomaremos N = 600 observaciones para A y M = 1000 observaciones para B. Dividiremos las observaciones en un total de 20 bines. En la Figura 7 mostramos la comparación con la metodología planteada. Vemos que para valores entre -1 y 1 en el eje horizontal, la discrepancia es positiva y por fuera de ese rango es negativa. Esto representa bien la diferencia entre ambas distribuciones dado que la población B tiene mayor desvió que la población A, dado que las probabilidades de los bines de la población B son más grandes que los de A lejos del centro y más chicos en el centro.

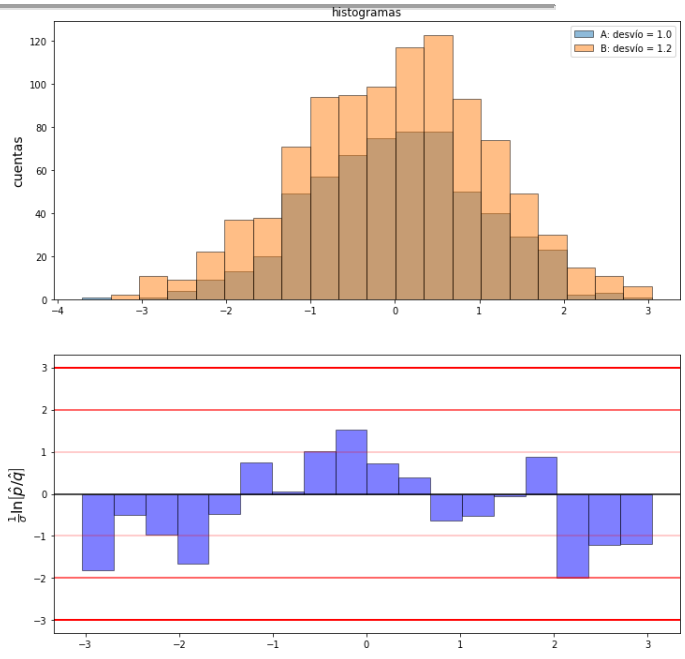


Figura 7. Comparación estadística de las poblaciones A y B. Su distribución es normal con valor medio 0 y desvió 1,0 y 1,2, respectivamente. En la figura de arriba se ven las observaciones por bin de cada población, con un total de N = 600 para la población A y M = 1000 para la población B. En la de abajo vemos el nivel de discrepancia por bin en unidades de σ.

AGRADECIMIENTOS

Queremos agradecer a Edgardo Carignano, Luciano Martín, Hernán Esquivel, Virginia Albarracín y Nadia Filipis, por discusiones interesantes y su ayuda en la conformación de la base de datos.

REFERENCIAS

[1] Smyth Wallace, J. Chemical Analysis of Firearms, Ammunition, and Gunshot Residue. CRC Press, 2008.
[2] Zeichner, A., Levin, N. Collection Efficiency of Gunshot Residue (GSR) Particles from Hair and Hands Using Double-Side Adhesive Tape. J. Forensic Sci., 38 (3), 13441J, may 1993.
[3] ASTM-International. Standard practice for gunshot residue analysis by scanning electron microscopy/energy dispersive x-ray spectrometry. Designation: E1588 20, 2020.
[4] Collins, P., Coumbaros, J., Horsley, G., Lynch, B., Kirkbride, K., Skinner, W., et al. Glass-Containing Gunshot Residue Particles: A New Type of Highly Characteristic Particle? Journal of Forensic Sciences, 48 (3), 1–15, may 2003.
[5] Wolten, G., Nesbitt, R., Calloway, A., Loper, G. Particle analysis for the detection of gunshot residue. ii: occupational and environmental particles. Journal of Forensic Sciences, 24 (2), 1979.
[6] French, J., Morgan, R. An experimental investigation of the indirect transfer and deposition of gunshot residue: Further studies carried out with SEM–EDX analysis. Forensic Science International, 247, 14–17, feb. 2015.
[7] French, J., Morgan, R., Davy, J. The secondary transfer of gunshot residue: an experimental investigation carried out with SEM-EDX analysis. X-Ray Spectrom.,43 (1), 56–61, ene. 2014.
[8] Tucker, W., Lucas, N., Seyfang, K. E., Kirkbride, K. P., Popelka-Filcoff, R. S. Gunshot residue and brakepads: Compositional and morphological considerations for forensic casework. Forensic Science International, 270, 76–82, ene. 2017.
[9] Lucas, N., Brown, H., Cook, M., Redman, K., Condon, T., Wrobel, H., et al. A study into the distribution of gunshot residue particles in the random population. Forensic Science International, 262, 150–155, mayo 2016.
[10] Fojtasek, L., Vacinova, J., Kolar, P., Kotrly, M. Distribution of GSR particles in the surroundings of shooting pistol. Forensic Science International, 132 (2), 99–105, mar. 2003.
[11] Berk, R. E., Rochowicz, S. A., Wong, M., Kopina, M. A. Gunshot Residue in Chicago Police Vehicles and Facilities: An Empirical Study. Journal of Forensic Sciences, 52 (4), 838–841, jul. 2007.
[12] Pregliasco, R., Onetto, M. GsrDB, 2019. URL https://wpregliasco.gitlab.io/gsrdb/

[13] Géron, A. Hands-on machine learning with Scikit-Learn and TensorFlow : concepts, tools, and techniques to build intelligent. O'Reilly Media, 2017.
[14] Hastie, T., Tibshirani, R., Friedman, J. The Elements of Statistical Learning. Springer Series in Statistics. Springer New York Inc., 2001.
[15] Rokach, L. Ensemble-based classifiers. Artif Intell Rev, 33 (1-2), 1–39, feb. 2010.
[16] Breiman, L. Random forests. Mach. Learn., 45 (1), 5–32, oct 2001.
[17] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., et al. Scikit-learn: Machine learning in python. Journal of Machine Learning Research, 12, 2825–2830, 2011.
[18] Katz, D., Baptista, J., Azen, S. P., Pike, M. C. Obtaining Confidence Intervals for the Risk Ratio in Cohort Studies. Biometrics, 34 (3), 469, sep. 1978.
[19] Koopman, P. A. R. Confidence Intervals for the Ratio of Two Binomial Proportions. Biometrics, 40 (2), 513, jun. 1984.

Elementos probatorios en entornos digitales

La tensión entre escasez y la sobreabundancia de información en la etapa de investigación

Matías José Meza. Poder Judicial de la Provincia de Córdoba. Universidad Siglo 21. abmatiasmeza@gmail.com

***Resumen*—El artículo tiene como objetivo iniciar un camino de reflexión sobre los elementos probatorios en entornos digitales durante la etapa de investigación. Para ello, en primer lugar, se realiza una aproximación al razonamiento probatorio en esta fase; seguidamente, se abordan dos extremos en tensión: por un lado, la falta de información típica de esta etapa y, por el otro, el efecto de desborde que se produce ante la gran cantidad de información relevante e irrelevante que se puede encontrar en las fuentes que la contienen. Con todo ello, se argumenta sobre la necesidad de un mayor razonamiento probatorio en la etapa de investigación, proponiendo algunas sugerencias para un abordaje adecuado del entorno digital, desde una concepción racionalista de la prueba y acorde a los requisitos de un debido proceso.**

***Abstract*-- The article aims to begin a path of reflection on evidentiary elements in digital environments during the research stage. To do this, firstly, an approach to evidentiary reasoning is carried out in this phase; Next, two extremes in tension are addressed: on the one hand, the lack of information typical of this stage and, on the other, the overflow effect that occurs due to the large amount of relevant and irrelevant information that can be found in the sources. that contain it. With all this, the need for greater evidentiary reasoning in the investigation stage is argued, proposing some suggestions for an adequate approach to the digital environment, from a rationalist conception of evidence and in accordance with the requirements of due process.**

I. INTRODUCCIÓN

Los presuntos hechos delictivos que investigamos cada vez se encuentran más envueltos en entornos digitales. La Academia Nacional de Ciencias de los EE.UU. advertía esta situación como una posible problemática cuando, hace aproximadamente una década, se refería a ellos como una disciplina de la ciencia forense emergente: "*los medios digitales se han convertido en testigos de las actividades cotidianas, como resultado, casi todos los delitos podrían tener evidencia digital asociada*"[1]. Hoy en día, algunos estudios revelan que alrededor del 90% de los casos criminales que se investigan contienen algún elemento digital asociado.[2]

Esto ha producido un cambio de paradigma, ya que la tradición investigativa se basaba, en gran parte, en abordar solamente los elementos probatorios materiales (indicios biológicos, físicos, químicos, cadáveres, etc.). Posteriormente, con el aumento de la utilización de dispositivos que contienen información digital, se hizo necesario incorporar una visión dual, que incluye tanto lo material como lo digital. Por este motivo, resulta importante indagar sobre el impacto de la dinámica descripta en el razonamiento probatorio.

Si consideramos los tres momentos claves en la actividad probatoria delineados por Ferrer Beltrán (2021, p. 22): "*1) el momento de la conformación del conjunto de elementos de juicio o del acervo probatorio; 2) el momento de la valoración de la prueba y 3) el momento de la decisión sobre la prueba*", es evidente que la información proveniente de entornos digitales enfrenta distintos desafíos en cada una de ellas, pero vale la pena notar que lo que suceda al inicio impactará fuertemente en todas las demás etapas del proceso.

Una de las características típicas de la etapa de investigación, de interés a nivel del razonamiento probatorio[3], se encuentra en relación con la marginalidad que tiene la racionalidad en la realización de las primeras actuaciones, que también se ve reflejada en forma particular cuando lo que se investiga está vinculado a entornos digitales. En general, los procedimientos realizados en dicha etapa están caracterizados por actividades mayoritariamente intuitivas[4], y en el mejor de los casos mediante razonamiento abductivo.[5] En ese sentido, en el tratamiento

[1] Cfr. NRC (2009). Strengthening forensic Science in the United Stated: A PathForward. National Academies Press. https://nap.nationalacademies.org/catalog/12589.

[2] En el reciente trabajo de Wilson-Kovacs, et al (2023) se aborda la creciente importancia de la evidencia digital en la práctica legal, destacando que, en la actualidad, elementos digitales están presentes en un 90% de los casos judiciales en Inglaterra y Gales. En esa línea de ideas, la empresa Cellebrite, especializada en el análisis forense de dispositivos móviles, señala que la evidencia digital se encuentra presente entre un 80 % y un 90 % de todos los casos delictivos que se investigan, abarcando delitos como «pornografía infantil, intrusión en redes, homicidios, crímenes de cuello blanco, pandillas, terrorismo y narcotráfico.». Para obtener más información, se puede consultar el siguiente enlace: https://cellebrite.com/es/principales-desafios-y-cambios-en-el-uso-de evidencia-forense-digital/

[3] Lo consideramos de interés debido a su escasa discusión. A ello se refiere Abimbola (2002, p. 337) cuando indica: "las cuestiones sobre la etapa de descubrimiento tienen un papel escaso o nulo en el razonamiento probatorio en derecho". En ese mismo sentido, Ferrer Beltrán (2020, p. 15) también advierte que, "las reflexiones sobre la fase de investigación penal reciben, lamentablemente, poca atención en la literatura sobre epistemología jurídica."

[4] Binder (1999, pp. 236-237) se refiere a esta etapa como una actividad creativa, que implica superar la incertidumbre mediante la exploración de diversos recursos que puedan proporcionar la información necesaria para disipar dicha incertidumbre.

[5] Para Tuzet (2021, p.125) en la fase de formulación de la hipótesis (fase de investigación o preparatoria) las inferencias son "sustancialmente abductivas". Por su parte para Anderson, Shum y Twining (2015, p.89) "es el proceso creativo del razonamiento. Más que razonar desde una hipótesis hacía una conclusión basada en pruebas, involucra un razonamiento que va desde la prueba hacía una hipótesis que la pueda explicar". Así mismo, Moscatelli (2022. p. 127) nos comenta que se lo utiliza como un instrumento de investigación

de la denominada evidencia digital, los protocolos o guías de buenas prácticas intentan disminuir la subjetividad característica de los primeros momentos de la investigación.[6]

Al igual que las investigaciones donde se procura obtener información sobre potenciales elementos de prueba materiales o tangibles, en las investigaciones en entornos digitales también existen lineamientos generales para abordar los sucesos delictivos o presuntamente delictuosos. En general, estos procesos están orientados en pasos que incluyen: el relevamiento, la adquisición, preparación, extracción y análisis para su posterior presentación.

Los dos primeros pasos, el relevamiento y la adquisición, constituyen puntos críticos y, por ello, ahí nos centraremos en la primer parte del presente trabajo. En relación con estos puntos críticos, la problemática inicial radica en la escasa información característica de la etapa de investigación. Desde una perspectiva crítica, Collie (2018. p.1) manifiesta que: saber cómo iniciar y recuperar evidencia digital puede ser desafiante, incluso para expertos. Sin embargo, la interpretación adecuada de los datos recopilados es crucial para la justicia. Frecuentemente, aquí es donde el sistema falla. En ese sentido podemos identificar al menos 3 aspectos: a) lo que se busca en un entorno digital no está bien definido; b) los elementos provenientes de entornos digitales se encuentran en multiplicidad de fuentes; y, c) hay menos control intersubjetivo ya que es la etapa donde predomina la intuición.[7]

En ese marco, el objetivo general de este trabajo es reflexionar sobre los elementos probatorios en entornos digitales durante la etapa de investigación. Y, específicamente, describir dos extremos: Por un lado, la falta de información típica de esta etapa y, por el otro, el efecto desborde que se produce ante la gran cantidad de información relevante e irrelevante que se puede encontrar en las fuentes que la contienen. Con todo ello, se pretende argumentar sobre la necesidad de un mayor razonamiento probatorio en la etapa de investigación, proponiendo algunas sugerencias para un abordaje adecuado del entorno digital, desde una concepción racionalista de la prueba y acorde a los requisitos de un debido proceso.[8]

II. ESCASEZ INFORMATIVA EN LA FASE DE INVESTIGACIÓN.

Con frecuencia, en los primeros momentos de la investigación la información es escasa.[9] Esto se debe a varios factores, como la complejidad del hecho, su tipología, que el lugar del hecho es abordado tardíamente, la novedad incipiente de la ocurrencia del hecho delictivo y, por supuesto, que el acto de investigar implica generar nuevos conocimientos sobre el suceso. En ese sentido, la persona responsable de la investigación criminal, al analizar los indicios recolectados en el lugar de un crimen o frente al informe de un posible delito, se enfrenta a la necesidad de elaborar una hipótesis que explique un conjunto específico de hechos pasados. Esto produce que se busque más información que confirme si la hipótesis es precisa o si, por el contrario, los datos disponibles son insuficientes para respaldarla, lo que puede implicar un cambio en la dirección de la investigación (Moscatelli, 2023, p. 127).

Frente a esta situación, los escasos datos o información disponible en los primeros momentos son transmitidos a las primeras personas que intervienen en el lugar del hecho para llevar a cabo las acciones necesarias en busca de elementos que puedan ser útiles en la investigación. Esta característica de la escasez de información nos enfrenta a un panorama inicial impreciso, lleno de incertidumbre, que sin duda tendrá un impacto en esta fase y en las que siguen. Si bien podríamos plantear varias cuestiones, nos centraremos en tres aspectos específicos: la problemática de lo que se busca, el control intersubjetivo limitado y la protección de los derechos fundamentales, todo esto orientado a la investigación criminal en entornos digitales.

que permita generar hipótesis para explicar un determinado fenómeno a partir de datos incompletos y disponibles.

[6] Si bien no es objeto del presente trabajo, es importante considerar que no siempre todos los protocolos o guías de buenas prácticas son eficientes; muchas de ellas camuflan procedimientos intuitivos o los formalizan. Un ejemplo de ello lo encontramos en documentos de instrucción policial de la policía de Brasil donde textualmente se afirma: "El policía civil, en el curso de una investigación policial, podrá apoyarse, como aporte, en la intuición, la presunción y las hipótesis, hasta completar su trabajo, que culminará con llegar a una conclusión determinada por la convicción o la certeza.". En el mismo documento posteriormente se establece una definición de intuición. Se puede acceder al documento en el siguiente enlace: https://www.acadepol.ms.gov.br/artigos/importancia-dapratica-didatica-na-investigacao-policial/

[7] El control intersubjetivo implica la capacidad de validar o verificar la comprensión o interpretación de un fenómeno entre diferentes individuos. En ese sentido, la verificación de la veracidad se basa en criterios reconocidos por los sujetos del sistema, que permiten evaluar la validez (probabilidad, plausibilidad) de los resultados obtenidos. (Haba, 1990, p. 178) En procesos intuitivos, donde la toma de decisiones se basa en percepciones internas y subjetivas, este control puede ser limitado debido a las diferencias individuales en experiencias, perspectivas y conocimientos. Partiendo que la concepción racionalista implica por definición razonamientos, podemos anclar la idea de razonamiento como vehículo de control intersubjetivo.

[8] Siguiendo esa línea de ideas, y como fundamento de la importancia de reflexionar sobre estas cuestiones, Haack (2015, p. 69) manifiesta: "es mejor, en la medida de lo posible, prevenir un problema que arreglar las cosas más tarde". Por su parte Gascón Abellán (2016, p. 365), en acuerdo con Haack, agrega "más efectivo concentrarse en lo que sucede "antes" con el fin de evitar que se produzcan cosas indebidas (fraudes en los laboratorios, malas prácticas en la investigación y en la promoción de una técnica, expertos incompetentes, sesgos evitables, etc.) y de que, si se producen, queden rápidamente al descubierto». Por último, refiriéndose a la etapa de investigación, y específicamente a la labor policial, Merkel (2022, p. 14) comenta que lamentablemente se ha puesto poco foco en la función policial, como si se ha hecho en otros órganos del Estado. De allí la importancia de abordar esta problemática.

[9] "La información no siempre está disponible gratuitamente para los investigadores, por lo que deben ser hábiles en diversas técnicas para perseguirlo, localizarlo y recuperarlo." (Fahsing, 2016, p. 5). En esa línea de ideas Borrás Andrés (2023, p. 24) nos explica que en estos primeros momentos "es frecuente que exista poca claridad acerca de los hechos acontecidos, su tipología delictiva o los sujetos que han participado en ellos." Además, en adición a la falta de datos, se presenta la circunstancia en la que el tiempo disponible para tomar acciones o decisiones es limitado y crítico. En este caso específico, la ausencia de información acerca de ciertas pruebas digitales entra en conflicto con la posibilidad de que estas sean modificadas, alteradas o incluso eliminadas.

A. ¿QUÉ SE BUSCA?

A pesar de que, por lo general, en los primeros momentos de la investigación aún no se cuenta con suficiente información para comprender la complejidad del hecho, el órgano encargado de la investigación debe tomar decisiones que la guíen. Las personas investigadoras, en el lugar del suceso, encargados del relevamiento y la recolección de los potenciales elementos de prueba, ya sean físicos o digitales, se encuentran ante un problema importante, si se cuenta con poca información: ¿Cómo abordar el relevamiento y la recolección? ¿Por dónde se empieza? ¿Qué se busca? ¿Cómo garantizar que los elementos relevados y recolectados sean los suficientes para conocer el hecho?

Por un lado, como la actividad de relevamiento consiste en poder captar de un universo de potenciales elementos de prueba cuáles serían aquellos que contengan la información para acercarse a conocer el hecho, resulta que existen diversas posibilidades de encontrar información digital y esta realidad no siempre es tenida en cuenta por los investigadores. Pondremos un ejemplo. Al investigar un presunto homicidio, en primer lugar, existirá una tendencia a buscar información digital en dispositivos tecnológicos tradicionales como computadoras, teléfonos, discos duros (dispositivos clásicos). Sin embargo, podría existir información relevante que se encuentre en dispositivos menos convencionales, como dispositivos IoT (Internet de las cosas), dispositivos camuflados[10], electrodomésticos inteligentes. En ese sentido, Semprini (2017, p. 91) nos comenta: *"Las evidencias digitales están adquiriendo formas cada vez más inesperadas en nuevos dispositivos o componentes tecnológicos que desafían los procedimientos y metodologías actuales."*

La cuestión aquí radica en preguntarse si las personas que intervienen en primer lugar tienen el conocimiento adecuado para, frente a esta escasez de información, saber dónde buscar. Atentos a ese interrogante, nos encontramos con dos realidades; por un lado, y lo más frecuente, es que la actividad de relevamiento la realice personal policial dotado de una instrucción general, es decir, sin conocimiento especializado en cuestiones tecnológicas específicas.

Por otro lado, nos encontramos con la segunda situación, personal policial o forense que tengan alguna o mucha formación en investigar en entornos digitales. Será obvia la respuesta de quien tendrá más herramientas para poder investigar eficazmente, aun contando con poca información sobre el hecho.[11] Entonces, podemos inferir que si no se sabe dónde específicamente buscar, se estará ante el problema de que el universo de elementos posibles será tan abundante que, posiblemente, mucha información relevante podría no ser recabada.

Frente a la escasez de información en la fase de relevamiento, se destaca una cuestión importante: a pesar de los esfuerzos mediante protocolos, guías de actuación o pautas de trabajo para dirigir de la mejor manera posible la actividad,[12] en general, se suele depender en gran medida de la "creatividad" o la "intuición" como herramientas principales para abordar esta actividad[13]. Con respecto a ello, Di Iorio, et al. (2017, p. 190) nos comenta que:

Debido a la falta de adecuación de normas procesales que definan concretamente la cuestión en análisis, estos se encuentran frente a un panorama de cierta incertidumbre, en la que impera el ingenio y la creatividad en la recolección de la evidencia que sustenta una investigación penal.

Con la finalidad de poder contrarrestar actividades tan subjetivas, la mayoría de los protocolos o guías de buenas prácticas recomiendan que se brinde información contextual a las personas investigadoras con la finalidad de poder guiar el relevamiento. López (2019, p. 8) Es decir, aportar información sobre el tipo de hecho para orientar qué dispositivos buscar en el lugar del suceso.

Una vez concluido el relevamiento, identificando las posibles fuentes de información digital, tiene lugar la segunda fase: la recolección. En ese sentido, surgen elementos conflictivos al plantearse qué se debe recolectar y qué no, y en cada caso, la fundamentación del porqué. La fase de recolección tiene su fundamento en que, frente a una diversidad de elementos de interés, se deben considerar recolectados (incautados o secuestrados) los que se consideren adecuados según los objetivos de la investigación. Un término vinculado a la

[10] Nos referimos a aquellos dispositivos que han sido alterados o camuflados para que parezcan diferentes de lo que realmente son. Los mismos pueden ocultar su verdadera función o contenido, lo que los hace útiles para diferentes propósitos de espionaje, seguridad o evasión. Por ejemplo, un dispositivo camuflado podría parecer un bolígrafo común, pero en realidad es un grabador de voz o un pendrive.

[11] En este sentido, algunos autores afirman que tener en claro la metodología de investigación sumada a la adecuada capacidad de los investigadores son elementos claves para lograr investigaciones eficaces. (Roatta et al. 2015, p. 1) Por otro lado, Haack (2009, p. 15) nos habla del aspecto actitudinal. "La investigación puede ser dificultosa y exigente, y con frecuencia ir por el camino equivocado. A veces, el obstáculo es una falla de voluntad; realmente no queremos saber la respuesta suficientemente mala como para cargar con el problema de explicar, o realmente no queremos saber, y generamos una cantidad de problemas para no llegar a saber."

[12] Los códigos no estipulan ningún requisito, más allá que en la práctica de las actividades de laboratorio. El personal debe cumplir con la norma ISO 17025 y, para las escenas del crimen, cumplir con la norma ISO 17020. (Wilson-Kovacs et al, 2023, p.240)

[13] Partiendo de lo que manifiesta Flashing (2016, p. 11), "los detectives criminales suelen dejarse llevar por sus propias intuiciones." La crítica en relación con el recurso de la intuición en las investigaciones criminales suele centrarse en la subjetividad y falta de fiabilidad como método de toma de decisiones. En ese sentido, la intuición puede estar influenciada por prejuicios personales, experiencias pasadas o emociones, lo que puede llevar a conclusiones erróneas o sesgadas. Además, la intuición no puede ser verificada ni validada de la misma manera que otras formas de evidencia, lo que la hace vulnerable a cuestionamientos sobre su credibilidad y objetividad. Por su parte, Anderson et al. (2021, p. 588) con respecto al recurso de la «experiencia» nos comenta: A medida que los límites de la experiencia se vuelven menos claros, también lo hacen la propiedad y la responsabilidad, lo que provoca que la evidencia digital, especialmente la proveniente de dispositivos móviles, sea cuestionada en los tribunales

actividad antes mencionada es el concepto de triage. El protocolo para la identificación, recolección, preservación, procesamiento y presentación de la evidencia digital (2023, p. 8) lo define como:

Proceso de selección de dispositivos o filtrado de información ordenado por la autoridad judicial, quien aporta los criterios de evaluación sobre los dispositivos electrónicos en el lugar del hecho, susceptibles a ser secuestrados para llevar a cabo un posterior análisis forense.

Ahora bien, de acuerdo con lo antes expresado, la información contextual y el triage se establecen como posibles soluciones a las prácticas subjetivas en los primeros momentos de investigación en entornos digitales. Sin embargo, estas dos prácticas traen aparejadas algunas complicaciones si ponemos a la luz de la cuestión probatoria.

En primer lugar, en relación con la información contextual, es importante destacar que la información referente al contexto del hecho suele ser proporcionada a los primeros intervinientes por la fiscalía o las áreas de investigación. El cuestionamiento surge al plantearse si la información suministrada se limita a una única hipótesis del caso (proveniente de la fiscalía), con el riesgo potencial de omitir elementos que respalden hipótesis alternativas, así como circunstancias exculpatorias, en contraposición al principio de inocencia. En segundo lugar, en cuanto a la utilización del triage en el ámbito de la recolección de evidencia digital, presenta ciertos desafíos y aspectos que podrían ser objeto de crítica.

En primer lugar, la dependencia de la autoridad judicial en la definición de los criterios de evaluación para el triage puede introducir sesgos cognitivos,[14] o tomar decisiones que no reflejan adecuadamente la complejidad de la investigación digital, debido a la pobre cultura digital de nuestros sistemas judiciales. Además, la rapidez requerida en el triage puede llevar a una selección apresurada de dispositivos o información, lo que podría resultar en la omisión de datos relevantes. Este enfoque, centrado en la eficiencia temporal, podría pasar por alto detalles cruciales para la investigación.

B. EL ESCASO CONTROL INTERSUBJETIVO.

Otra de las cuestiones que se plantea frente a la escasez informativa en los primeros momentos de la investigación, y de alguna manera en continuidad con el planteamiento establecido en el punto anterior, consiste en la limitación o insuficiencia en el control sobre qué elementos deben ser relevados y recolectados.

La problemática del escaso control intersubjetivo se refiere a las dificultades asociadas con la verificación y supervisión mutua entre las diferentes personas involucradas en el proceso investigativo, ya sean forenses, fiscales, jueces o defensores. En entornos digitales, donde la complejidad técnica y la rápida evolución de la tecnología son prominentes, la falta de control intersubjetivo puede generar diversas complicaciones.

En los puntos anteriores, hemos reflexionado sobre la naturaleza intuitiva y la falta de regulación en la verificación de actuaciones en el ámbito judicial. Esto nos lleva a considerar un problema fundamental: ¿cómo podemos verificar si las actuaciones son adecuadas y se ajustan a un debido proceso? Por ejemplo, ¿cómo puede un fiscal verificar si un experto forense realizó un relevamiento adecuado si carece de las herramientas específicas para hacerlo? ¿O cómo podemos saber si un oficial de policía llevó a cabo correctamente su labor si el fundamento de la actuación se basó únicamente en la experiencia y la intuición? Otra de las principales complicaciones se encuentra en relación con la brecha de conocimientos técnicos entre las áreas jurídicas y las áreas forenses o expertos en investigaciones en entornos digitales.

Esto implica estar al tanto de los avances tecnológicos, que incluyen el aumento en las capacidades de almacenamiento de datos y la variedad de sistemas, así como realizar inversiones costosas en infraestructura y formación del personal. A pesar de los esfuerzos en curso para abordar estos problemas, las capacidades actuales de los involucrados en el sistema de justicia penal se ven superadas por estas demandas. (Wilson Kovacs et al., 2023, p. 237). En esta etapa de la investigación es crucial que la información se transmita adecuadamente, incluso si es escasa, para que pueda cumplir su función. En esa línea de ideas Wilson-Kovacs et al. (2023. p. 237) afirma: "*un elemento central de esta interacción es la selección de información y su comunicación oportuna entre la policía, la fiscalía y la defensa*". Pero estas cuestiones se vuelven dificultosas cuando no se tiene conocimientos mínimos en tecnología. Esto puede resultar en la falta de comunicación efectiva y en la duplicación de esfuerzos, lo que afecta la eficiencia global de la investigación.

Se produce una dinámica muy particular: si se tiene poca información sobre el hecho que se está investigando, difícilmente se podrá aplicar una estrategia adecuada para el relevamiento y la recolección. Por su parte, si se tiene poca información y además poca instrucción en cuestiones tecnológicas, difícilmente se podrá reconocer qué potenciales elementos de prueba (además de los convencionales) puedan permitir obtener información sobre las circunstancias del

[14] Estos sesgos podrían producirse por la falta de información, conocimiento u objetividad. Duce (2022, p. 79) indica que: "Los sesgos cognitivos son errores sistemáticos en el razonamiento que tienen lugar cuando los seres humanos procesamos e interpretamos información y, por supuesto, las decisiones y conclusiones que tomamos se ven afectadas por ello". La manipulación sesgada de indicios y la elección tendenciosa de premisas para respaldar una hipótesis defensiva o acusatoria generan un efecto antiepistémico al distorsionar y manipular los vestigios del delito (Borrás Andrés, 2023, p. 195). En este caso particular, por ejemplo, podría producirse un sesgo de confirmación al buscar evidencia que respalde una hipótesis en lugar de considerar pruebas que puedan contradecirla, o un sesgo de contexto cuando se expone a los investigadores a datos contextuales que, aunque pertinentes para la situación, no son necesarios para sus funciones (Vázquez, 2023, p. 31).

hecho. La falta de información típica, sumada a la falta de conocimiento en cuestiones tecnológicas, puede ocasionar que los investigadores judiciales, tienden a confiar en demasía en los operadores forenses o primeras personas interventoras. Este exceso de confianza en las prácticas, específicamente en las actividades de relevamiento y recolección de potenciales elementos de prueba, no permitiría que se tenga un control intersubjetivo adecuado.

C. La protección de los Derechos fundamentales

Finalmente, en lo que respecta a las cuestiones que surgen ante la escasez de información y considerando las actividades de relevamiento y recolección, podemos señalar la problemática en relación con la protección de los derechos fundamentales.

En este sentido, nos centraremos brevemente en un desafío que consideramos evidente en el contexto del presente trabajo: la vulneración del derecho a la intimidad.[15]La falta de información precisa, sobre lo que se busca, sumado a la falta de control que se tiene sobre ello, puede dar como resultado que potencialmente los derechos fundamentales y, específicamente, el derecho a la intimidad, sean vulnerados. Estas situaciones se dan, por ejemplo, cuando por falta de información característica de los primeros momentos de la investigación, y ante la imposibilidad de buscar información precisa, las personas investigadoras obtienen información de la esfera íntima de la persona irrelevante para la causa,[16] pero que es captada de igual forma por el efecto red de pesca.[17]

Esta problemática ya era avizorada años atrás. En el año 2001, el Consejo de Europa, durante su reunión en Budapest, firmó el Convenio sobre Ciberdelincuencia. En su preámbulo, destacó la necesidad de respetar los derechos humanos reconocidos por varios tratados internacionales, incluyendo explícitamente la privacidad de todas las personas y la protección de sus datos personales y comunicaciones. Demandando un "*equilibrio adecuado*" entre ellos. (Bernard, 2021, p. 40).

Específicamente, nos referimos en este caso a aquellas situaciones donde en los primeros momentos de la investigación se relevan dispositivos o fuentes de información digital, que además de la información autorizada a buscar, se obtiene otro tipo de información sensible sobre la vida del individuo o también información considerada neutral.[18]

La característica propia de la era digital trae aparejada esta problemática que debe ser tenida en cuenta para no vulnerar los derechos fundamentales. Teniendo en cuenta que tienen la capacidad de poner en riesgo seriamente la privacidad de los individuos, dado que significa que una gran cantidad de datos personales estará accesible para las autoridades y las fuerzas de seguridad, (Ferreyra, 2018, p. 9) y los cuestionamientos que puedan surgir con relación al uso inadecuado de dicha información.

Es importante recordar que una computadora o un teléfono celular no constituyen evidencia en sí mismos, sino que son dispositivos de almacenamiento. La verdadera evidencia digital reside en los datos contenidos dentro de estos dispositivos. Esta distinción plantea dificultades al tratar de aplicar las mismas reglas a la evidencia física y digital por analogía, lo que puede resultar en la violación de las garantías constitucionales de los ciudadanos. (Suarez, 2021, p. 4)

Considerando, que no todos los datos personales son sensibles y cualquier petición de información no necesariamente vulnera derechos constitucionales, existen diversos niveles de impacto, desde una intrusión mínima hasta una más significativa, y su admisión está condicionada al cumplimiento de ciertos requisitos. (Bernard, 2021, p.52). Sin embargo, resulta importante poder remarcar la potencial vulneración de derechos fundamentales en estas situaciones particulares cuando se investiga en entornos digitales.[19]

Tal vez, el problema central radica en no tener la notable distinción entre la evidencia física y la evidencia digital, y que ello tiene un impacto directo tanto en la forma en que se llevan a cabo las medidas de investigación como en las garantías constitucionales de los ciudadanos (Suarez, 2021, p. 3). En ese sentido, se requiere reconsiderar y reexaminar los conceptos legales convencionales y considerar las nuevas formas y usos de los derechos constitucionales tradicionales, establecidos en

[15] El derecho a la intimidad comprende el conjunto de actividades que forman un círculo íntimo, personal y familiar, facultando a todo individuo a excluir a los extraños de entrometerse en él, evitando así una publicidad que no desea el interesado. Se encuentra relacionado con el derecho al honor, a la propia imagen y a la protección de datos, todos derechos personalísimos y protegidos en la gran mayoría de las constituciones estatales. (Becerra; Zarate, 2015, p. 2018). Para Merkel (2022, p. 255) "cuenta con dos componentes: uno positivo, que consiste en el derecho a ejercer el control sobre nuestros datos y la información que queremos compartir con los demás, y uno negativo, que consiste en el derecho a no ser importunado por nadie y a poder excluir a los demás de nuestra esfera privada."

[16] "Se advierte que, con facilidad, se puede vulnerar la privacidad de las personas investigadas si se realizan pedidos de información indiscriminados, en base a sospechas fundadas en datos sensibles como orientación política, religión, raza, etc., que podrían conducir incluso a prácticas que atenten contra el derecho a la igualdad y el ámbito de reserva de cada ciudadano." (Bernard, 2021, p. 42)

[17] El término «efecto red de pesca» lo utilizamos en este sentido para describir una práctica en la que los investigadores, en un intento de obtener información relevante para una investigación criminal, recopilan datos de manera indiscriminada y extensiva, ya sea por la falta de información o con la esperanza de atrapar cualquier información potencialmente útil. Este enfoque a menudo se asocia con la obtención de información masiva, incluida la que no está directamente relacionada con la causa que se investiga

[18] Como información neutral queremos significar aquella que no ofrece inconvenientes, salvo que se almacenen junto a otros o se crucen.

[19] Como ejemplo ilustrativo de la problemática, se puede mencionar el caso Estados Unidos vs. Walser. Durante una investigación relacionada con la venta de drogas, una oficial de policía entró en contacto con una computadora portátil propiedad de Walser. Después de varias horas de búsqueda, encontró material visual relacionado con pornografía infantil, lo que llevó a su acusación por posesión de dicho material, a lo que se declaró culpable. Posteriormente, Walser solicitó al Tribunal de Distrito que excluyera las pruebas obtenidas durante el registro de su computadora personal, argumentando que la oficial había excedido el alcance de la orden al abrir un archivo de video que no guardaba relación con la investigación. Se argumentó que los archivos apropiados para la búsqueda serían aquellos de texto o planillas. Este caso se puede consultar en el siguiente enlace:https://caselaw.findlaw.com/court/us-10th-circuit/1004455.html

un contexto completamente diferente al presente (Merkel, 2022, p. 15).

III. El desborde de información digital en la fase de investigación.

Sumado a la problemática de la falta de información cuando se investiga en entornos digitales encontramos los inconvenientes relacionados con la cantidad de información generada en esta instancia. Para comprender mejor la problemática, podemos considerar algunos datos de referencia. Por ejemplo, los informes de análisis de dispositivos con posible evidencia digital suelen entregarse en formato PDF por parte de las áreas de investigación. Un teléfono de 8 GB produce un informe de aproximadamente 10.000 páginas, uno de 32 GB de 40.000 páginas, y uno de 128/256 GB de 100.000 páginas. Aunque estos números no son impactantes en sí mismos, pueden resultar abrumadores al analizarlos en un caso específico.

Los investigadores de hechos criminales tienen acceso a una amplia gama de dispositivos, y las capacidades de almacenamiento de los mismos están en constante aumento. Además, se pueden agregar los datos proporcionados por las empresas tecnológicas y los provenientes de fuentes de acceso público (Di lorio, 2017, p. 554). En este apartado, nos referiremos a dos aspectos relacionados con el efecto desborde que se produce en la investigación en entornos digitales y que resulta interesante tener en cuenta en el contexto del impacto que puede producir en la actividad probatoria: a) la multiplicidad de las fuentes, y b) el riesgo de pérdida de información relevante.

a) En relación al primer aspecto, consideramos que requiere fundamental reflexión cuando nos referimos al desborde de información digital, por el impacto que puede producir cuando se está investigando en entornos digitales. Con la creciente digitalización de la sociedad, el universo de fuentes de información disponibles para las investigaciones criminales ha experimentado un crecimiento exponencial.

Las opciones de búsqueda de información son variadas y heterogéneas y las fuentes de datos pueden ser muy diversas. (Di lorio, 2017, p. 68). En ese sentido, podemos destacar dos aspectos, uno positivo y otro negativo. El aspecto positivo se refiere a la mayor posibilidad que trae aparejado la inclusión de fuentes que antes no existían. El aspecto negativo, y que representa realmente un gran desafío en la actualidad, consiste en la problemática de la diversidad de dispositivos clásicos y no tan clásicos que podrían contener información de interés para la investigación, sumado a la caudalosa información que es aportada por los mismos.

. En referencia a ese asunto, a nivel de la práctica investigativa, frecuentemente se solicita a los investigadores la obtención de diversas fuentes que potencialmente puedan contener evidencia digital, indicando que se extraiga del dispositivo información relevante para la causa sin especificar un criterio determinado.

Esta dinámica trae varias problemáticas en el contexto de la investigación criminal, como son: falta de claridad en los criterios de relevancia, pérdida de datos potencialmente importantes (cuestión que trataremos en el siguiente punto) y potencialmente, la vulneración de derechos fundamentales como vimos anteriormente. El desafío surge al considerar que una fuente de evidencia digital produce una gran cantidad de datos. Si esto se extiende a varias fuentes, la cantidad de datos aumenta considerablemente, lo que podría dificultar su análisis adecuado debido a la limitación de tiempo durante la investigación y a la frecuente escasez de recursos materiales y financieros.

Frente a esta situación, el sistema de justicia suele reaccionar de la siguiente manera: a mayor cantidad de fuentes de evidencia digital, menor capacidad de análisis de los datos. La multiplicidad de fuentes presenta desafíos en la investigación, especialmente en los primeros momentos. A corto plazo, no parece haber una mejora en esta situación debido a la creciente dependencia de dispositivos electrónicos en la sociedad.

Aunque esta tendencia podría ofrecer más información para las investigaciones, también conlleva desafíos adicionales, como la selección de fuentes pertinentes y el manejo de grandes cantidades de datos en fases posteriores. Este riesgo se agrava aún más por la naturaleza cambiante y en constante evolución de la tecnología (Wilson-Kovacs et al., 2023, p. 250) b) En relación al segundo aspecto, la sobreabundancia de información digital presenta un riesgo significativo para la investigación en entornos donde se gestiona gran cantidad de datos. Este exceso de información puede dificultar la identificación de los elementos cruciales, además, puede llevar a la pérdida de tiempo y recursos al tener que revisar una cantidad considerable de datos, muchos de los cuales pueden resultar irrelevantes.

Lo interesante sería preguntarnos, ¿con qué criterios se establece la relevancia de una determinada fuente de información digital en los primeros momentos de la investigación? Si recurrimos al criterio de relevancia señalado por la norma ISO/IEC: 27037:2012, se indica un aspecto técnicamente jurídico que se refiere a los elementos pertinentes a la situación en cuestión, destinados a demostrar o refutar una hipótesis planteada sobre los hechos. Todo aquello que no satisfaga este criterio será considerado como irrelevante y no será tomado en cuenta como evidencia en el caso que se está analizando (Semprini, 2017, p. 92), Esto no lleva a inferir que el criterio de relevancia digital deviene del criterio de relevancia o pertinencia de todo contexto epistemológico. Pero evidentemente, se constata una carencia de pautas racionalmente acordes a la complejidad de investigar en estos entornos. Lo anteriormente expuesto se verifica en la práctica. A veces se opta por secuestrar la mayor cantidad de fuentes, otras veces las “más significativas”.

Ahora bien, este último punto podría ocasionar problemas considerables para determinar cuál es la prueba relevante. Partiendo de la idea de que existen casos en los que ni siquiera se sabe si se cometió un delito, es decir, no se tiene claridad en estos primeros momentos de la investigación si el hecho constituye un ilícito. O, por otro lado, existen casos en los que se sabe que se cometió un delito, pero no se conoce cuál fue el delito específico ni los detalles del caso. ¿Cuál sería entonces el objeto de prueba a relevar o adquirir? ¿Cómo se podría garantizar que no se pierda la información relevante?

Teniendo en cuenta que «*la atención en la racionalidad de la valoración de la prueba tiene sus raíces en la asunción de que ésta es la mejor garantía de la mayor aproximación entre lo que resulta probado en el procedimiento y la verdad sobre los hechos*» (Vázquez, 2015, p. 102), resulta indispensable considerar en los momentos iniciales de la investigación, donde los elementos probatorios comienzan a conformarse, la multiplicidad de las fuentes, el escaso control intersubjetivo y la pérdida de información relevante son aspectos que deben ser tenidos en cuenta para lograr un razonamiento adecuado.

IV. La tensión entre la poca información en los primeros momentos de la investigación y la sobreabundancia de información digital. Su impacto en el debido proceso.

La escasez informativa y la sobreabundancia de información parecieran ser una contradicción paradójica. Sin embargo, forman parte de la realidad compleja que implica investigar en contextos actuales, donde los diferentes dispositivos, fuentes de información digital, son fundamentales para aproximarse a la verdad sobre los hechos.

A continuación, describiremos brevemente dos puntos de contacto donde se produce dicha tensión en la investigación criminal y sus implicancias en el debido proceso.

a) La tensión entre la recolección indiscriminada de información y la vulneración de los derechos fundamentales. Como pudimos constatar, una de las cuestiones que surgen debido a la escasa y abundante información, cuando se investigan en estos entornos, es lo referido a la potencial vulneración de garantías constitucionales. En este sentido, se intensifica la continua tensión entre el interés por la persecución de los crímenes y el respeto por las libertades de los individuos. (Merkel, 2022, p. 47).

Debido a la falta de regulación específica sobre la evidencia digital en nuestros sistemas procesales, se revivió esta tensión entre la necesidad de investigar por parte del Estado y el derecho de los ciudadanos. Agregando otras aristas a debatir, cómo la diferencia entre el tratamiento de la evidencia física, la digital y su uso como prueba en el proceso.

. La discusión no es nueva; dicha tensión es un tema bastante tratado en el ámbito probatorio.[20] Sin embargo, la cuestión digital la intensifica, debido a las características propias de este tipo de evidencia, las nuevas tecnologías, y las diferencias que se plantean con la evidencia material. En esa misma línea de ideas, Dupuy (2021, p. 272) considera que "*el derecho penal y procesal clásicos se han construido sobre un modelo de delincuencia física e individual*."

Teniendo en cuenta esa consideración, la dinámica entre la necesidad de investigar y la protección de los derechos de los individuos debe evolucionar y actualizarse mediante discusiones actuales. Si consideramos un ejemplo actual y muy habitual, como lo es, el acceso del Estado al teléfono inteligente de un individuo sospechoso de haber cometido un delito, implica una intromisión mucho más invasiva que la que se produce con un registro domiciliario o una requisa personal en la vía pública.[21] En consecuencia, dado el mayor impacto en la garantía constitucional, parece razonable que existan mayores controles para permitir tal intromisión, a pesar de que esto no esté específicamente contemplado en ninguna cláusula constitucional o convencional. (Lanzón, 2023, p. 114).

Sin duda, la falta de regulación en la temática, junto a actividades de búsqueda basadas en la experiencia o en la intuición podrían provocar una recolección indiscriminada de información y, con ello, la obtención de gran cantidad de datos que dudosamente podría ser procesado racionalmente respetando, por ejemplo, la intimidad de las personas.

Teniendo en cuenta que el cuidado de los derechos fundamentales de las personas acusadas es un requisito riguroso para un debido proceso enmarcado en las constituciones y tratados internacionales, resulta imprescindible considerarlo al investigar en entornos digitales.

b) La tensión entre la escasez de información que tiene como efecto la adquisición indiscriminada de datos, versus la abrumadora cantidad de datos y su impacto en el derecho de defensa. De la misma forma en que para la fiscalía es dificultoso poder analizar la inmensa cantidad de información relevante e irrelevante que se obtiene de la investigación en entornos digitales, para la defensa lo es aún más, principalmente, porque no hay paridad de armas.

Considerando la interpretación de Maier (1999, p. 577) sobre el derecho de defensa, implicando la capacidad de probar y controlar la prueba para garantizar la igualdad de posiciones, surgen varias problemáticas en este sentido. La primera de ellas se refiere al escaso control que puede ejercer la defensa ante las

[20] Como ejemplo, podemos señalar las discusiones en relación al uso de tecnologías de vigilancia masiva mediante reconocimiento facial, en relación al derecho a la privacidad, la interceptación de las comunicaciones, etc.

[21] En este caso, Lanzón (2023, pp.119) considera la marcada diferencia entre los datos obtenidos en un registro virtual (por ejemplo, un teléfono móvil) en relación con el físico (allanamiento de morada). En el primero se obtiene una inmensidad de datos relacionados con toda la esfera del individuo, inclusive relaciones con otras personas, etc. En la física, el límite es más claro y restringido.

actividades intuitivas, fundamentadas desde la experiencia y realizadas en las fases de relevamiento y recolección, por parte de los investigadores en los primeros momentos de la investigación.[22]

Como mencionamos, la falta de regulación en la temática dio lugar a normas técnicas diversas y no vinculantes, que muchas veces imposibilitan que la defensa pueda esgrimir algún cuestionamiento sobre los procedimientos llevados a cabo en el lugar del hecho. Y en el caso de hacerlo y utilizar normas técnicas, como por ejemplo las normas ISO, dichos planteos pueden no ser considerados si el juez así lo determina, debido a la falta de carácter vinculante.[23]

También deberíamos sumar a esa cuestión que dichas normas no son de acceso público, es decir, requieren una suscripción para poder entrar en contacto con tales recomendaciones. Por otro lado, podemos advertir que, ante la inmensidad de datos proporcionados por la multiplicidad de fuentes provenientes de entornos digitales, en la práctica judicial es muy habitual que la fiscalía presente un extracto de la información considerada relevante, es decir, datos filtrados de acuerdo con el supuesto interés de la investigación. Wilson-Kovacs et al., (2023, p. 245) se refiere a ello cuando indica que debido a la abundancia de información disponible no se exhiben todos los datos en su totalidad, sino más bien una síntesis del análisis del dispositivo.

Dado que los equipos de defensa suelen recibir informes adaptados (como documentos PDF u hojas de cálculo de Excel) en lugar de datos en bruto y archivos de casos generados durante las fases iniciales de una investigación. La claridad y la transparencia cobran una relevancia particular cuando se tiene que ejercer una adecuada defensa.

Aun en el mejor de los casos, la información aportada por el entorno digital es tan abundante que, si la fiscalía proporcionara datos sin procesar, la defensa se encontraría con una gran cantidad de información, parte de la cual puede resultar irrelevante. Revisar exhaustivamente todo el contenido del dispositivo puede ser un desafío considerable y consumir una cantidad de tiempo muy notable (Wilson-Kovacs et al., 2023, p. 245).

Estos aspectos en tensión, deben ponerse en contexto con realidades que, usualmente, se manifiestan desde la práctica de la defensa y que no deben pasarse por alto como: la desigualdad de armas en relación con los recursos tecnológicos para analizar las fuentes de evidencia digital, en comparación con los recursos del Ministerio Público Fiscal.

V. CONCLUSIONES Y ALGUNAS PROPUESTAS PARA ABORDAR LOS DESAFÍOS IDENTIFICADOS.

Como pudimos constatar, la tensión entre la escasez y la sobreabundancia de información cuando se investiga en entornos digitales tiene implicancias significativas para el debido proceso, por eso es necesario poder abordarlos desde diferentes perspectivas, porque indudablemente si los problemas son complejos el abordaje debería ser lo más integral posible. En este último apartado, y a modo de conclusión, veremos algunas propuestas que, si bien seguramente no serán las únicas, pueden ser útiles para ampliar la discusión y contribuir a una mejora en el sistema de justicia.

Un aspecto que consideramos transversal a las problemáticas descritas se relaciona con la alfabetización digital y la necesidad de una cultura forense digital en el sistema. En ese sentido, nos referimos a la necesidad de adquirir conocimientos y habilidades adecuadas para los procesos de investigación actuales. No es suficiente proporcionar simplemente herramientas tecnológicas a los sujetos que integran el sistema de justicia, ya que la alfabetización digital no se desarrollaría automáticamente como un efecto de osmosis.[24] Sino más bien, la adquisición de tecnología debería implicar también un programa formativo que permita crear habilidades, destrezas y una visión crítica de la información obtenida por esos medios.

El primer paso podría ser el más obvio: ser conscientes de que el sistema de justicia requiere una reflexión en este sentido y que los integrantes del sistema, en su mayoría, necesitan adquirir conocimientos tecnológicos para realizar procedimientos racionales acordes a un debido proceso.[25]

El asunto de la formación tiene un rol fundamental y empezó a ser muy debatido en el ámbito doctrinario. Por ejemplo, Marina Gascón (2016, p.365) se refiere a la educación de los jueces, pero perfectamente aplicable a otros sujetos que conforman el

[22] A eso deberíamos sumarle la actitud acrítica de las hipótesis policiales (Borrás Andrés, 2023, p. 231). Nieva Fenoll (2021, pp. 491-492) al criticar el sistema acusatorio advierte sobre esta situación, manifestando: "según el sistema, quienes recogieran el cuerpo del delito de la escena de un crimen, por ejemplo, lo que es absolutamente obvio que no es así. Incluso en los casos en que no hay nada que recoger al no implicar el delito la sangre de nadie, jueces y fiscales tienen la demasiado frecuente costumbre de encargar informes policiales en algunos delitos económicos o de otra índole que no dejan de ser forzados, al no tener la policía preparación para tales investigaciones que implican complejas operaciones económicas, societarias, urbanísticas o administrativas en general."

[23] Sobre la cuestión de los protocolos y la utilización por parte de la defensa, Merkel (2022, p. 215) considera que la jurisprudencia debe definir claramente las implicaciones del incumplimiento de los protocolos. Sin embargo, la falta de uniformidad en dichos protocolos resulta en una posición difusa, especialmente en lo que respecta a las consecuencias legales de su violación. La jurisprudencia, siguiendo el principio de legalidad, tiende a ser cautelosa al rechazar pruebas en estos casos, prefiriendo abordar la resolución del problema en el ámbito de la evaluación de la evidencia.

[24] "Podría pensarse que con el solo hecho de situarnos en un ecosistema de digitalidad nos encontramos permeados por algún tipo de pedagogía digital, como si este proceso se agotara sólo a través del acceso y el manejo de tecnologías digitales. Esta creencia se ve impulsada por la presencia de una ingeniería legal aparentemente eficiente (al menos como diseño enunciativo), pero vivir en una sociedad soportada por tecnologías digitales, cuya dinámica se define por sistemas informativos, no presupone una comprensión de los efectos de esta cultura, y lo determinante que se han vuelto estas herramientas para las capacidades cognoscitivas." (Morán Reyes, 2022, p. 195)

[25] Como conocimientos tecnológicos nos referimos a: nociones sobre tipos de dispositivos, sistemas de almacenamiento de datos, sistemas de comunicación, redes sociales, perfiles, cuentas, registros de conexión, etc.

sistema de justicia. En ese sentido, la pregunta que surge es la siguiente: ¿Qué conocimientos deberían ser considerados básicos? La autora propone instruir en cuestiones básicas como método científico, estadística, etc., y en cuestiones elementales de las disciplinas forenses más requeridas, teniendo en cuenta que hay gran diversidad de temáticas. Sin lugar a dudas los conocimientos tecnológicos se presentan como un contenido necesario para las investigaciones actuales y que ningún sujeto que integre el sistema de justicia en la actualidad podría realizar su actividad de manera eficiente (de defensa, investigación, acusación, y juzgamiento) sin contar con herramientas que provengan de la cultura digital.

Con respecto a lo anterior, desde la práctica, hace algún tiempo se comenzó a observar la creación de fiscalías especializadas con el propósito de enfrentar las diversas dificultades asociadas con la investigación en estos entornos. La falta de conocimiento forense digital en el sistema de justicia ha llevado a la formación de unidades especiales, como las dedicadas al cibercrimen. Estas fiscalías si bien constituyeron un gran paso para el momento, hoy por hoy, pensar que los hechos que investigamos donde también buscamos evidencia digital son especiales, podría ser un error. La investigación en entornos digitales pasó a ser la regla y no la excepción.[26]

Según Dupuy (2021, p. 282), los delitos informáticos no constituyen un conjunto definido, lo que implica que la recolección de pruebas no se limita únicamente a los delitos tipificados en la ley 26.388.73 Para investigar es necesario contar con pruebas electrónicas que respalden algún aspecto de la teoría del caso tanto del fiscal como de la defensa, o para complementar la evidencia obtenida de fuentes físicas. Como vimos, el problema no les compete solo a los juristas.

Las áreas investigativas, policiales, la defensa e inclusive los científicos forenses requieren de un progresivo avance de su cultura digital. Cultura que implica, como dijimos anteriormente, la adquisición de conocimientos, habilidades, destrezas en procesos racionales que generen una postura epistémica adecuada frente a la información proporcionada por los medios tecnológicos.

Consideramos en ese sentido que investigar en entornos digitales, hoy en día, no debe ser una especialidad, debe formar parte de un conocimiento general. Al ser un tema complejo dijimos que las soluciones deben ir de la mano con otras acciones necesarias, como una mayor regulación en la gestión de la evidencia digital. Aquí reside nuestro segundo aspecto considerado transversal, lo referido a la necesidad de una regulación específica en pruebas digitales.[27]

Esta cuestión, sin duda, creemos que es la más compleja de abordar porque depende de varios factores por tratarse de una política pública. Frente a la necesidad de regulación, una experiencia a destacar, independientemente de lo referido sobre las normas técnicas que indican procedimientos para el tratamiento de la evidencia digital (normas ISO), se constata en el Consejo de Europa.[28]

Uno de los documentos, EEG, por ejemplo, está orientado (a diferencia de las ISO) a servir como un punto inicial para que los legisladores desarrollen reglamentos específicos sobre el tratamiento de la evidencia digital acordes a un debido proceso.

Por su parte, la guía de ENISA se centra en los requisitos formativos que deben cumplir los primeros interventores en investigaciones en entornos digitales. Por último, las directrices de la OLAF (2016) profundizan en una cuestión muy relevante a la luz de las problemáticas abordadas en el presente trabajo, proponiendo etapas intermedias que actúen como filtros. Esto podría ayudar a enfrentar la problemática de la multiplicidad de fuentes y la abrumadora cantidad de información que, potencialmente, podría afectar los Derechos Fundamentales

En conclusión, los primeros momentos de la investigación demandan un mayor debate y reflexión. Es crucial un razonamiento probatorio sólido en estas etapas iniciales para establecer un marco acorde con el debido proceso. Esto podría ayudar a prevenir el tratamiento inadecuado de la información obtenida de los entornos digitales, mejorar su calidad epistémica y salvaguardar los Derechos Fundamentales. Una regulación adecuada en el tratamiento de la evidencia digital proporcionaría directrices (actualmente muy escasas) para los integrantes del sistema de justicia, lo que permitiría un mayor control de los procesos de relevamiento y adquisición, así como en las fases subsiguientes, asegurando un abordaje adecuado en los primeros momentos de la investigación. Además, promover una mayor alfabetización digital en el sistema de justicia colaboraría en la reducción de actividades intuitivas, facilitando un tratamiento más racional y, por ende, con mayor control intersubjetivo de los elementos probatorios provenientes de estos entornos.

[26] 2 Lanzón (2023, p. 124) se manifiesta en esa dirección, afirmando que la situación actual requiere no solamente la creación de unidades especializadas y organismos de apoyo con conocimientos técnicos para abordar los desafíos mencionados. Además, es necesario implementar programas de formación para todo el personal del sistema penal. Es preocupante que las facultades de derecho no estén respondiendo a esta realidad ajustando sus planes de estudio para incluir el estudio de las implicaciones técnicas y jurídicas de la evidencia digital, como destacan expertos en la materia. En Argentina por ejemplo hace unos años se crearon: Unidad Fiscal Especializada en Ciberdelincuencia (UFECI, 2015, MPF de la Nación), Fiscalía especializada en cibercrimen (2018, MPF Córdoba) destinados a abordar delitos específicos como, aquellos casos en los cuales el sistema informático haya sido el objeto del delito o haya sido el medio principal o accesorio para cometerlo. https://www.mpf.gob.ar/ufeci/

[27] Dupuy (2021, p. 283) afirma en este contexto, que existe una carencia de normas procesales penales para investigaciones 4.0. Con ello se refiere a que, la evolución en las formas delictivas subraya la importancia de contar con marcos legales que permitan aprovechar el potencial de la tecnología para llevar a cabo investigaciones criminales efectivas, al mismo tiempo que se garantizan los derechos fundamentales de las personas, según lo establecido en la constitución.

[28] En ese sentido, nos referimos a: La Guía para Policías Fiscales y Jueces EEG (2014); Guía básica para primeros intervinientes ENISA (2015) y las directrices sobre procedimientos forenses digitales para el personal de la OLAF (2016).

REFERENCIAS

[1] K. Abimbola, "Abductive Reasoning in Law: Taxonomy and Inference to the Best Explanation," in M. Maccrimmon and P. Tillers (Eds.), The Dynamics of Judicial Proof: Computation, Logic and Common Sense, Physica-Verlag Heidelberg, 2002.

[2] T. Anderson, D. Shum, and W. Twining, Análisis de la prueba, Marcial Pons, 2015.

[3] N. Borrás Andrés, La instrucción sin perjuicios. La necesaria limitación a la recogida de vestigios, Marcial Pons, 2023.

[4] A. Binder, Introducción al Derecho Procesal Penal, AD-HOC, 1999.

[5] J. Collie, "Digital forensic evidence—Flaws in the criminal justice system," Forensic Science International, vol. 289, pp. 154-155, 2018.

[6] Convenio sobre ciberdelincuencia, Budapest, 2001.

[7] A. Di Iorio, M. Castellote, B. Constanzo, y H. Curti, "El rastro digital del delito: Aspectos técnicos, legales y estratégicos de la informática forense," UFASTA, 2017.

[8] M. Duce, Las comunidades expertas y los sesgos cognitivos de los peritos. Manual de prueba pericial, Escuela Federal de Formación Judicial. Consejo de la Judicatura Federal, 2022.

[9] Dupuy, Tratado de la prueba electrónica. Tomo III, La Ley, 2021.

[10] European Anti-Fraud Office, "Guidelines on Digital Forensic Procedures for OLAF Staff," 2016.

[11] I. Fahsing, "The making of an expert detective. Thinking and Deciding Criminal Investigations," 2016.

[12] J. Ferrer Beltrán, Del Derecho al razonamiento probatorio, Marcial Pons, 2020.

[13] J. Ferrer Beltrán, Prueba sin convicción. Estándares de prueba y debido proceso, Marcial Pons, 2021.

[14] E. Ferreyra, "La Convención de cibercrimen de Budapest y América Latina. Breve guía acerca de su impacto en los derechos y garantías de las personas," Asociación por los Derechos Civiles, no. 1, 2018.

[15] E. Haba, "Racionalidad y método para el Derecho: ¿Es eso posible?," DOXA. Cuadernos de filosofía del Derecho, no. 07, pp. 169-247, 1990.

[16] S. Haack, "Esperando una respuesta: El desordenado proceso de buscar la verdad," trad. E. Otero B., en Ciencia, Sociedad y Cultura, Ensayos Escogidos, Universidad Diego Portales, republicado en Cuadernos de neuropsicología, vol. 3, pp. 12-23, 2009.

[17] S. Haack, "The Expert Witness: Lessons from the U.S. Experience," Humana Mente: Journal of Philosophical Studies, vol. 28, pp. 39-70, 2015.

[18] R. Lanzón, "La búsqueda de evidencias en los dispositivos de almacenamiento digital: Alcances y límites al análisis forense en el marco del procedimiento penal," Revista de Derecho Penal y Criminología, vol. 2, pp. 107-125, 2023.

[19] C. López, "Evidencias electrónicas," TFM, Máster Universitario en Seguridad de las Tecnologías de la Información y de las Telecomunicaciones, Universidad Oberta de Catalunya, 2019.

[20] L. Merkel, "Derechos Humanos e investigaciones policiales: Una tensión constante," Marcial Pons, 2022.

[21] L. Moscatelli, "La importancia de la abducción en la etapa de investigación criminal," Quaestio Facti. Revista Internacional Sobre Razonamiento Probatorio, vol. 5, pp. 125-155, 2023.

[22] J. Nieva Fenoll, "La decadencia del sistema penal acusatorio," Revista Vasca de Derecho Procesal y Arbitraje, vol. 33, pp. 489-500, 2021.

[23] NRC, Strengthening Forensic Science in the United States: A Path Forward, 2009.

[24] Protocolo para la identificación, recolección, preservación, procesamiento y presentación de evidencia digital, Ministerio de Seguridad de la República Argentina, 2023.

[25] G. Semprini, "El análisis integral de la evidencia digital," en Simposio Argentino de Informática y Derecho, Río Negro, 2017.

[26] M. Suarez, "Vulneración de las Garantías Constitucionales en la Investigación en entornos digitales," Revista Pensamiento Penal, vol. 401, pp. 1-30, 2021.

[27] G. Tuzet, Filosofía de la prueba jurídica, traducción de D. Dei Vecchi, Marcial Pons, 2021.

[28] C. Vázquez, "La admisibilidad de las pruebas periciales y la racionalidad de las decisiones judiciales," DOXA, Cuadernos de Filosofía del Derecho, vol. 38, pp. 101-130, 2015.

[29] C. Vázquez, Guía sobre el contenido de los informes periciales y su impacto en el debido proceso, Escuela Federal de Formación Judicial, Consejo de la Judicatura Federal, 2023.

[30] D. Wilson-Kovacs, R. Helm, B. Growns, y L. Redfern, "Digital evidence in defence practice: Prevalence, challenges and expertise," The International Journal of Evidence & Proof, vol. 23, pp. 235-253, 2023.

Guía para la adquisición, preservación y presentación de la evidencia digital: experiencias de su desarrollo y validación

M. Fernanda Rosales, María Belén Álvarez Cestona, Bruno Constanzo, Ana Haydée Di Iorio, Marisa Repetto
Universidad FASTA – Universidad de Champagnat

***Resumen*— En este trabajo se presenta la Guía de Actuación para la Adquisición, Preservación y Presentación de la Prueba Digital que tiene como finalidad la definición de un conjunto de buenas prácticas de extracción, adquisición, preservación y presentación de prueba digital, a fin de dar validez a la evidencia digital en los procesos judiciales civiles y comerciales, laborales y de familia. Se constituye en una solución para los abogados, escribanos, peritos informáticos, justiciables y ciudadanos en general. Esto fue posible gracias a la asociación y trabajo conjunto entre la Universidad FASTA, la Universidad Champagnat, la Ju.Fe.Jus - Junta Federal de Cortes y Superiores Tribunales de Justicia de las provincias argentinas y Ciudad Autónoma de Buenos Aires.**

I. Introducción

La evidencia digital ha emergido como un componente central en las investigaciones judiciales. Esta evidencia incluye cualquier tipo de información almacenada o transmitida electrónicamente. Con el uso creciente de dispositivos electrónicos en casi todas las actividades humanas, la cantidad de evidencia digital generada ha aumentado exponencialmente. Sumado a la información que obtenemos de correos electrónicos, servicios de mensajería, documentos digitales, datos de redes sociales y contenidos de páginas web, se ha visto una proliferación de dispositivos conectados a internet, como teléfonos inteligentes, asistentes virtuales, wearables y electrodomésticos inteligentes (IoT), que generan una cantidad masiva de datos.

La adopción generalizada de tecnologías digitales ha incrementado la creación de datos, transformando la naturaleza y el volumen de la evidencia disponible para fines legales. Preservar la evidencia digital bajo los principios forenses adecuados es esencial para garantizar su integridad y validez. La preservación implica no solo el almacenamiento seguro de los datos, sino también la aplicación de métodos que aseguren que la información no sea alterada o manipulada después de su adquisición. La correcta aplicación de estos métodos es fundamental para asegurar que la evidencia digital sea admisible en un proceso judicial y mantenga su valor probatorio.

La preservación de la evidencia digital es un gran desafío debido a la naturaleza volátil de los datos digitales lo que implica que deba ser adquirida y preservada de manera urgente y válida.

En causas penales, donde los que se dedican a trabajar con la evidencia digital, son los forenses informáticos, ya existen guías que abarcan temas desde cómo trabajar con la evidencia digital (desde la recolección hasta en análisis) hasta cómo generar ámbitos de trabajo adecuados en laboratorios.

Para causas no penales los ciudadanos, dueños de esa evidencia digital, muchas veces no cuentan con los recursos culturales, educativos, o con la posibilidad económica para contratar a un perito informático que realice el proceso de adquisición y preservación. Estas situaciones llevan a que sea el mismo abogado, escribano, o incluso el ciudadano, quien finalmente se encarga de estos procedimientos.

Con el fin de atender a esta necesidad es que la Junta Federal de Cortes y Superiores Tribunales de Justicia de las Provincias Argentinas y la Ciudad Autónoma de Buenos Aires -Ju.Fe.Jus- impulsó el desarrollo de la Guía de actuación para la Adquisición, Preservación y Presentación de la Prueba Digital para fueros no penales, que se implementó entre el InFo-Lab, Laboratorio de Investigación de Desarrollo de Tecnología en Informática Forense de Universidad FASTA y la Universidad Champagnat.

II. Desarrollo de la Guía

En el año 2022 se comenzó el desarrollo de la Guía. A mediados de 2023, al concluir el primer año del proyecto de investigación, se creó la primera edición de la Guía en formato digital PDF, con ISBN 978-631-90168-3-3. En agosto de 2024 se llegó a la Versión Final, encontrándose próxima a ser registrada y publicada.

Fue desarrollada por un equipo interdisciplinario de investigadores, conformado por abogados, ingenieros informáticos, fiscales y magistrados, pertenecientes al InFo-Lab, de la Facultad de Ingeniería y la Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA (Mar del Plata) y de la Facultad de Derecho de la Universidad Champagnat (Mendoza). El equipo trabajó de forma asincrónica y sincrónica mediante reuniones de coordinación semanales, durante los dos años de trabajo.

A. Diseño Metodológico

El diseño metodológico se dividió en tres tramos:

Tramo 1: Marco Teórico.

1.1 Estudio del Estado del Arte desde el Aspecto Técnico.

[*] Revista Argentina de Trabajos Estudiantiles. Patrocinada por la IEEE.

1.2 Estudio del marco legal de la prueba digital en el proceso civil y comercial, laboral y de familia.
1.3 Recopilación y estudio de normas nacionales e i internacionales vinculadas.
1.4 Determinación de elementos que integrarán la Guía.
1.5 Armado del Informe Marco Teórico y Estructura de la Guía.
Entregable: Informe Marco Teórico y Estructura de la Guía.

Tramo 2: Desarrollo de la Guía.
2.1 Desarrollo del marco legal Civil y Comercial de la Guía.
2.2 Desarrollo del marco legal Laboral de la Guía.
2.3 Desarrollo del marco legal Familia de la Guía.
2.4 Desarrollo del marco técnico de la Guía.
Entregable: Primera Versión Borrador de la Guía de Actuación.

Tramo 3: Validación.
3.1 Validación interna de la Guía de Actuación.
3.2 Adaptación de la Guía en base a resultados de la validación interna.
3.3 Validación externa y abierta de la Guía de Actuación
3.4 Adaptación de la Guía en base a resultados de la validación externa.
3.5 Tercera Validación
3.6 Adaptación de la Guía en base a resultados de la tercera validación.
Entregable: Versión Final de la Guía de Actuación

III. CONTENIDO DE LA GUÍA

La Guía fue redactada utilizando un lenguaje claro, sencillo y no estrictamente técnico (en la medida de lo posible) , considerando que está dirigida a usuarios que, en su mayoría, no son expertos en el uso de tecnología. Se optó por emplear términos comprensibles para un público amplio, como abogados, funcionarios y otros profesionales del ámbito judicial o para el ciudadano.

La intención es que cualquier usuario pueda seguir los procedimientos descritos sin necesidad de conocimientos técnicos avanzados, asegurando así una amplia utilidad y accesibilidad. Sin embargo, en los casos en que sea necesario un análisis más detallado de la evidencia digital recolectada, la participación de un perito informático forense se vuelve indispensable y necesaria en el proceso. Esta estructura permite que los procedimientos básicos sean accesibles para todos, mientras que el análisis especializado queda reservado para expertos, asegurando que la evidencia mantenga su integridad y valor probatorio en un contexto legal.

A. Secciones Abordadas

- Fases de la Prueba Digital en el Proceso Judicial: temporalidad del proceso en que se encuentra, adquiere, preserva, ofrece, admite, produce y valora la prueba digital.
- Principios Generales de la Prueba Digital.
- Recomendaciones generales para el aseguramiento de la Prueba Digital: para ser considerada válida a lo largo de los diferentes momentos del proceso.

B. Procedimientos Desarrollados

Teniendo en cuenta los requisitos de preservación de evidencia digital más frecuentes, se tomó la decisión de colocar en la guía los siguientes procedimientos:

- Sitios web
- Redes sociales
- Servicios de mensajería
- Correos electrónicos
- Archivos en general

La organización de los contenidos dentro de cada procedimiento en la Guía se divide en las siguientes secciones:

Aspectos Generales: Esta sección describe conceptos generales relacionados con el tipo de prueba digital con la que se va a trabajar.

- Aspectos Jurídico-legales: Aquí se detalla la normativa que respalda o fundamenta cada uno de los procedimientos o buenas prácticas sugeridas.
- Procedimiento: Se enumeran una serie de pasos que indican cómo realizar las tareas de adquisición, preservación y presentación de la prueba digital. Para garantizar que todos los usuarios puedan seguir los procedimientos, no se sugiere el uso de herramientas específicas.
- Consideraciones: En cada procedimiento se incluyen consideraciones particulares a tener en cuenta, que pueden estar relacionadas con el tipo de evidencia digital o con el programa desde el cual se debe obtener la evidencia.
- Casos de uso: Para ejemplificar los procedimientos y aportar mayor claridad, se han agregado casos de uso que proponen ejemplos de los programas más frecuentes.

IV. VALIDACIÓN

Tras su primera publicación, en su versión borrador, se dio inicio al proceso de validación de la misma. El objetivo general de este proceso fue difundir y validar con la comunidad judicial, abogados y peritos informáticos los protocolos de adquisición de información de sitios web, redes sociales, servicios de mensajería, correos electrónicos y archivos, así como las recomendaciones de preservación y presentación.

Para lograrlo, era necesario que los usuarios y/o profesionales entre los que se encontraban los destinatarios a los que está dirigida la Guía participen en el proceso de validación para garantizar la calidad, eficacia, legitimidad y legalidad de los procedimientos. Este proceso no solo ayudó a verificar que los procedimientos fueran adecuados y contribuyeran a los fines previstos, sino que también permitió identificar aspectos que necesitaban mejoras o una mayor precisión en la explicación. Es así, que validar la Guía fue fundamental para generar confianza en el producto final que sería publicado, asegurando su legitimidad y adopción por parte de la comunidad.

A. *Primera Validación*

El proceso de validación comenzó en noviembre de 2023, mediante una convocatoria abierta a través de redes sociales, dirigida a abogados, escribanos, magistrados, funcionarios, operadores judiciales, peritos y otros profesionales del ámbito de la informática relacionados con la prueba en procesos judiciales. Además, se extendieron invitaciones a instituciones nacionales relevantes en el tema, para que aportaran en la validación.

Del total de validadores inscriptos, se seleccionó un grupo de especialistas para que hicieran sus aportes no en la primera fase de validación, sino posteriormente, aportando sus observaciones y sugerencias tras esta primera etapa.

Cada postulante tuvo la libertad de inscribirse en todas las secciones de la Guía en las que quisiera participar, de acuerdo con sus intereses y experiencia. A cada participante se le envió la sección correspondiente a validar, junto con un formulario diseñado para recoger sus comentarios y sugerencias basados en su experiencia con el procedimiento evaluado.

En el caso de las instituciones, además de la validación individual, se les solicitó una devolución detallada y cualitativa, que debía ser entregada en papel membretado y firmada por las autoridades de la institución y por los validadores que participaron en el proceso. Esto aseguraba que las observaciones tuvieran un respaldo formal, aumentando la credibilidad y el rigor del proceso de validación.

En el proceso de validación participaron un promedio de 40 validadores por cada procedimiento. De las 24 jurisdicciones del país, 18 estuvieron representadas, quedando sin representación las provincias de Corrientes, San Juan, San Luis, Santa Cruz, Santiago del Estero y Tierra del Fuego. Del total de participantes, el 60% eran abogados, mientras que el 40% restante se dividió entre peritos informáticos e informáticos en general. En cuanto a la utilidad percibida de las instrucciones, el 70% de los participantes consideró que fueron muy útiles, el 25% las calificó como útiles, y el 5% restante las encontró solo algo útiles o nada útiles.

Una vez que se recibieron todas las devoluciones de los validadores, se incorporaron las mejoras y modificaciones sugeridas, asegurando que la Guía mantuviera su valor y finalidad tanto en los aspectos técnicos como jurídicos.

B. *Segunda Validación*

En el mes de julio de 2024, tras finalizar las incorporaciones, la Guía fue enviada al grupo de especialistas que habían sido seleccionados anteriormente para una revisión final. En esta etapa, no se utilizó un formulario de evaluación; cada validador realizó sus observaciones y aportes de manera libre y según su criterio. Con todas estas contribuciones, se implementaron los cambios pertinentes y, en agosto de 2024, se inició el proceso de registro de la Guía.

V. Beneficiarios de la Guía

La creación de esa Guía es un gran aporte, ya que no existía un enfoque uniforme en la adquisición, extracción, preservación e incorporación de la evidencia digital en los procesos civiles, comerciales, laborales y familiares genera decisiones desiguales y, en ocasiones, contrarias a los derechos humanos reconocidos constitucionalmente. Este desarrollo combina de manera compleja los campos de la Informática y el Derecho, lo que representa un avance significativo en ambas disciplinas. Los conocimientos científicos y tecnológicos de estos campos se han integrado para crear un producto innovador que constituye un avance sustancial y original para los organismos de justicia.

Se espera que esta Guía, fruto de un trabajo interdisciplinario e interinstitucional, sea de gran utilidad práctica y que, eventualmente, sea adoptada por diversas provincias. La transferencia de estos conocimientos se realizará a través del Instituto Federal de Innovación, Tecnología y Justicia (IFITEJ) de la Ju.Fe.Jus.

VI. Conclusión

Actualmente, los organismos de justicia provinciales enfrentan una notable falta de protocolos claros y estandarizados para la adquisición, preservación y presentación de la prueba digital. Esta carencia normativa genera incertidumbre y desafíos tanto para abogados como para jueces, quienes deben lidiar con la complejidad de la evidencia digital sin un marco adecuado que respalde su manejo.

La guía propone un conjunto de requisitos que debería cumplir una prueba para ser considerada valiosa y útil en los procesos judiciales no penales, y que a un tiempo permita la búsqueda de la mejor evidencia posible dentro un contexto real y concreto de acceso equitativo a la justicia.

El producto desarrollado no solo representa un avance significativo para la sociedad en general, sino que también fortalece la confiabilidad del proceso judicial y asegura la integridad de la prueba presentada. Este enfoque apunta a reducir las brechas tecnológicas y normativas que impactan en la práctica judicial cotidiana, promoviendo un entorno donde la evidencia digital pueda ser tratada con el mismo rigor y validez que la prueba física tradicional.

La Guía de actuación para la adquisición, preservación y presentación de la prueba digital aborda estas carencias mediante la promoción de buenas prácticas que aseguren la certeza, autenticidad y valor probatorio de la evidencia digital a lo largo del proceso judicial. Este documento pretende establecer un estándar que respalde a los operadores jurídicos en cada etapa del proceso, desde la recolección hasta la presentación en juicio, minimizando los riesgos de manipulación o pérdida de integridad.

Uno de los aspectos más innovadores del proyecto fue la inclusión activa de la comunidad y de instituciones especializadas en la validación del instrumento, lo que no solo enriqueció su contenido, sino que también fortaleció la legitimidad y aplicabilidad de la guía. Esta colaboración permitió llevar a cabo una prueba piloto de alcance federal, evaluando la efectividad del documento y su adecuación en términos de lenguaje claro, con el objetivo de que sea accesible y comprensible para todos los operadores del sistema, independientemente de su grado de especialización tecnológica.

La implementación de la Guía de actuación para la adquisición, preservación y presentación de la prueba digital representa un paso esencial hacia la estandarización del manejo de la evidencia digital en los procesos judiciales no penales. Al establecer un marco claro y accesible que integra buenas

prácticas y estándares de actuación, se busca garantizar que la prueba digital se trate con principios forenses, promoviendo un acceso equitativo a la justicia. Este esfuerzo colaborativo, validado por la comunidad y expertos, sienta las bases para una justicia más transparente, inclusiva y adaptada a los desafíos tecnológicos actuales, minimizando así las brechas normativas que afectan a los operadores jurídicos y, en última instancia, a la sociedad en su conjunto.

VII. Equipo de Trabajo

Este desarrollo solo fue posible gracias a un equipo de trabajo comprometido con la mejora continua, convencido que la integración de las disciplinas de la Informática y el Derecho es clave para lograr avances genuinos de conocimientos para desarrollar un producto que constituye un avance sustantivo y original para los organismos de justicia.

Este esfuerzo conjunto demuestra que el trabajo colaborativo y el cruce de saberes son fundamentales para transformar los desafíos judiciales en oportunidades de mejora concreta y efectiva.

Directora: Esp. Ing. Ana Haydée Di Iorio Facultad de Ingeniería de la Universidad FASTA

Codirectora: Esp. Abg. Lic. Marisa Repetto Facultad de Derecho de la Universidad CHAMPAGNAT

Investigadores Facultad de Ingeniería de la Universidad FASTA - Facultad de Ciencias Jurídicas y Sociales de la Universidad FASTA FASTA:

- Esp. Ing. Ana Haydée Di Iorio (FI UFASTA)
- Ing. Santiago Trigo (FI-UFASTA),
- Esp. Abg. Pablo Cistoldi (FCJyS-UFASTA, FI-UFASTA),
- Ing. Bruno Constanzo (FI-UFASTA).
- Lic. Lucía Algieri (FCJyS-UFASTA, FI-UFASTA)
- Esp. Ing. Fernanda Rosales (FI-UFASTA)
- Lic. María Belén Álvarez Cestona (FCJyS-UFASTA, FI-UFASTA)
- Dra. Bibiana Luz Clara (FCJyS-UFASTA)

Investigadores Facultad de Derecho de la Universidad CHAMPAGNAT:

- Abg. Mgter. María Fernanda Díaz (FD-UCHAMP)
- Abg. Marisa Repetto (FD-UCHAMP)
- Abg. Mgter Mario Adaro (FD-UCHAMP)

Referencias

[1] Bielli, Ordoñez, Quadri, "Tratado de la Prueba Electrónica", *La Ley, Ciudad Autónoma de Buenos Aires,* Tomo I, 2022.
[2] A. Di Iorio, M. Repetto, et al, "Guía de actuación para la Adquisición, Preservación y Presentación de la Prueba Digital", *InFo–Lab, Mar del Plata*, 2023.
[3] A. Di Iorio, M. Mollo, et al, "Consideraciones para el diseño de un Laboratorio Judicial en Informática Forense", *InFo–Lab, Mar del Plata*, 2016.
[4] A. Di Iorio, P. Cistoldi, et al, "Guía técnica para el diseño de laboratorios judiciales de informática forense", *InFo–Lab, Mar del Plata*, 2019.

Adquisición forense de videos en requisitorias periciales en el Departamento Forensia Digital de Gendarmería Nacional

B.A. Del Frari Vázquez

IUGNA - "Instituto Universitario de Gendarmería Nacional" - badelfrarivazquez@gna.gob.ar

***Resumen*— Análisis de la adquisición forense de videos en DVR en la División Análisis de Videos e Imágenes de Gendarmería Nacional entre 2019 y 2021. Se examinaron casos y procedimientos, comparando métodos manuales y con software forense para obtener videos en investigaciones criminales. La investigación identificó limitaciones técnicas en la obtención de imágenes sin software especializado y comparó la eficacia de ambos enfoques. Los resultados demuestran que los peritos pueden lograr resultados similares con diferentes métodos, cada uno con sus ventajas y desventajas. El estudio destaca la importancia de la preparación forense ante el aumento de sistemas CCTV y el uso de archivos de video como evidencia judicial. Esta investigación proporciona información valiosa para investigadores y laboratorios forenses, mejorando la comprensión de los desafíos en la adquisición de videos para fines judiciales.**

***Abstract*-- This study analyzes the forensic acquisition of videos from DVRs in the Video and Image Analysis Division of the National Gendarmerie between 2019 and 2021. Cases and procedures were examined, comparing manual methods and forensic software for obtaining videos in criminal investigations. The research identified technical limitations in image acquisition without specialized software and compared the effectiveness of both approaches. Results demonstrate that experts can achieve similar outcomes using different methods, each with its own advantages and disadvantages. The study highlights the importance of forensic preparedness given the increase in CCTV systems and the use of video files as judicial evidence. This research provides valuable information for investigators and forensic laboratories, improving the understanding of challenges in video acquisition for judicial purposes.**

Introducción

La Criminalística a lo largo de su evolución, producto de la actualización que envuelve a las disciplinas que la componen, adquirió nuevos métodos y herramientas para llegar a resultados concluyentes, analizando nuevos tipos de evidencias para ser valoradas por la justicia. De acuerdo a lo que dice Lerena en su prólogo;

Hoy la tecnología interpela al derecho penal y desafía a la criminalística; "obtener pruebas" y "hacer justicia" requiere indefectiblemente del dominio de la tecnología, en particular de la informática aplicada. Esto hace que la informática se constituya en la herramienta fundamental de las Ciencias Forenses en la actualidad [1].

Hasta hace un tiempo, esta ciencia sólo abarcaba un determinado campo de estudio, en el cual se destacaban, por ejemplo, pericias del tipo balísticas, accidentológicas, químicas, documentológicas, de huellas y rastros, etc. Sin embargo, hoy en día, la implementación de cámaras de video en diferentes entornos estructurales tanto en el espacio público como en el privado, hace que estos dispositivos puedan convertirse en elementos potencialmente útiles para la investigación judicial, ya que al estar instalados en diversos tipos de espacios, como por ejemplo los que existen en una entidad bancaria, un comercio o simplemente en una vivienda familiar, pueden capturar en sus imágenes diferentes situaciones que puedan tener que ver con hechos relacionados a delitos. Esos videos actualmente se pueden ofrecer como documentos probatorios en un proceso judicial. De allí su importancia [2].

Los avances en tecnología y la entrada masiva de marcas asiáticas en el mercado no solo han reducido significativamente el costo de los DVRs y de las cámaras, sino que también han hecho que la tecnología sea accesible para muchos usuarios como para utilizarla en un local comercial, en un club, en el hogar, etc.

Teniendo en cuenta la creciente instalación de cámaras de seguridad, se puede interpretar que el tratamiento de videos en procesos judiciales se incrementa. Tales así que el Estado debe establecer normativas para su implementación en procesos que buscan justicia. Por ejemplo, podemos citar lo fundamentado para la creación de la Ley 14.172 de la provincia de Buenos Aires, entre cuyos textos sostiene que:

"El carácter siempre cambiante de los fenómenos sociales e institucionales, y el permanente avance de la tecnología en materia de prevención e investigación de hechos delictivos, reclama la permanente revisión de los marcos regulatorios para concretar una mayor efectividad de la actividad estatal a la hora de dar respuestas concretas a la ciudadanía, dotando a la justicia de nuevas herramientas en la investigación de delitos." [3]

En cuanto a la modalidad de funcionamiento de los sistemas que los Circuitos Cerrados de Televisión (CCTV) poseen, estos pueden resultar ser dispositivos pocos conocidos, por los magistrados de la justicia o los diferentes funcionarios públicos afines. Por ello, mayoritariamente, la doctrina posibilita la utilización de pruebas que provienen de videocámaras sin dejar de prestar atención a la forma de su obtención, preservación, traslado y análisis para que puedan convertirse en pruebas válidas y auténticas. Los diferentes proyectos de ley de un Estado hoy en día vislumbran la inclusión de videograbaciones para que, en un posterior análisis de los peritos, puedan interpretar una escena y sus efectos [4].
Planteamiento del problema: Están en constante aumento la

gran cantidad de casos en los que la comisión de un delito puede quedar grabado en un video y convertirse en material que ayude a individualizar personas, objetos, etc. Por ello es importante que, desde la obtención de estas evidencias, los procesos se realicen de forma apropiada. El principal problema radica en que los sistemas informáticos de los DVRs que generan esos videos son diferentes a los que por ejemplo se pueden encontrar en una computadora de uso habitual. Sumado a ello, suelen cometerse errores o no resulta fácil poder obtener de manera forense, este tipo de material digital, para luego ser analizado por los expertos. Existen diferentes factores técnicos y/o procedimentales que deben sortearse. Por ello los funcionarios encargados de hacer cumplir la ley, deben formarse en el manejo de evidencia digital, particularmente en este caso, sobre las formas de obtener estos tipos de videos y así estar capacitados a la hora en que se deba manipular esos "testigos digitales". Cabe destacar que un video al estar alojado en un soporte magnético de almacenamiento; sea este un disco duro, Pendrive, DVD, etc, el mismo puede destruirse, conforme la evidencia digital resulta vulnerable y volátil. Es así que se deben tomar los recaudos necesarios a fin de que el mismo sea íntegro y apto para su posterior análisis, y por sobre todas las cosas que no se destruya. Gendarmería Nacional posee un área que se encarga de trabajar y analizar estos tipos de requisitorias periciales, ese lugar se conoce como la División Análisis de Videos e Imágenes, dependiente del Departamento Forensia Digital, en la Dirección de Criminalística y Estudios Forenses, ubicada en la Ciudad Autónoma de Buenos Aires. En esta oficina trabaja personal idóneo en el tratamiento de evidencia digital, realizando a lo largo de cada año una considerable cantidad de informes periciales a nivel local y nacional e incluso de trascendencia relevante. Los mismos son solicitados por los fueros federales y eventualmente también por el fuero ordinario. Se elaboran diferentes informes clasificados en; análisis y captura de imágenes, mejoramiento de imágenes, análisis de integridad, digitalización de VHS y el tema que nos compete; extracción forense de videos. En este último tipo de pericia es donde se presentan los mayores aspectos que se deben tener en cuenta por parte, tanto de los investigadores judiciales como de los peritos, ya que, por los métodos de trabajo, que más adelante se explican, es donde mayor coordinación, tiempo, metodología compleja, recursos humanos y materiales se puede demandar. Dentro de ese departamento la oficina denominada "Análisis de Videos e Imágenes", realizó y puede generar aún este tipo de pericias sin el uso de software forense. Para llegar a establecer un proceso de trabajo en sus informes periciales, los peritos recurrieron a la propia investigación y desarrollo para aplicar procesos internamente estandarizados de acuerdo a las buenas prácticas forenses en materia digital. Ello en razón de que no existe al momento del inicio de este trabajo, a nivel nacional y de forma estandarizada, un protocolo o guía de actuación íntegramente específica sobre el levantamiento u obtención de videos de los dispositivos de grabación que se corresponden a un DVR, tanto en el lugar donde se encuentra funcionando el dispositivo electrónico, como posteriormente en un laboratorio informático.

No obstante, desde el año 2020 esta oficina luego de obtener versiones de prueba (demo) del software propietario: DVR EXAMINER, ejecutó informes periciales trabajando con esa aplicación, aprovechando así, la posibilidad de entregar un producto pericial certificado por los procedimientos y reportes propios de un software reconocido internacionalmente por sus prestaciones exclusivas.

Sin embargo, en esa dependencia, nunca se analizaron los resultados comparativos, tanto de las operaciones de adquisición de videos de forma tradicional o "en caliente", contra los que puede ofrecer con el uso de software forense, el cual procesa y reporta de forma rápida y segura, el mismo tipo de evidencia.

Para finalizar este apartado, el cuestionamiento global a responder será el siguiente; ¿Cómo es la metodología de trabajo para la adquisición forense de videos de forma manual o, como se denomina en informática, "en caliente", que implementó esta oficina y cuáles son los resultados al comparar esos procesos, con el uso de software forense; respecto de eficacia y eficiencia? y ¿Cuáles son sus ventajas y desventajas?

Justificación: En el libro "El Rastro Digital del Delito" se define a la Criminalística:

"Como la ciencia aplicada, que, mediante el empleo del método científico, técnicas y conocimientos aportados por otras disciplinas, busca y estudia las evidencias materiales vinculadas con presuntos hechos delictivos, con el objeto de auxiliar a los órganos que procuran y administran justicia, brindándoles elementos reconstructores, identificadores y probatorios para que conozcan la verdad técnica e histórica de los hechos que investigan" [5, p. 53]

En las investigaciones actuales, además de huellas físicas, se buscan evidencias en el entorno digital. La capacidad de respuesta y adaptación de la criminalística en forensia digital es clave para satisfacer a los investigadores y quienes buscan justicia. Según el Dr. Rodríguez Manzanera, la criminalística implica aplicar conocimientos para descubrir y verificar científicamente un delito ya su posible responsable, permitiendo integrar la informática forense en la búsqueda y análisis de evidencias digitales, ayudando a expertos a decidir qué evidencias buscar. [6, pp. 52-54]

En lo que hace a la informática forense y los principios criminalísticos, la "escena del hecho" puede llegar a estar distribuida en diferentes lugares físicos, constituyendo entre todos ellos una "escena virtual". Por ello el proceso de adquirir, analizar, preservar y presentar datos producto de un conjunto de algoritmos electrónicos alojados en un soporte para elementos informáticos, es el novedoso y valioso auxiliar de la Criminalística [7].

Existen diversos tratados, protocolos, guías y manuales sobre evidencia digital, pero los procedimientos para el levantamiento de evidencia cuando se trata de videos generados por los DVR, resultan tener particularidades específicas que pueden desconocerse. El uso de sistemas de archivos tradicionales como los que se pueden encontrar en el común de las computadoras en la actualidad (NTFS, EXT2, EXT3, etc) serían difíciles de emplear en un DVR, ya que eso implicaría una mayor demanda de recursos, y dada la acotada disponibilidad de RAM que estos dispositivos poseen y la necesidad de realizar acciones de escritura y lectura lo más eficientes posibles, llevó a implementar sistemas de archivos propietarios y específicos que optimicen la grabación y la reproducción de videos.

Los sistemas de archivos de los DVRs son muy básicos ya que implementan un conjunto acotado de funciones necesarias para el almacenamiento y recuperación de las grabaciones, sin crear estructuras de carpetas o la posibilidad de permitir borrar o renombrar determinados videos [8]. Eso hace imposible por ejemplo conectar el disco duro de uno de estos equipos a una PC de escritorio y poder ver los videos que allí se encuentren grabados.

Es importante investigar los procedimientos para obtener videos como evidencia digital, considerando la experiencia de un laboratorio pericial. Estos, al ser datos digitales, son volátiles y vulnerables, ya que pueden alterarse o copiarse indefinidamente. La manipulación incorrecta puede destruir esta evidencia, por lo que es fundamental que los investigadores garanticen su autenticidad e integridad. El perito informático debe utilizar herramientas de forma específica y controlada, en un proceso demostrable y reproducible, para asegurar la validez de la prueba ante las autoridades judiciales respectivas. [7].

Por lo desarrollado en los párrafos precedentes, describir la metodología de trabajo sobre el tema y analizar cómo esta dependencia puede arribar a un mismo resultado aplicando técnicas diferentes, puede tratarse de un tema interesante a la vez que poco explorado o documentado académicamente en el campo de la criminalística y los estudios forenses.

Objetivos

Objetivo General

Analizar los procedimientos realizados para la extracción forense de videos en la División Análisis de Videos e Imágenes dependiente del Departamento Forensia Digital de Gendarmería Nacional, entre los años 2019 al 2021.

Objetivos Específicos

- Describir las formas de obtención de videos en DVRs, ofrecidos por la justicia a esa oficina, para realizar informes periciales.
- Identificar los problemas o limitaciones técnicas que se pueden presentar en el procedimiento de adquisición de videos sin el uso de software forense y sus posibles soluciones.
- Comparar los procedimientos para la obtención de videos de forma tradicional, con los casos en que se utilizó el software forense llamado DVR EXAMINER.

ESTADO DEL ARTE

Luego de investigar se pueden citar las siguientes publicaciones como antecedentes que articulan con el tema, en cuanto al tema que se aborda en este trabajo de investigación.

Un estudio presentado en la novena Conferencia Internacional sobre Análisis Forense Digital (2013) aborda las limitaciones de los sistemas CCTV, como la baja calidad de imágenes. Los autores Ariffin, Slay y Choo proponen una técnica novedosa para extraer archivos de video de discos duros de DVR dañados o corruptos.

La técnica se basa en identificar la marca y tipo de sistema de archivos del DVR, verificar la hora real y la marca de tiempo (timestamp), leer sectores del disco, identificar firmas de archivos y patrones hexadecimales para extraer videos, y finalmente documentar los resultados. [10].

El estudio demostró que la técnica es efectiva y puede ser aplicada a diferentes marcas de dispositivos sin requerir interacción con el fabricante. Los autores planean desarrollar un software forense CCTV fácil de usar para extraer archivos de video.

En el documento de conferencia de Silva (2018), que se titula “Ingeniería inversa del sistema de archivos de DVRs PCBox”, se plantea la dificultad y la imposibilidad de poder contar con los videos de estos tipos de dispositivos, incluso utilizando los softwares de uso más común en cualquier laboratorio informático. Menciona que, si bien en el mercado existen dos programas, DVR Examiner y HX Recovery, que lo pueden hacer de forma rápida y automatizada, el principal problema son los costos económicos de los mismos [11]. Analiza para este caso, el sistema de archivos de un DVR de la marca PCBox, utilizando la ingeniería inversa para analizar y comprender la estructura de los archivos en el disco duro y sus metadatos. Para ello cuenta con un software forense llamado FTK que desglosa dicha información. Una vez comprendida la estructura de los archivos que el disco duro del DVR aloja y luego de diferentes trabajos de campo como pruebas realizadas; el autor desarrolló un software para poder descargar y reproducir los archivos de videos de este dispositivo, pudiendo incluso filtrar los resultados obtenidos por fecha y hora. Finalizando, el autor plantea que, si bien se llegó al resultado esperado de forma positiva, el mismo demanda mucho tiempo de análisis y trabajo por lo que, ante los casos judiciales en los que urge contar con estos videos, este tipo de tareas no podrá satisfacer dicha demanda [11].

En el trabajo académico traducido del idioma inglés, S. Sandeepa, A. Reyaz and M. Silpa (2018) "An Efficient Approach to Recover CCTV Video from Proprietary DVR File System," 2018 International CET Conference on Control, Communication, and Computing (IC4)” [12], expone que Las grabaciones de vídeo son cada vez más utilizadas como prueba en causas judiciales. Este documento propone métodos innovadores para mejorar el análisis forense de videos digitales, destacando la importancia de la calidad de imagen en la identificación biométrica y el reconocimiento facial, especialmente en sistemas de inteligencia artificial. El estudio revela que la resolución de la cámara y la distancia de los sujetos afectan los resultados del reconocimiento facial. Aunque la posición fija de la cámara fue una limitación, se sugiere que múltiples ubicaciones podrían mejorar los resultados. [13] Finalmente, los autores desarrollaron un sistema de investigación digital basado en video para mejorar la calidad y recuperación de pruebas, incluyendo un método de extracción inversa para combatir el crimen

En la investigación de Orellano Benancio, L. (2021), titulada “El uso de la pericia de identificación de la placa de rodaje vehicular y su relación con la calidad del video digital en los hechos delictivos de robo en la oficina de peritajes del Ministerio Público, Lima, 2019-2020” [14]. El estudio analiza la relación entre la calidad del video y los resultados de las pericias de identificación de placas de vehículos en la oficina de peritajes de una ciudad. Se examinaron informes del área de análisis digital forense, considerando variables como placas de

rodaje y indicadores alfanuméricos. Los videos se obtuvieron de equipos de grabación SVV (DVR) y se extrajeron de manera forense utilizando software especializado.

La conclusión es que existe una relación directa entre la calidad del video y la cantidad de caracteres identificados en una placa de rodaje. Por lo tanto, se recomienda que las evidencias digitales tipo video o imagen que remiten las fiscalías posean la mayor calidad posible para asegurar resultados precisos y confiables en las pericias de identificación de placas de vehículos

En el artículo publicado por Medina Gómez y Hernández Bejarano (2021), titulado "Análisis forense para móviles", se plantea que la gran existencia de teléfonos móviles permite que los mismos aporten ayuda en un proceso judicial. Entre sus objetivos se plantea la importancia en el proceso de la evidencia digital, destacando la forma de su diseño, obtención, reproducción, análisis, presentación, etc. Así, plantea la importancia del SOP (traducido como Proceso Operativo Estandarizado) en el análisis forense en evidencia digital. Un SOP es un proceso diseñado para realizar rutinas con tiempo y recursos limitados [15]. La importancia en equipos profesionales, radica en la aplicación habitual de especificaciones de trabajo documentadas, ligadas al ambiente de trabajo, vinculadas a la aplicación de tecnología y operación de herramientas, y su contenido está organizado por texto, gráficos y otras especificaciones. Propone resaltar la importancia de la cadena de custodia en la evidencia digital a la vez que se brindan recomendaciones y una metodología para realizar los procesos de análisis forense en dichos dispositivos, clasificando en dos partes importantes, la estructura de los mismos (la SIM y el ME). Posteriormente se mencionan softwares del tipo Open Source y describe tres de los más conocidos programas cuyas licencias pagas permiten analizar y crear reportes de manera forense y así obtener evidencia de forma segura y documentada. Estos son: MSAB, CELLEBRITE Y OXYGEN FORENSIC DETECTIV.

Finalizando la búsqueda de material documentado públicamente, relacionado a la obtención de evidencia digital en DVR; Valencia Álvarez (2022) sostiene un punto de vista destinado especialmente a los profesionales del derecho en general, ya que el autor es abogado especializado en materia informática. Él plantea que en la actualidad existe aún una problemática relacionada con el correcto levantamiento de evidencia física como sangre, semen, cabello, etc, donde resulta complejo determinar la manipulación intencionada o contaminada, pero más aún lo es para la evidencia del tipo digital, donde una persona no especializada en la materia, puede no advertir dichas irregularidades en este tipo de evidencia. Para el levantamiento de las pruebas digitales que se pueden encontrar en un DVR, se requiere de procedimientos y cuidados específicos para su conservación y autenticación que para ser satisfechos deben ser llevados a cabo por personal idóneo en la Informática forense [16].

Antes de concluir el autor propone una tabla como guía para clasificar los diferentes tipos de dispositivos de almacenamiento de potencial prueba electrónica, su recolección, transporte, preservación, copia del mismo y concluye diciendo que, si bien los encargados de impartir justicia en su formación en materia de derecho pueden no saber al respecto de estas técnicas que resultan novedosas, deben asesorarse y auxiliarse en los expertos o formarse al respecto. De esta manera ofrecer una prueba electrónica adecuada permitirá inclusive, dado el caso, advertir alguna irregularidad en la que ofrezca la contraparte, destacando la importancia que, de corresponder, la misma puede ser desvirtuada por no haberse observado un protocolo correcto en su recolección inicial entre otros aspectos a tener en cuenta legalmente.

I. METODOLOGÍA

De acuerdo a lo que plantea Sampieri (2010), el diseño metodológico comprende los procedimientos necesarios para definir los pasos con los cuales obtendremos los datos necesarios a fin de cumplir con los objetivos.

El presente Trabajo, es una investigación documental del tipo mixta, con variables cualitativas y cuantitativas, con un enfoque descriptivo y retrospectivo. Para ello, se utilizaron como insumos para el marco teórico y el estado del arte, información relacionada a investigaciones, artículos, tesis, presentaciones escritas en seminarios y conferencias, textos con bibliografía específica de la temática sobre informática forense y equipos DVR.

Para proceder al estudio de campo, se obtuvo acceso a la información documentada de los diferentes informes periciales sobre causas judiciales reales en las que se enviaron equipos de grabación digital de videos (DVR) a la oficina de la División de Análisis de Videos e Imágenes, entre los años 2019 al 2021. Se establece que por cada caso hay un DVR que se analiza. Asimismo, se accedió a los informes periciales y a las anotaciones complementarias que cada caso tuvo en su etapa de elaboración.

Para apreciar la metodología de trabajo de la dependencia, sobre las mismas, se tuvieron en cuenta las siguientes variables:

- Las marcas de los DVRs
- El volumen de información del disco duro del DVR
- El método de adquisición aplicado
- La recepción del equipo con la cadena de custodia
- El envío de la fuente de alimentación junto con el equipo
- Conocimiento del usuario y contraseña del DVR
- Acceso al equipo sin contar con la contraseña aplicando métodos alternativos
- Existencia real de las grabaciones de los días solicitados
- Posterior pedido de realización de otras pericias sobre los videos obtenidos
- Horas y días que demanda cargar las grabaciones en un soporte de almacenamiento externo.

Las unidades de análisis fueron los 24 DVRs y sus discos duros, seleccionados de una población de 44 casos entre 2019-2021. Los DVRs elegidos tenían un disco duro SATA 3 de 1-2 Terabytes y se utilizaron herramientas forenses como TABLEAU TD3 para realizar duplicados o imágenes forenses.

Después de obtener la autorización necesaria, se recolectó información sobre los procedimientos utilizados para obtener videos de forma forense, analizando métodos, alcances, limitaciones y variables. Se respetaron protocolos de seguridad y confidencialidad, evitando revelar datos personales sensibles. Los datos se organizaron en una tabla Excel para analizar y presentar resultados, concluyendo con observaciones relevantes sobre la extracción forense de videos.

II. PROCESAMIENTO Y ANÁLISIS DE DATOS

A. PROCESAMIENTO Y ANÁLISIS DE DATOS

Vale aclarar que cada caso representa un DVR que fue peritado en esa dependencia. En la presente tabla, se registraron los 24 casos que se analizaron junto a las diferentes características observadas principalmente en cuanto al tiempo procesado.

TABLE I
MATRIZ DE DATOS: UNIDADES DE ANÁLISIS: 24 CASOS

TABLA DE VARIABLES MÁS IMPORTANTES ANALIZADAS EN ADQUISICIÓN FORENSE DE VIDEOS					
CASO	MÉTODO APLICADO	TIPO DE COPIA DEL DISCO ORIGINAL	CANTIDAD DE VIDEOS A EXTRAER	DEMORA EN HORAS PARA LA EXPORTACIÓN DE LOS VIDEOS	DEMORA EN DÍAS HÁBILES PARA LA EXPORTACIÓN
1	MANUAL SIN SOFT FORENSE	DUPLICADO FORENSE	SOLO 24 HORAS	16	4
2			TOTALIDAD	93	23
3			SOLO 30 MINUTOS	NO EXISTE PERIODO SOLICIDADO	NO EXISTE PERIODO SOLICIDADO
4			TOTALIDAD	104	26
5			TOTALIDAD	160	40
6			SOLO 72 HORAS	60	12
7			SOLO 3 HORAS	NO SE PUDO REETEAR CONTRASEÑA	NO SE PUDO REETEAR CONTRASEÑA
8			TOTALIDAD	396	99
9			SOLO 24 HORAS	10	3
10			SOLO 6 HORAS	NO SE LOGRÓ ENCENDER EL DVR	NO SE LOGRÓ ENCENDER EL DVR
11			SOLO 3 HORAS	1	1
12			TOTALIDAD	67	17
13	CON SOFT FORENSE "DVR EXAMINER"	IMAGEN FORENSE	TOTALIDAD	5	1
14			SOLO1 HORA	NO EXISTE PERIODO SOLICITADO	NO EXISTE PERIODO SOLICITADO
15			TOTALIDAD	6	1
16			TOTALIDAD	7	1
17			TOTALIDAD	15	1
18			TOTALIDAD	5	1
19			TOTALIDAD	8	1
20			SOLO 24 HORAS	0.21	1
21			TOTALIDAD	6	1
22			SOLO 24 HORAS	0.14	1
23			TOTALIDAD	7	1
24			SOLO 24 HORAS	0.12	1

ANÁLISIS DE DATOS

B. Dando respuesta al primer objetivo específico se observa que:

Es posible identificar dos formas de obtención forense de videos: Sin uso de software forense y con uso del mismo. En el método sin uso de software forense; Método manual o tradicional (también conocido informáticamente como: "en caliente"), se aplica de forma directa sobre el DVR, sin el uso del software específico para la adquisición de los archivos de videos. El mismo debe ser enviado con su correspondiente fuente de alimentación, a fin de encenderlo luego de que se inserte el disco clonado. Esto significa que los peritos de dicha dependencia realizaron previamente, con los recaudos necesarios, la apertura del equipo de grabación (DVR), a fin de desinstalar el disco duro. Posteriormente realizaron la identificación del mismo, describiendo sus características, como marca, modelo, capacidad de almacenamiento, cantidad de cámaras, etc. Este proceso involucra la documentación de lo anteriormente expresado con las correspondientes constancias escritas y tomas fotográficas. Seguidamente realizaron la duplicación del disco interno, colocando como destino, otro disco interno formateado que la misma oficina posee para este tipo de tareas. Vale destacar que, en este trabajo, se detallaron únicamente los duplicados de HDD que se hicieron a través del duplicador forense TABLEAU modelo TD3, perteneciente al Departamento Forensia Digital.

Posteriormente los peritos procedieron en cada caso, a colocar y conectar el disco duplicado en el DVR, y a resguardar el disco duro original en un estuche dedicado para tal fin, hasta su devolución a las autoridades correspondientes.

La ejecución de la aplicación que la mayoría de los fabricantes desarrolla para sus equipos DVR/NVR, (ejemplo: GDMMS, HIK CONNECT, IDMSS, IVMS4500, etc) permitió a los peritos, en algunos de los casos indicados en la tabla, exportar los videos a un disco externo, de forma más rápida en comparación a la gestión que se puede realizar desde el propio grabador digital, las cuales suelen ser más lentas o limitadas. (backup de forma remota).

Finalmente, los archivos de videos se resguardan en un disco externo habiendo realizado los cálculos HASH para otorgar integridad a la información obtenida para su posterior documentación y traslado a la autoridad que lo requiera.

Ahora bien, para la aplicación del método, con uso de software forense, resulta indistinto si el equipo viene con o sin fuente de alimentación, si se informó o no el usuario y contraseña del equipo e incluso si solo se envía el disco duro sin el DVR. No se utiliza algún método alternativo o de fuerza bruta simple para romper las contraseñas de los mismos. Tampoco es necesario el método de exportación remota mediante el uso de la aplicación del fabricante, para intentar gestionar órdenes de backup más rápidas. Simplemente se realiza la imagen forense del disco instalado en el DVR en un disco externo que luego, a través de un bloqueador de escritura se puede conectar a la PC que ejecuta el DVR EXAMINER. Posteriormente se abre el software forense y se selecciona el disco a analizar para luego inspeccionar dicho elemento y a partir de las configuraciones del operador que correspondan, se indica el rango horario y los videos de las cámaras deseadas o bien se exportan todos los que estén grabados en el disco. El mismo permite realizar al mismo tiempo, los cálculos de HASH de forma automática cómo así también el reporte con demás metadatos del equipo de grabación y sus videos. Es por ello tal como puede observarse en la tabla 1, que las columnas que reflejan aspectos necesarios para operar con el método manual identificadas con color amarillo, ya no son tareas necesarias para esta modalidad de adquisición.

Continuando con el análisis de los datos y la descripción de los procedimientos que se llevan a cabo para la adquisición forense de videos, se destacan aspectos claves para interpretar diferencias básicas entre ambos métodos forenses. Tal como

puede observarse en la Tabla 1, a partir de la utilización del software forense DVR EXAMINER, desde el caso número 13, no se necesitó realizar duplicado forense, sino imagen forense, ya que dicho programa trabaja con el formato de sistema de archivos de imagen, como; DD, E01, RAW, entre otros. Asimismo, se destaca que se puede operar sin conocer las contraseñas, sin encenderlo o directamente sin contar con el equipo DVR y demás aspectos nombrados anteriormente.

En otra de las columnas de la tabla se consigna la cantidad de videos solicitados por los magistrados intervinientes. En algunos casos se solicitó obtener la totalidad de los videos y en otros un tiempo delimitado, independientemente del método forense aplicado.

En cuanto al posterior pedido de otro tipo de pericia consignado en la tabla 1, se observó que pueden solicitarse de acuerdo a la nomenclatura de la oficina; "Análisis y Captura de Imagen", "Análisis de Integridad" y "Mejoramiento de imagen". En la tabla se puede observar que en los casos número 1, 3, 4, 8, 11, 13, 14, 19, 20, 22 y 24; fueron solicitadas estas pericias adicionales. No obstante, en los casos 3 y 14, no fue posible debido a que no se encontraron los mismos en el rango horario solicitado.

Otro de los aspectos importantes analizados tiene que ver con el tiempo neto en horas reales que demandan las exportaciones de los videos con ambos métodos. Aquí se destacan considerables cantidades de horas para la obtención de los videos.

Para el caso número 8 con un disco duro de 2 terabytes de capacidad, se registró la demora de 396 horas, es decir 99 días hábiles. Este dato se convierte en la mayor demora registrada para la presente investigación.

La marcada diferencia en los tiempos de demora en estos dos últimos casos, (9 y 11) respecto a los anteriores con el mismo método, se corresponde a que se solicitó un rango acotado de tiempo de videos (24 y 3 horas, respectivamente, de un determinado día). En cambio, en los casos con más demoras, se corresponden a solicitudes netamente ligadas al copiado de la totalidad de las horas de las grabaciones contenidas en cada DVR.

Asimismo, se destaca que la determinación de cantidad de días que toma realizar las exportaciones de video de forma tradicional, se corresponde a un cronograma interno de labores en esta oficina, a razón de 4 horas diarias de trabajo de un operador asignado exclusivamente a esa actividad.

C. En respuesta al segundo objetivo es posible decir que que:

Como problemas o limitaciones, se pudo establecer que en 4 de los casos analizados no recibieron la fuente de alimentación, por ello con las especificaciones técnicas de voltajes, amperios y tipos de conectores necesarios los profesionales del área, procedieron a utilizar una fuente alternativa, que se encuentra dispuesta para tal fin en el laboratorio de la dependencia. No obstante, en una de las causas, más precisamente en la número 10, no les fue posible encender el DVR, en razón de que la ficha de conexión resultó ser muy específica para el tipo de pin de carga.

Por otra parte, en 6 de los 12 casos, los usuarios y contraseñas que los equipos DVR suelen tener, no fueron informados a los peritos. Por lo que esta situación llevó a las siguientes maniobras:

Para los casos 5 y 12, procedieron a colocar las contraseñas por defecto establecidas de fábrica para usuarios catalogados como "admin" o "root", las cuales son: "0123456789", "888888", "666666", "admin", etc. Pero en otras situaciones, previo asesoramiento y autorización de la autoridad competente; para los casos 2, 9 y 11; los peritos llevaron a cabo el reseteo de claves. Esto lo realizaron de acuerdo a las especificaciones que se pueden encontrar en portales web como: www.webyservicios.com, www.redesbps.com, de la página oficial de HIKVISION; www.hikvision.com, de las páginas de otras marcas y/o a través de la app para dispositivos móviles, "CCTV Super Password". Sin embargo, para el caso 7 de la marca del DVR "HANBANG" no les fue posible utilizar ningún método alternativo para restablecer el acceso. Esa situación por ende hizo que no se pudieran descargar los videos que el equipo contenía, a pesar de contar con la fuente de alimentación y el disco duplicado.

En los casos número 2 y 4, se realizó la copia de los videos a un disco externo, a través de una interfaz que se usa conectando un cable UTP con sus respectivas fichas, desde el puerto RJ45 del DVR, hacia su par en una laptop, debido a que se dejó constancia en las anotaciones del informe pericial, que hacerlo de esa forma resultaba más rápido. No obstante, en los casos 7 y 10 no fue posible obtenerlos, netamente debido a la falta de cable de alimentación y la imposibilidad de encender los equipos.

Con respecto al desfasaje de horas en el timestamp (marca de tiempo), se observó en los antecedentes de las pericias realizadas que en los casos identificados para este trabajo como: 1, 6 y 22, existía desfasaje con la hora real. Para advertir esa condición, se analizaron los informes periciales que llegaron a esa conclusión. Donde los peritos dejaron constancia en sus informes que de la observación en pantalla de determinados videos y al analizar el reloj digital que indica el tiempo fecha y hora, no observaron concordancia entre lo que se veía con lo que el reloj indicaba (por ejemplo, escena de noche con horas AM de día). Los peritos advirtieron esta situación en los apartados correspondientes del Informe Pericial, para alertar a los investigadores judiciales, ya que las referencias de tiempo pueden mal interpretarse y arrojar contradicciones en las respectivas declaraciones de las partes involucradas. Un respaldo equivocado de tiempo de video, o un análisis erróneo de imágenes, pueden no coincidir con la cronología real de los hechos investigados.

En cuanto a las requisitorias periciales en las cuáles se solicitaron una cantidad específica de horas de video y no la totalidad, en los casos número 3 y 14, no se encontraron videos. Para documentar dicha situación en el caso 3, del método sin software forense, los peritos ingresaron al menú de opciones y en el comando que permite reproducir los videos guardados se analizó el calendario digital de los DVRs con la marca de días que poseen grabaciones, buscando incluso meses anteriores a fin de incluir en sus informes los períodos de tiempo que el DVR resguardaba al momento de llegar a la oficina.

Para el caso 14 con el uso del DVR EXAMINER, sólo se examinó la copia del disco contenido en el DVR (imagen del original), se realizó la inspección de la cantidad total de días contenidos en el disco y se procedió a la búsqueda de grabaciones de forma filtrada, sobre el tiempo solicitado por la autoridad y desde las fechas más antiguas a las más modernas. En consecuencia, ese rango de fecha u hora no se encontraba grabado, por ende, los expertos realizaron las capturas de

pantallas necesarias y generaron el reporte del software para graficar esa situación e incluirlo en los informes.
Por último, se puede citar que sólo en 4 de los 24 casos, los DVRs fueron remitidos para su análisis con la correspondiente cadena de custodia. En este caso este Departamento, procedió a generar dicha cadena, de forma detallada para cada elemento de juicio recepcionado, (DVR) desde el momento que llegó para ser peritado, hasta que al finalizar es entregado con la misma, a fin de continuar registrando quiénes seguirán trasladando o resguardando el dispositivo de grabación.

E. En respuesta al tercer objetivo específico, se observa que:

Se pueden comparar aspectos que se destacan y que tienen que ver con el tiempo de demora que demandan las exportaciones de los videos al disco duro externo para enviar a la Magistratura correspondiente.

A continuación, se indican los casos, en los que se realizaron comparaciones en cuanto a cantidad de días de videos solicitados por los magistrados, teniendo en cuenta un mismo volumen de información contenido en el disco duro (1Terabyte). Es por ello que se identificaron 5 casos de cada método (Sin Software y Con Software) en los que se solicitaron la totalidad de los videos y 2 casos de cada método en los que se solicitaron sólo 24 horas de videos. Ver Gráficos 1 y 2.

Comparación 1 - Totalidad de los videos

Para el caso número 13 con un disco duro de 1 terabyte, en donde se solicita la totalidad de los videos, se observa que hubo una demora para obtenerlos de 5 horas, en un único día de trabajo. Sin embargo, para el caso número 5 sin uso del DVR EXAMINER, donde también se pide la totalidad de los videos que el DVR contenía, se registró una demora de 160 horas en 40 días hábiles de trabajo. Ver Gráfico 1.

Comparación 2 - Totalidad de los videos

Para el caso número 15 con un disco duro de 1 terabyte, en donde se solicita la totalidad de los videos, se observa que usando el DVR EXAMINER, hubo una demora de 6 horas, en un único día de trabajo, mientras que para el caso Nro. 4 donde se pide la misma cantidad, en un disco duro de 1 terabyte, se registró una demora de 104 horas en 26 días hábiles de trabajo. Ver Gráfico 1.

Comparación 3 - Totalidad de los videos

Para el caso número 18 con un disco duro de 1 terabyte, en donde se solicita la totalidad de los videos, se observa que hubo una demora en obtenerlos de 5 horas, en un único día de trabajo. Mientras que para el caso número 12 donde se pide la totalidad de los videos que el DVR poseía en un disco duro de 1 terabyte, se registró una demora de 67 horas en 17 días hábiles de trabajo. Ver Gráfico 1.

Comparación 4 - Totalidad de los videos

Para el caso número 21 con un disco duro de 1 terabyte, en donde se solicita la totalidad de los videos, se observa que hubo una demora para obtenerlos de 6 horas, en un único día de trabajo. En el caso número 2 donde se pide la misma cantidad de tiempo, es decir la totalidad de los videos que el DVR poseía en un disco duro de 1 terabyte, se registró una demora de 93 horas en 23 días hábiles de trabajo. Ver Gráfico 1.

Comparación 5 - Totalidad de los videos

Para el caso número 17 en el que se trabajó con el DVR EXAMINER un equipo que tenía un disco duro de 2 terabytes, la exportación de los videos demoró 16 horas. En cambio, como se registró en el caso número 8 con el método manual tomó 396 horas, es decir 99 días hábiles de trabajo siendo que se solicitó en ambos casos la totalidad de los videos y que el DVR poseía similares capacidades de almacenamiento de grabación; disco de 2 terabytes. Este caso resulta ser el que más demora registró, y teniendo en cuenta la información de la tabla, se podría inferir que realizar la adquisición de videos con el método con software forense, representa una demanda tan sólo del 4,04% de lo que conlleva realizarlo sin software forense. Por esta razón se adjunta más abajo otro gráfico al respecto. El mencionado resultado surge de la realización de una regla de tres simples directa en donde se conoce que 396 es el 100% y se averigua cuánto representa 16. Ver Gráficos 1 y 2.

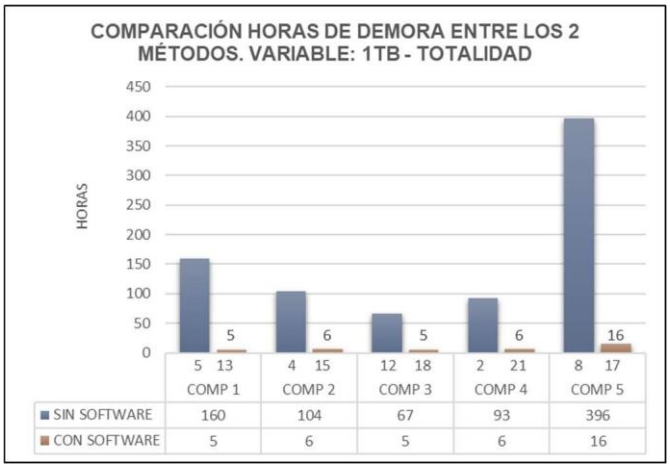


Fig. 1. Comparación de tiempo de demora para la obtención de videos (5 casos)

Fig. 2. Comparación de tiempo empleado de un caso respecto a otro

Continuando con las comparaciones, se mencionan a continuación aquellas en las que se solicitó únicamente 24 horas de videos.

Comparación 1 - 24 horas de video

Para el caso número 20, con un disco duro de 1 terabyte, en donde se solicita solo los videos de un día determinado (24 horas), se observa que con el uso del DVR EXAMINER, hubo una demora en obtener los videos de tan solo 21 minutos, en un único día de trabajo, mientras que para el caso número 1 donde se pide la misma cantidad de tiempo, es decir 24 horas y que el

DVR poseía un disco duro de 1 terabyte, se registró una demora de 16 horas en 4 días hábiles de trabajo. Ver Gráfico 3.
Comparación 2 - 24 horas de video

Por último, para el caso 24, en el que se solicitaron los videos de 24 horas, se registró la demora de tan sólo 12 minutos. Siendo que para el caso 9, para la misma cantidad de horas solicitadas con el método sin software, hubo una demora de 10 horas en 3 días hábiles de trabajo. Ver Gráfico 3.

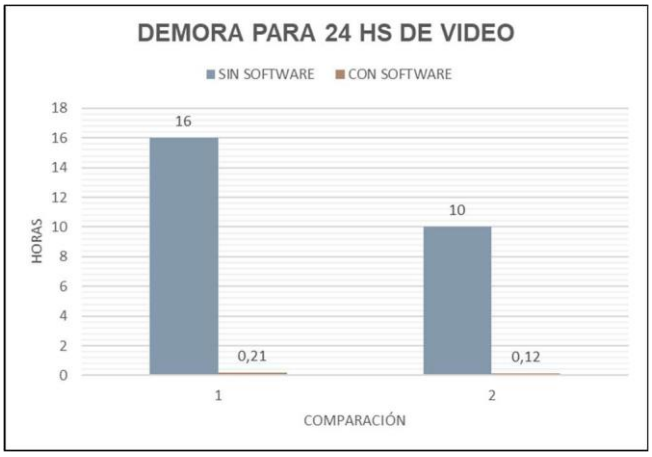


Fig. 3. Comparación entre los 2 casos para obtener 24 horas de video

Para finalizar esta etapa de procesamiento y análisis de datos, se expone a continuación una tabla donde se ve reflejado en una línea que representa los tiempos de demora para adquirir los videos a lo largo de los 24 casos. Obsérvese la tendencia a la baja desde el caso número 13 donde se incorporó a la oficina, el uso del Software DVR EXAMINER. Ver gráfico 4.

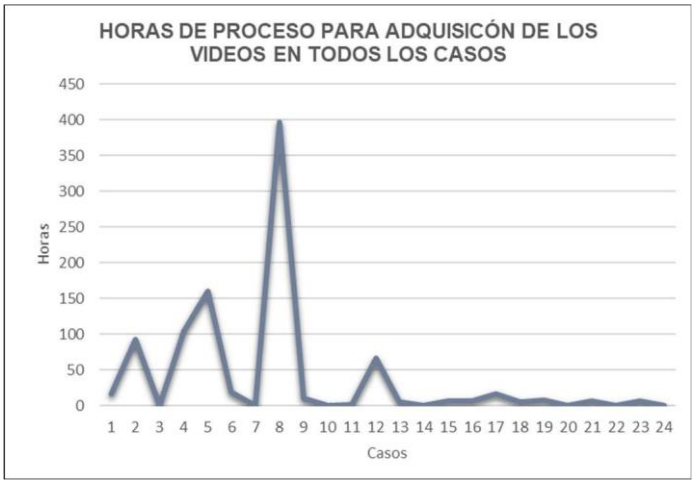


Fig. 4. Tendencia en las horas de los procesos

III. RESULTADOS Y DISCUSIÓN

En función de los datos procesados precedentemente, se puede afirmar que se encontraron dos métodos por los cuales esa oficina procede a obtener los videos de manera forense.
Uno de ellos es el método tradicional, manual o "en caliente" y el otro es con el uso de software forense propietario llamado DVR EXAMINER. Ahora bien, según lo expresado en el trabajo de Orellano Benancio (2021), se puede decir que existe una similitud ya que el objeto de estudio se trata también de una oficina pericial que tiene entre sus funciones el tratamiento de videos. Sin embargo, esa averiguación tiene como objetivo establecer una correspondencia entre la calidad de los videos y los resultados para determinar placas patentes de vehículos. Por otra parte, si bien se coincide en que el proceso de adquisición de los videos se realiza de forma forense, únicamente se lleva a cabo con el uso del software que aquí se citó, DVR EXAMINER, y no a través de un procedimiento alternativo o manual en el laboratorio, tal como sí lo hace la oficina de videos en Gendarmería [14].

En los resultados de la división estudiada, se puede observar que entre los años 2019-2021 se alternaron los procesos con ambos métodos, aplicando un Proceso Operativo Estandarizado (SOP en inglés) en el análisis forense en evidencia digital, tal como se menciona en el artículo publicado por Medina y Hernández (2021) y cumplimentando aspectos ligados al manejo de la evidencia digital siendo, Justificable, Auditable, Repetible y Reproducible. Eso se sustenta en el trabajo de Di Iorio (2016) y en el trabajo de Dupuy y, Kiefer (2017), en donde se habla acerca de la idoneidad del perito forense, que debe entregar un dictamen pericial en donde produzca una explicación consistente para cada punto pericial propuesto, con fundamentos técnicos-científicos [7, 17]. Además, este proceso de trabajar sobre el mismo DVR, también se fundamenta en el trabajo de Airala y Rapetti (2007), donde se habla acerca de que existen casos en los que se puede trabajar inevitablemente sobre un dispositivo original, pero dejando constancia de todo lo actuado y explicando los motivos por los cuales se lleva a cabo dichas acciones [18].

La complejidad de acceder a los videos cuando no se cuenta con la fuente de alimentación del DVR o no se conoce la contraseña, concuerda y se fundamenta con el trabajo de Silva (2018), allí se expone que los archivos de videos son de difícil acceso si no se tienen los datos de usuario y contraseña. No obstante, el autor realizó ingeniería inversa para acceder a dichas grabaciones, algo que no se realizó aún en la División estudiada, pero que coincide en que los procesos de obtención de video sin el uso de software específico demandan un considerable tiempo de ejecución y complejidad [11].

Los DVRs poseen en la gran mayoría de los casos, un sistema de archivos propietarios. Por lo que conectar el disco duro del dispositivo a una computadora, el sistema operativo no comprenderá la estructura de los sistemas de archivos patentados, según la marca del DVR. Eso se fundamenta en lo que dice, Ariffin, Slay y Choo (2013), donde advierte que las grabadoras de video digital (DVR) de circuito cerrado de televisión (CCTV) suelen incorporar la capacidad limitada de exportar archivos de video almacenados a medios de almacenamiento. Su contenido no se puede exportar fácilmente [19]. Esto hace que la recuperación forense adecuada de archivos de video sea una tarea costosa y difícil. Asimismo, otro aspecto coincidente en el trabajo de Silva (2018), es que también menciona que se puede usar el software DVR EXAMINER, pero teniendo en cuenta entre otras cuestiones su costo comercial, no pudo ser aplicado [11].

Por otro lado, se observa que, en diferentes casos, la contraseña y usuario fueron informados, lo que permitió que luego de haber realizado la copia forense bit a bit del disco original del DVR y colocarlo en el mismo, se lograra acceder. Si bien esas operaciones pueden dejar registros en la copia del

disco duro o en la memoria interna del DVR, en la dependencia analizada, estos cambios se documentan y justifican como cambios controlados que no afectan lo más importante; los videos y sus metadatos, por lo que se puede verificar la información obtenida con este método. Esta última metodología forense, el autor de referencia no lo recomienda, aunque lo da por válido.

También se destaca que, en las metodologías nombradas para acceder al DVR, Silva menciona que no se tuvo en cuenta la alternativa de acceder con el uso de fuerza bruta simple, es decir, prueba y error en los DVR que permitan hacerlo teniendo en cuenta la cantidad de intentos o reseteando la contraseña a partir de la investigación en portales web de las marcas fabricantes y/o contactando al proveedor del equipo [11].

Asimismo, se destaca que en los casos donde no se logró obtener los videos, incluso con el método con software forense, se debió a que las fechas solicitadas por los investigadores judiciales, no estaban grabadas en el HDD del DVR al momento de su análisis, esto concuerda con lo expuesto por la Acordada número 5/2022 del superior tribunal de justicia de Río Negro, ya que menciona que es posible que no se encuentren los videos de interés para la causa [20]. En tal caso indica que se extraigan los logs (registros de actividad) y se documente fotográficamente. Esto se fundamenta en razón a que estos equipos suelen funcionar sobrescribiendo el disco constantemente tal como lo indica Silva (2018), cuando un canal se queda sin espacio de bloque de metadatos mientras se escribe, el sistema de archivos asigna el siguiente bloque de metadatos disponible a ese canal, hasta el número máximo de bloques posibles en el HDD. Si no hay bloques disponibles en la partición, se utilizan los bloques de la siguiente partición. Si alguna de las particiones no tiene bloques, esa partición se sobrescribirá en modo de escritura cíclica [11].

Dentro de los aspectos que se pueden destacar respecto al objetivo de analizar los procedimientos que se llevan a cabo para la obtención forense de videos, es que en la tabla 1 se expuso una de las variables que demuestran que no todos los elementos ofrecidos como elementos de juicio, llegan al área con su correspondiente cadena de custodia. Se observó que solo en 4 de los 24 casos expuestos, fueron recibidos en el laboratorio informático con su correspondiente cadena labrada por el primer interventor. Orellano Benancio (2021) menciona que la Fiscalía envía a la oficina pericial la evidencia digital, rotulada con formato de cadena de custodia [14], tal como lo recomiendan las buenas prácticas forenses, sustentado en lo que dice Marqués Arpa, (2014), entre otros autores al respecto. No obstante, se destaca que, ante la falta de la cadena de custodia del DVR, se genera una cuando el mismo arriba a la dependencia, a fin de registrar quién es el responsable del elemento de juicio en cada instancia [21].

Otro de los aspectos a considerar es que al obtener los archivos de video estos pueden presentar un desfasaje entre el tiempo que evidencian los mismos y el horario real en que se grabó. Esto coincide con el trabajo de Ariffin, Slay y Choo (2013), donde dice que a la hora de proceder a identificar el DVR se verifique si existe correspondencia entre la hora real y la hora con la que fue configurado el aparato de acuerdo al timestamp y se fundamenta conforme a lo redactado en la Acordada Nº 005/2022 [20, 19].

Si bien el protocolo de la provincia de Río Negro anteriormente mencionado destaca algunos aspectos básicos y legales sobre el levantamiento de los videos en el lugar donde se encuentre el DVR, lo que se debe tener en cuenta tal como se demostró en este trabajo, son los tiempos y los volúmenes de información que se desean obtener, ya que existen diversas variables que no permitirán, por ejemplo, obtener la totalidad de los videos de un disco de 1 terabyte. Conforme la experiencia de los peritos en esta oficina, se desprende que, en la mayoría de los casos, colocar un disco externo de similar capacidad o incluso un soporte pequeño, como un pendrive de 16 gigabytes, puede no ser soportado por el sistema del DVR. Por lo que es muy beneficioso para estos casos contar con una dependencia que utilice en sus procesos softwares forenses para tal cometido. Es por ello que Silva (2018) concluye que, si bien se pueden cumplir con los requerimientos de la justicia sin contar con softwares pagos, realizarlos de forma rápida no será una opción. En todo caso siempre será ideal que el magistrado interviniente pueda delimitar o acotar el rango horario a extraer.

Para finalizar en cuanto a los objetivos de analizar los procedimientos y comparar los mismos, se destaca que existe una gran diferencia entre los tiempos de procesos de un método en comparación al otro. Los resultados de dicha observación se pueden evidenciar en la matriz de datos, en los gráficos y en la bibliografía citada que da cuenta que los procesos de adquisición forense de los videos de un DVR, pueden ser extensos y complejos. Por esta razón autores como Silva (2018) idearon un método para hacerse con los mismos basados en ingeniería inversa y con el uso del software DVR EXAMINER como el indicado para estas tareas. La desventaja puede radicar en el costo económico que significa adquirir la licencia y/o su mantenimiento anual [11].

La comparación que se realizó en iguales condiciones de trabajo en cuanto al volumen del disco duro inserto en el grabador digital y la cantidad de volumen de información (videos) a obtener, demuestra una marcada diferencia en los tiempos de trabajo. Es importante destacar que el tipo de exportación de vídeos de modo manual o tradicional exige que un operador esté ejecutando órdenes de descarga de videos de forma constante sobre el equipo. En cambio, en el modo con software forense, se lleva a cabo de forma automatizada, luego de indicar el periodo de tiempo a obtener. Podría considerarse que el proceso es aproximadamente 24,75 veces más rápido con el uso de DVR EXAMINER. Este cálculo surge de la división entre 396 / 16; siendo que 396 es el tiempo en horas, más largo registrado para la adquisición de la totalidad de los videos en un disco duro de 2 terabytes con el método tradicional, sobre el tiempo más largo registrado con el uso del software forense; 16 horas.

IV. CONCLUSIONES

Este estudio analiza los procedimientos de adquisición forense de videos en la División Análisis de Videos e Imágenes de Gendarmería Nacional. Los objetivos fueron:

1. Describir formas de obtención de videos en DVR.
2. Identificar problemas técnicos sin software forense.
3. Comparar procedimientos tradicionales con software forense. Metodología:

- Selección de 24 casos.
- Análisis de variables estudiadas.

Resultados:
- Diferencia sustancial en procesos con software forense.
- Mejora en eficiencia y calidad de la adquisición de videos.

Conclusión:
- Los peritos aplicaron conocimientos científicos para realizar un trabajo metódico, auditable y reproducible.
- El software forense mejoró significativamente los procedimientos de adquisición de videos.

Para finalizar se puede decir que es importante dentro de una organización pericial o investigativa, permitirse indagar, desarrollar y resolver experimentaciones controladas, sobre diversas cuestiones ligadas a la informática forense. Esto podría permitir, junto a tareas comprometidas en la proactividad y la mejora continua, no atrasarse en la carrera constante contra los delitos en el espacio digital, para finalmente brindar un producto comprometido con la verdad científica al servicio de la justicia.

REFERENCIAS

[1] L. Cortés Monsalve, A. Di Iorio y M. Lagos Enríquez, «Nuevas tecnologías en la investigación criminal: aportes de la informática a la criminalística y las ciencias forenses.,» 2020.
[2] M. Ardila Mejía, L. Ortiz Triviño y C. Villegas, «La importancia de cámaras de seguridad y la evidencia fílmica en el esclarecimiento de un hecho punible,» 2017. [En línea]. Available: https://repository.ugc.edu.co/items/7fcd647e-1425-43e1-be54-283d02c3b7c4.
[3] «Ley 14.172 Filmaciones y Grabaciones,» 08 11 2010. [En línea]. Available: https://normas.gba.gob.ar/ar-b/ley/2010/14172/11618.
[4] H. Granero, E. Molina Quiroga, G. Bielli, J. Resqui Pizarro, S. Toscano, L. Galmarini, L. Ramunno, J. Gasparini, S. Putschek, P. Romeo, G. Quadri, M. Abarrategui Fernández, J. Ordoñez, G. Aboso, C. Sueiro, G. Yuba, A. Quaranta y M. G. Pirota, E-Mails, chats, WhatsApps, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías: Validez probatoria en el proceso civil, comercial, penal y laboral, Buenos Airs: El Dial, 2019.
[5] M. A. Castellone, C. Bruno, H. Curti y J. Waimann, El rastro digital del delito: aspectos técnicos, legales y estratégicos de la informática forense, Buenos Aires: Universidad Fasta, 2017.
[6] L. Rodríguez Manzanera, Criminología, Buenos Aires: Porrúa, 2018.
[7] A. A. Di Iorio, La Informática Forense y el proceso de recuperación de información digital, Buenos Aires: Universidad Fasta, 2016.
[8] B. Carrier, File system forensic analysis, USA: Addison Wesley Professional, 2005.
[9] A. Ariffin, J. Slay y K. Choo, «Data Recovery from Proprietary Formatted Cctv Hard Disks,» de Advances in Digital Forensics IX. DigitalForensics 2013. IFIP Advances in Information and Communication Technology, vol. 410, Berlin, Springer, 2013, pp. 213-223.
[10] J. Rojas Campo, «DVR: qué son, tipos y cuáles son sus principales características,» 2024. [En línea]. Available: https://www.tecnoseguro.com/faqs/cctv/dvr-que-es-tipos-caracteristicas.
[11] G. Silva, «Ingeniería inversa del sistema de archivos de DVRs PCBox,» de XVIII Simposio Argentino de Informática y Derecho (SID) - JAIIO 47, Ciudad Autónoma de Buenos Aires, 2018.
[12] S. Sandeepa, A. Reyez y M. Silpa, «An Efficient Approach to Recover CCTV Video from Proprietary DVR File System,» de 2018 International CET Conference on Control, Communication, and Computing (IC4), Thiruvananthapuram, India, 2018.
[13] S. Sandeepa, A. Reyaz y N. Silpa, «An Efficient Approach to Recover CCTV Video from Proprietary DVR File System,» de International CET Conference on Control, Communication, and Computing (IC4), 2018.
[14] L. Orellano Benancio, «El uso de la pericia de identificación de la placa de rodaje vehicular y su relación con la calidad del video digital en los hechos delictivos de robo en la oficina de peritajes del Ministerio Público, Lima, 2019-2020,» 2021. [En línea]. Available: https://alicia.concytec.gob.pe/vufind/index.php/Record/UWIE_e33098f35f404b82794913f10eb69307
[15] D. Medina y M. Bejarano, «Análisis forense para Móviles,» Revista Avenir, vol. 4, nº 2, pp. 1-8, 2020.
[16] A. Valencia Álvarez, «Las pruebas digitales o electrónicas y sus desafíos jurídicos actuales,» Desafíos Jurídicos, vol. 2, nº 2, pp. 56-73, 2022.
[17] D. Dupuy y M. Kiefer, Cibercrimen. Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicios de Internet., Montevideo, Buenos Aires: Edigorial B de F, 2017.
[18] A. D. Airala y O. Rapetti, «A las puertas de una Nueva Especialización: La Informática Forense,» Segu Info, 30 10 2007.
[19] A. Ariffin, J. Slay y K. K. Choo, «Data Recovery from Proprietary Formatted Cctv Hard Disks,» Advances in Digital Forensics IX - IFIP Advances in Information and Communication Technology, pp. 213-223, 2013.
[20] Repositorio Institucional, «Acordada Nº 005/2022 - Protocolo de identificación y adquisición de videos de cámaras de seguridad generados en Grabador de Video en Red o Grabadora de Video Digital : Aprobación - Formulario de cadena de custodia de evidencia digital : Aprobación,» 25 04 2022. [En línea]. Available: https://digesto.jusrionegro.gov.ar/handle/123456789/13441. [Último acceso: 02 07 2022].
[21] T. Marqués Arpa y J. Serra Ruiz, «Cadena de custodia en el análisis forense: Implementación de un marco de gestión de la evidencia digital,» de RECSI XIII: actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información, Alicante, 2014.
[22] J. Cano, Computación Forense. Descubriendo los Rastros Informáticos, Bogotá, Buenos Aires, México: Alfaomega, 2016.
[23] A. Carrió, Garantías Constitucionales en el Proceso Penal, Buenos Aires: Hammurabi, 1984.
[24] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, USA: Academic Press Inc, 2011.
[25] Committee IT/012, Guidelines for the Management of IT evidence, Sydney: Standards Australia International, 2003.
[26] «Copia Forense,» 2022. [En línea]. Available: https://kripkit.com/copia-forense/.

Detección e Identificación de vehículos mediante técnicas de Inteligencia Artificial

Lic. E. V. Iglesias, *Esp. Informática Forense*

Alumno de Universidad Fasta. www.ufasta.edu.ar

***Resumen*—En esta investigación se entrenó un modelo de inteligencia artificial que detecta, rastrea e identifica vehículos en la vía pública. Para construirlo se utilizó como base el modelo YOLO y el algoritmo Deep-Sort.**

El modelo resultante logró mantener el rastreo de vehículos en diferentes oclusiones sobre los vehículos detectados y condiciones ambientales variables aun con un bajo resultado de sus métricas de evaluación. Permitiendo que en el caso de ser detectado e identificado el vehículo, el mismo pueda ser rastreado por el modelo de forma eficiente. Como derivado del desarrollo del modelo también se creó un dataset de vehículos que cotidianamente se ven en las calles de la República Argentina contiene 1769 imágenes etiquetadas para el sistema YOLO. Todo el trabajo en su conjunto representa un punto de partida para generar nuevos y mejores modelos con funcionalidades que escapan incluso a las desarrolladas en el presente trabajo de investigación.

I. INTRODUCCIÓN

Esta presentación se enfoca en la exposición del trabajo final integrador, construido para culminar la carrera de Especialista en Informática Forense, título de posgrado que brinda la Universidad FASTA.

Se pretende transmitir lo aprendido, mostrando al lector, de qué manera, al tomar como área de investigación la Inteligencia Artificial y en particular las redes neuronales artificiales convolucionales aprovechando las capacidades que estas redes nos ofrecen, poder crear un modelo ad hoc, que permita la identificación y rastreo de vehículos automotores exactamente como los que normalmente podemos observar en las calles de nuestra República Argentina. Todo esto con la esperanza de originar un punto de partida para un desarrollo más amplio, elevado y de calidad en esta área de estudio.

Para dar inicio podemos indicar que dentro del espectro de modelos de aprendizaje automático se encuentran aquellos que se crearon específicamente para imágenes y, por extensión, videos. Nos referimos a las redes neuronales convolucionales CNN (Convolutional Neural Networks).

Entender que las imágenes para estos algoritmos son matrices, o, con una denominación más apropiada, *tensores*, es entender por qué hablamos de convolución. Una imagen está compuesta por características de las cuales, en este campo, nos interesan su alto, su ancho en píxeles y su profundidad (cantidad de canales de colores). Aplicar una operación convolucional sobre la imagen es realizar operaciones matemáticas simples como la suma o la multiplicación escalar entre el tensor que conforma la imagen y un filtro que tiene pesos, lo que genera una nueva matriz a la cual se le aplica una función de activación y una capa de agrupamiento. Es muy útil para detectar características en las imágenes en principio elementos simples como líneas o bordes y conforme van pasando las capas convolucionales, se van descubriendo características cada vez más abstractas o de mayor nivel.

En el presente trabajo de investigación se realizó la construcción de un modelo de aprendizaje automático, mediante el uso del algoritmo YOLO en su versión 5, el cual permitió detectar vehículos, además, se los rastreo en su paso por el lente de la cámara mediante la incorporación de la lógica que ofrece el algoritmo DeepSort.

Utilizando YOLO y DeepSort mediante el lenguaje Python se entrenó un modelo propio *ad hoc*, cuya materia "prima" de entrenamiento se obtuvo de una serie de videos de cámaras de video vigilancia ciudadana. El objetivo del mismo es el de detectar, rastrear e identificar vehículos en la vía urbana, ofreciéndole a cualquier operario una herramienta que mejore el uso de los recursos humanos y tecnológicos para que se generen resultados de calidad y en menor tiempo en cualquier tipo de investigación con fines de seguridad pública. Sin prescindir del conocimiento y capacidades del operario.

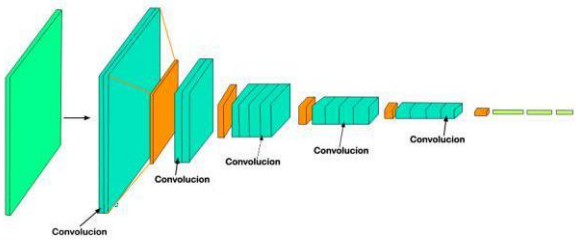


Fig. 1. Estructura simple de una CNN

Fig. 2. batch del proceso de validación de la red entrenada.

II. YOLO

Para lograr los objetivos de la investigación, se comenzó estudiando las redes neuronales artificiales en general, también su estructura y funcionamiento. Desde la primera descripción de una neurona desarrollada por Frank Rosenblatt en el año 1956 a través de su interpretación del *perceptrón* como las variables de pesos y función de activación Ref.[1]. Hasta las actuales redes de capas profundas.

Se estableció entonces la necesidad para abordar nuestro objetivo utilizando una subcategoría del machine learning e inteligencia artificial denominado aprendizaje maquina supervisado. Este enfoque requiere de datos etiquetados para entrenar modelos que los clasifican a través de algoritmos que miden la precisión de las detecciones predichas a través de la función de perdida, ajustándose hasta que el error es mínimo.

Dentro del conjunto de modelos que existen, se optó por la familia de modelos YOLO Ref.[2] que se encuentran disponibles para cualquier usuario que requiera utilizarlos. Actualmente estamos en la versión 10 de YOLO. Ya hace mucho tiempo que su principal autor Joseph Redmon dejo de ser participe principal de las mejoras y modificaciones que se fueron implementando, siendo su última participación en la versión 3 de YOLO. Desde esa versión a la fecha el modelo sufrió cambios que atendieron a diversas necesidades de la comunidad y nuevos desarrolladores, desde modelos de negocio tales como modelos industriales a otros tipos. Sin embargo, hay una versión que a consideración de este investigador es la adecuada para este trabajo tanto por su estabilidad como sus prestaciones y esa es la versión 5 de YOLO.

A. *You Only Look Once – v5*

La versión 5 ofrece una amplia variedad de modelos con los cuales trabajar desde los denominados modelos *nano*, tales como YOLOv5n hasta modelos *extra large* como YOLOv5x, para imágenes de entrada de 640 pixeles o sus homólogos YOLOv5n6 a YOLOv5x6 para imágenes de entrada de 1280 pixeles y en caso de usar TTA (test time augmentation) hasta 1536 pixeles.

Por supuesto que la elección de un modelo u otro no es tan sencilla como pensar “tomo el mejor”, hay que tener en cuenta nuestras limitantes de hardware ya que esto es un factor determinante al momento de seleccionar modelos.

En este trabajo se utilizó el modelo YOLOv5m o *médium* elección que no se realizó a la ligera sino, que fue el resultado de evaluar los modelos YOLOv5n y YOLOv5s con rendimientos muy bajos a los fines requeridos y el modelo YOLOv5l superior inmediato del elegido, el cual no se logró aprovechar de forma satisfactoria con el hardware disponible. Por otro lado, esta elección tuvo un costo no menor en la aleatoriedad de elección de los *batchs* y *epochs* a utilizar en el entrenamiento del modelo ad hoc. Optando por aplicar 16 batch bajo el criterio de mejorar la generalización mediante actualizaciones más frecuentes y tomar 100 epochs bajo el criterio de darle mas tiempo de entrenamiento al modelo tanto en el aprendizaje como en la modificación de pesos.

B. *Funcionamiento de YOLO.*

La función inicial de este modelo es “detectar de una sola pasada”, para lograrlo utiliza cuadriculas de dimensiones s x s si el centro del objeto de interés que se busca detectar se ubica dentro de alguna de las celdas. Esa celda en cuestión es la encargada de detectar el objeto. Para lograr esta detección cada una de las celdas en la cuadricula predice los cuadros delimitadores conocidos como boundingboxes, su dimensión y la puntuación de confianza. La ecuación general para realizar esta tarea es la siguiente:

$$puntuacion\ de\ confianza = p(objeto) * IoU \frac{verdad}{prediccion} \quad (1)$$

Cuanto más alto es el valor resultante de esta ecuación más seguro se encuentra el modelo que dentro del boundigbox existe el objeto detectado. Sin embargo, el ejecutarse esta tarea se generan múltiples boundingboxes, lo cual provoca caos de detecciones en la imagen. Y la forma de tratar este problema mediante YOLO es utilizar el concepto de supresión de no máximo o NMS, mediante valores de umbral (treshold) que de acuerdo a su valor nominal eliminan cuadros que no contienen detecciones, logrando esto mediante el uso de la función de perdida.

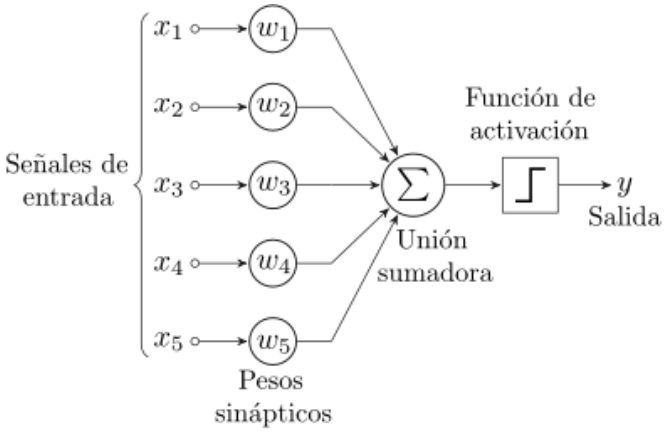


Fig. 3. Perceptrón – red neuronal mas simple que se acepta.

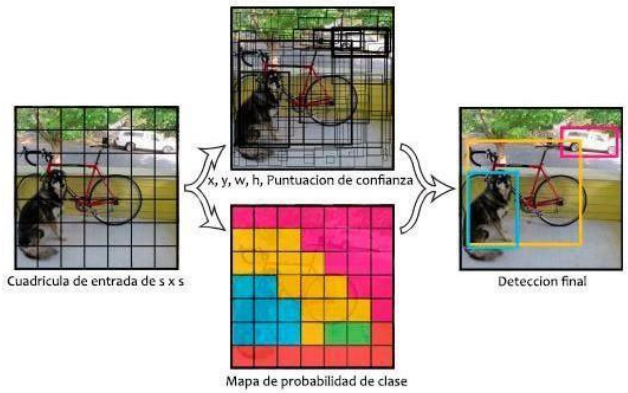


Fig. 4. Proceso de detección de YOLO.

III. DEEP-SORT

A continuación, para avanzar en la obtención de conocimiento se estudiaron algoritmos de rastreo de objetos, eligiendo DeepSort como el algoritmo de uso por su facilidad y rápida implementación, además de la capacidad de ser un MOT (multiple object tracking). Este algoritmo, vino a completar el requerimiento del trabajo de investigación en cuanto al "rastreo" de vehículos y también en beneficio de la identificación al asignar un identificador único a cada detección que obtiene.

Históricamente podemos decir que fue desarrollado por Nicola Wojke, Alex Bewley y Dietrich Paulus en el año 2017 Ref.[3] con la intención de sus desarrolladores en mejorar el rastreo de objetos manteniendo el ID (identificador único) de la detección por periodos mas largos en las oclusiones. Para lograrlo tomaron toda la estructura del algoritmo SORT Ref.[4]. y le incorporaron una métrica de asociación profunda que combina información de movimiento con información de apariencia. Sus autores indican que aplicaron una red neuronal convolucional entrenada para discriminar peatones y que mediante la aplicación de esa red aumentaron la robustez frente a fallos y oclusiones.

A. Desafío del algoritmo.

DeepSort tiene como fin ampliar las funcionalidades del algoritmo SORT pero también al igual que su predecesor, el desafío principal es lograr la re identificación de una detección de forma correcta. Lo que permite al observador estar seguro de que el objeto detectado es el mismo a lo largo de todo el video.

En este trabajo en concreto la necesidad se corresponde en asociar un rastreo a un único vehículo, a medida que se mueve por el plano de visión de la cámara. Movimiento que puede ser de forma lineal o no, lo cual puede generar cambios en la forma del mismo, ya sea por la velocidad, el cambio de dirección del vehículo, una obstrucción generada por la superposición de un objeto delante del vehículo rastreado, etc. Esto obliga a darle mayor importancia a las características utilizadas para rastrear el vehículo.

B. Repositorio elegido.

Luego de analizar el repositorio que los autores de DeepSort ofrecen y entender que para obtener las capacidades que los mismos indican se valieron de una red neuronal convolucional entrenada offline, con dataset de peatones. Resultó necesario hacer lo mismo. Se generó una nueva red de apariencia para vehículos, pero por una cuestión de temporalidad y métricas resultantes. Se optó por finalizar el trabajo con un repositorio ya desarrollado para detectar peatones y vehículos Ref. [5]. Al cual se le realizaron algunas modificaciones para que permita aplicar los requerimientos iniciales de este trabajo.

IV. MODELO AD HOC

Se tomaron los videos de cámaras de vigilancia ciudadana distribuidas en la ciudad de San Luis. Cada uno de estos videos cuenta con un promedio de 2 horas de grabación.

La primera tarea consistió en la extracción y procesamiento de las imágenes contenidas en los videos es decir en cada uno de sus frames, que contengan la presencia de vehículos automotores pasibles de ser etiquetados bajo la premisa de "automotor presente". Para ello utilizamos VLC media player [https://www.videolan.org/vlc/index.es.html] con la que se extrajo cada una de las imágenes que representan los frames de los videos, para luego almacenarlos en formato Joint Photographic Experts Group (JPG).

Como resultado se obtuvieron un total de 1 483 053 imágenes. Este número sin embargo es muy elevado para la capacidad humana disponible y material de procesarlas a todas de forma manual, por lo que se tomó la decisión de realizar recortes en los videos originales con los que se inició, utilizando la misma herramienta VLC media player, con la que se logró extraer porciones de videos que contenían la premisa impuesta y descartando aquellos espacios de tiempo donde no se observan o se consideran innecesarios atento a las características observadas.

Como resultado, se lograron obtener un total de 24 recortes de video, a los cuales se les extrajo las imágenes contenidas, utilizando la misma herramienta ya mencionada. Para luego analizar cada uno de los frames obtenidos, en busca de aquellos donde se pudieron observar con detalle las características de los vehículos representadas por su marca, modelo y elemento distintivo. Buscando distintos ángulos de captura, es decir obtener distintas imágenes del mismo vehículo en posiciones espaciales diferentes sobre una misma cámara y en cámaras distintas, teniendo especial atención a los diferentes escenarios ambientales y circunstancias viales tales como: bloqueos parciales o totales que los vehículos puedan sortear al desplazarse por el campo de visión que presenta el lente de la cámara. Toda esta tarea se practica de forma manual y visual por parte del investigador lo que arroja como resultado luego de procesar las imágenes, un conjunto de 1 769 imágenes que contienen las características buscadas en los vehículos que se consideran necesarias para su utilización en el entrenamiento del modelo.

Ya con las imágenes procesadas, se realizó la actividad de etiquetado utilizando los datos de las diferentes marcas y modelos que se pueden observar en los vehículos de la vía pública en cualquier provincia argentina como características relevantes.

Para etiquetar se utilizó el programa LabelImg, escrito en Python, el cual mediante una interfaz gráfica creada con la librería PyQt, permite al operador llevar adelante esta tarea.

El resultado de la actividad de etiquetado fue la obtención de un archivo llamado "classes.txt" generado por el programa, que contiene un total de 119 etiquetas de vehículos, cuyos nombres fueron dados por el investigador con la configuración de marca y modelo, ejemplo: *Peugeot_Partner*.

Fig. 5. Interfaz gráfica de LabelImg.

Para el caso particular de las bicicletas y motos, se optó por generalizar la etiqueta con la salvedad de identificar si el ciclista y/o motociclista llevaba puesto o no el casco, ejemplo: *Motociclista_conCasco*, *Ciclista_sinCasco*. Además, se obtuvo cada uno de los archivos de imágenes con su respectivo archivo de texto que contiene las coordenadas etiquetadas dentro de las imágenes donde se identificaron vehículos.

A. Entrenando el modelo

Como práctica estándar al entrenar modelos de Inteligencia Artificial, del total de las imágenes se tomó un grupo conformado por el 75% del total para el entrenamiento y un segundo grupo conformado por el 25% para la validación. Esta no es una regla, pero es una práctica común.

A continuación se creó el archivo "*dataset.yaml*", mediante el cual se trata y describe la información de entrenamiento y de prueba, estableciendo una estructura mediante rutas, números de clase y nombres de clase. El archivo creado en esta investigación contiene los siguientes datos:

train: dataset/images/train Es la ruta a las imágenes de entrenamiento.

val: dataset/images/val Es la ruta a las imágenes de validación.

nc: 118 Es el número de clases, que representa las 119 etiquetas al iniciar en 0.

names: Que contiene todas las etiquetas construidas con marcas y modelos de vehículos.

B. Hardware y Software utilizado

Para entrenar y validar el modelo se utilizó hardware propio. Específicamente, se utilizó una PC de escritorio con microprocesador Intel i7-4790k, con 8 GB de memoria RAM y una tarjeta gráfica Nvidia GTX970 de 4 GB de procesamiento.

Como base de trabajo se utilizó Visual Studio Code, mediante un entorno virtual y todas las librerías necesarias para hacer de Pytorch nuestro marco de trabajo.

C. Métricas

Se tomó como métricas representativas las curvas F1 de entrenamiento y validación, la matriz de confusión, la curva P, la curva PR y la curva R. las cuales en su conjunto ofrecieron una realidad sobre las capacidades del modelo.

Tanto la curva F1 del conjunto de entrenamiento como la curva F1 del conjunto de validación, tuvieron solo una milésima de diferencia en el valor de confianza que devolvieron como resultado al evaluarse sobre el modelo.

Así mismo de la matriz de confusión se determinó que las clases "*Toyota_Hilux*", "*Colectivo*", "*Fiat_Uno*", "*Peugeot_207*" y "*Fiat_Qubo*" fueron las clases en las que el modelo realizó mejores predicciones correctas e incorrectas. Mientras que tuvo mayores errores de predicción con la mayoría de las clases restantes, siendo las clases más afectadas aquellas en las que se contaba con menor cantidad de imágenes representativas.

De la curva P se logró extraer, que para que una predicción sea confiable en las detecciones de verdaderos positivos, la probabilidad tenía que ser de 0.954, lo cual es claramente muy exigente.

La curva PR informa que el modelo es de bajo rendimiento en términos relativos con solo un 18.6% de precisión al 0.5 de umbral IoU. Finalmente, la curva R informo que el modelo es capaz de recuperar el 77% de las detecciones positivas reales con 0.0 de confianza y disminuye significativamente a medida que se requiere más confianza, resultando que a 0.5 de confianza la recuperación de detecciones positivas reales es alrededor del 15%.

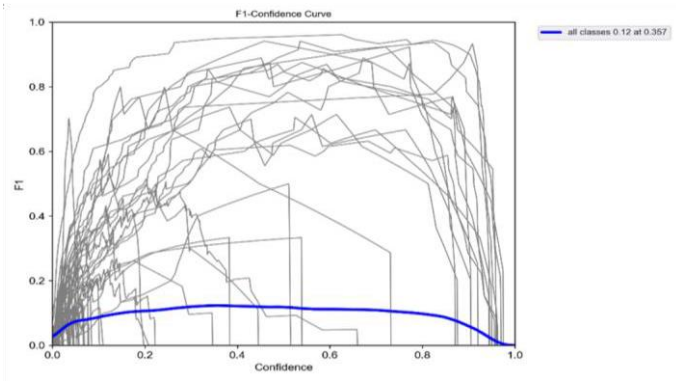


Fig. 6. Curvas F1 de validación.

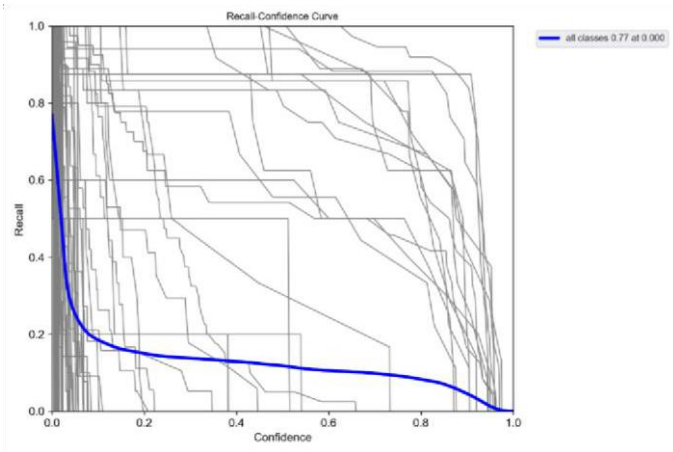


Fig. 8. Curva R.

Fig. 9. Batch de entrenamiento.

Fig. 10. Batch de validación.

Una vez que contamos con el modelo de detección, se realizó la re identificación de vehículos para poder hacer uso del rastreo proporcionado por DeepSort. Sin embargo, esta tarea no se concluyó a tiempo y extendía los requerimientos del trabajado final de carrera por lo cual se tomó la decisión de tomar un repositorio Github, que ya contaba con la integración de YOLOv5 y DeepSort ver Ref. [5]. A este repositorio se le realizaron modificaciones en el script principal "main.py", se le cambio el uso por defecto que hacía mediante el parser *"– weights"* para que tome el modelo entrenado ad hoc, se modificó draw.py para que grafique los bounding boxes con el nombre de los vehículos por marca, modelo y nivel de confianza de la detección. Se corrieron los videos de prueba obteniendo como resultado nuevos videos con los vehículos rastreados.

CONCLUSIONES

En el trabajo se llevó a cabo el diseño e implementación de un modelo de aprendizaje automático que detecta y rastrea vehículos. Uno de los objetivos del trabajo es que se tome como base para el desarrollo de mejoras o para la creación de nuevos modelos de detección y rastreo de vehículos en la vía pública mediante cámaras de seguridad, tanto públicas como privadas.

Sin lugar a dudas, se logró construir y evaluar un modelo de aprendizaje automático cuyo propósito es detectar y rastrear vehículos que habitualmente transitan por calles y rutas de la República Argentina. Durante el transcurso del proceso de investigación, se encontró con diversas dificultades técnicas que se describen a continuación con el fin de que el lector pueda aprovechar el conocimiento adquirido y mejorarlo.

Al momento de seleccionar la herramienta de procesamiento para entrenar el modelo y posteriormente validarlo, se consideró utilizar Google Colab, un servicio que puede entrenar el modelo mediante un notebook virtual. Esta herramienta ofrece más de 50 horas de tiempo de ejecución, 12 GB de memoria RAM y más de 100 GB de espacio en disco de forma gratuita; sin embargo, también advierte en su documental que esto "no está garantizado". Esta última afirmación fue valorada por el investigador. Por lo cual se tomó un video de prueba, obtenido de internet y ajeno a esta investigación, para procesarlo y utilizarlo con el fin de "testear" Google Colab y su rendimiento. Sin embargo, al transcurrir el tiempo y ejecutar el proceso, se encontraron fallas en los tiempos de ejecución, disminuciones en la cantidad de memoria y cortes inesperados debido a la conexión de red. Estas circunstancias unidas al hecho de tener que subir la información a la nube fueron los elementos decisivos para descartar el uso de esta herramienta y de otras similares como AWS, Azure o Kaggle.

Por lo que se decidió realizar el entrenamiento mediante una PC de escritorio propia, con los recursos de hardware ya descritos en la presente investigación. Lo que permitió al investigador mantener el control total del proceso desarrollado. Esta elección debe considerarse correcta, especialmente en investigaciones judiciales, ya que no es recomendable subir videos que puedan contener elementos de interés pericial a servicios de terceros en la red.

La implementación del modelo y su evaluación permitieron comprender que, con el hardware disponible, habiendo evaluado todas las métricas, el hardware resulta insuficiente para obtener un modelo que cuente, por ejemplo, con un alto valor de equilibrio entre precisión y recuperación de detecciones si consideramos las curvas F1. Por lo cual se recomienda a futuros investigadores, contar con un hardware mínimo de 64 GB de RAM, una GPU RTX 3090, un microprocesador Ryzen 9 o i9, y suficiente espacio en disco, dado que los videos son datos de gran volumen. Con la finalidad de obtener resultados que sean extrapolables a la realidad cotidiana con el efecto deseado.

Así mismo y mediante las evaluaciones sobre los resultados arrojados por la matriz de confusión, se logró establecer que ciertas etiquetas, como *Toyota_Hilux*, Colectivo, *Fiat_Uno*, *Peugeot_207* y *Fiat_Qubo*, presentan más predicciones correctas e incorrectas.

Concluyendo esta investigación, que se debe a dos componentes fundamentales. El primero es el número de datos de entrenamiento, es decir, la cantidad de vehículos etiquetados de la misma marca y modelo; y en contraste, el segundo componente, como lo son en el presente caso las etiquetas *Colectivo* y *Fiat_Qubo*, ocurrieron debido a la forma característica (física) de estos vehículos, que les permite diferenciarse del resto de los evaluados por el modelo de forma significativa, conjuntamente con la particularidad de que al momento del entrenamiento la cantidad de vehículos de estas características etiquetados era la de más bajo número en el conjunto considerado.

Como se observó en las métricas reportadas y en las imágenes de ejemplo de los videos resultantes que fueron plasmadas con anterioridad, el modelo presenta un bajo nivel de detección y rastreo; sin embargo, una vez que el vehículo es detectado y rastreado, el modelo mantiene el seguimiento en diversas condiciones ambientales y con obstrucciones en los lentes de las cámaras a lo largo de los cuadros del video. Esto es un indicador suficiente de que el proyecto es viable si se aumenta el número de datos de entrenamiento, se incrementa el tamaño de las conexiones entre neuronas del modelo YOLO elegido y se emplea un hardware lo suficientemente robusto para entrenarlo y validar sus resultados.

Finalmente, se considera que el "dataset" creado para esta investigación, es un elemento valioso para la comunidad científica, por lo cual se pretende robustecerlo, ampliando el número de clases y etiquetas, para luego ponerlo a disposición de la comunidad, brindando un elemento útil y de interés para investigadores.

REFERENCIAS

[1] Frank Rosenblatt, Año 1958. “The Perceptron”.

[2] Ultralytics “Computer Vision Company AI” especializada en el estado del arte de los modelos de deteccion de objetos, con foco en la familia YOLO.
Recuperado de https://docs.ultralytics.com/yolov5/#explore-andlearn

[3] Nicolai Wojke, Alex Bewley, Dietrich Paulus. Año 2017 “Simple Online and Realtime Tracking With a Deep Association Metric,”

[4] A. Bewley, G. Zongyuan, F. Ramos, and B. Upcroft, “Simple online and realtime tracking,” in ICIP, 2016, pp. 3464–3468.

[5] Repositorio archivado a la actualidad por su propietario se puede ver en https://github.com/HowieMa/DeepSORT_YOLOv5_Pytorch

[6] Muhammad Hussain Año 2023, “Yolo-v1 to Yolo-v8, The Rise of Yolo and Its Complementary Nature Toward Digital Manufacturing and Industrial Defect Detection“.Recuperado de https://www.researchgate.net/publication/371875367_YOLOv1_to_YOLO-v8_the_Rise_of_YOLO_and_Its_Complementary_Nature_toward_Digital_Manufacturing_and_Industrial_Defect_Detection

[7] Pagina oficial IBM “Que son las Redes Neuronales Convolucionales”. Recuperado de https://www.ibm.com/es-es/topics/convolutional-neuralnetworks

[8] Zhao, X., Wang, L., Zhang, Y. et al. Año 2024, “A Review of Convolutional Neural Networks in Computer Vision”. Recuperado de https://doi.org/10.1007/s10462-024-10721-6

[9] Alan M Turing – octubre de 1950 “Computing Machinery and Intelligence”.
Recuperado de https://doi.org/10.1093/mind/LIX.236.433

[10] Conferencia de Dartmouth. Año 1955. Recuperado de http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf

[11] James Moor Año 2006 “The Dartmouth College Artificial Intelligence Conference: TheNext Fifty Years”.
Recuperado de https://www.researchgate.net/publication/220605256_The_Dartmouth_College_Artificial_Intelligence_Conference_The_Next_Fifty_Years

[12] Sergey Ioffe, Christian Szegedy – febrero de 2015 “Batch Normalization: Accelerating Deep Network Training By Reducing Internal Covariate Shift”.
Recuperado de https://arxiv.org/abs/1502.03167

[13] Vaibhav Rastogi Año 2003 "Max Pooling Layer In Computer Vision". Recuperado de https://medium.com/@vaibhav1403/max-pooling-layerin-computer-vision-8cccfd91c521

[14] Warren S. McCulloch and Walter Pitts Año 1943 “A Logical Calculus Of The Ideas Immanent In Nervous Activity”. Recuperado de https://www.cs.cmu.edu/~./epxing/Class/10715/reading/McCulloch.and.Pitts.pdf

Fundamentos de la Metodología de análisis y resguardo de potenciales elementos de prueba digital asociados a Criptomonedas y Criptoactivos

Cintia V. Gioia, Emiliano A. Zárate, Serena R. Donato, Mario J. Krajnik, Jorge E. Eterovic

Universidad Nacional de La Matanza (UNLaM), Buenos Aires, Argentina
cgioia@unlam.edu.ar, ezarate@unlam.edu.ar, srdonato@unlam.edu.ar, mkrajnik@unlam.edu.ar, eterovic@unlam.edu.ar

***Resumen*— La Informática Forense aplicada a la tecnología de blockchain y específicamente a las criptomonedas y criptoactivos en general, involucra poseer los conocimientos y herramientas necesarias para encarar una pericia informática como parte de un proceso o investigación judicial, lo cual, posibilita seguir la historia de las transacciones en la cadena de bloques de las principales criptomonedas y otros criptoactivos. Se plantean los fundamentos del diseño de una metodología integral para el análisis y resguardo de posibles elementos de prueba digital asociados a criptomonedas y criptoactivos, la cual fortalece la eficacia y la confiabilidad de los procedimientos forenses a aplicar en pericias informáticas que forman parte de procesos o investigaciones judiciales, asegurando que se generen resultados técnica y legalmente válidos.**

***Abstract*—Forensic Informatics applied to Blockchain technology, and specifically to cryptocurrencies and crypto-assets in general, involves possessing the knowledge and tools required to conduct a digital forensic examination as part of a judicial process or investigation. This enables the tracing of transaction histories within the blockchain of major cryptocurrencies and other digital assets. The paper presents the foundations for designing a comprehensive methodology for the analysis and preservation of potential digital evidence related to cryptocurrencies and crypto-assets. This methodology strengthens the effectiveness and reliability of forensic procedures applied in digital investigations that are part of judicial processes, ensuring that the results obtained are both technically and legally valid.**

I. INTRODUCCIÓN

El desarrollo y la masiva adopción a nivel global, del uso de Internet, de computadoras personales, dispositivos móviles, servicios y plataformas asociadas, ha tenido un vasto impacto sobre la velocidad y naturaleza de las interacciones sociales, del que no están exentos las transacciones comerciales o financieras. Una de las manifestaciones de la transición de la actividad humana desde el mundo físico al virtual ha sido el surgimiento de activos virtuales (AV), entendidos, conforme la definición del Grupo de Acción Financiera Internacional (GAFI[1]), como una representación digital de valor que puede ser intercambiada o transferida digitalmente, y utilizada como forma de pago o instrumento de inversión. En este escenario, el desarrollo más importante ha sido, sin dudas, la creación de las criptomonedas, que desde su nacimiento en 2008 - con la publicación del célebre "White paper" de Satoshi Nakamoto sobre el Bitcoin - se convirtieron en uno de los mercados no regulados más grandes del mundo.

La aparición de las criptomonedas[2], los criptoactivos[3] y de la tecnología de Blockchain[4], constituye un fenómeno que bien puede estar llamado a revolucionar positivamente muchos aspectos del sistema financiero. Pero como muchas innovaciones, también es susceptible de ser explotada para favorecer la actividad ilícita, los cuáles deben ser abordados desde la Forensia Digital.

La tecnología de Blockchain es la tecnología sobre la que se sustentan las criptomonedas y criptoactivos. En términos similares, la Unidad de Información Financiera (UIF)[5], en su resolución 300/2014 "Prevención del Lavado de Activos y de la Financiación Del Terrorismo" [1] definió a las "Monedas Virtuales" como la representación digital de valor que puede ser objeto de comercio digital y cuyas funciones son la de

[1] GAFI (Grupo de Acción Financiera Internacional) es un organismo intergubernamental creado en 1989 por el G7 para establecer estándares y promover políticas destinadas a prevenir el lavado de dinero, la financiación del terrorismo y otras amenazas al sistema financiero global.

[2] Criptomonedas: activos digitales que funcionan como medio de intercambio, basados en criptografía para asegurar las transacciones y controlar la creación de nuevas unidades.

[3] Criptoactivos: categoría más amplia que incluye a las criptomonedas y otros activos digitales tokenizados que representan valor, derechos o bienes en entornos digitales.

[4] BlockChain: tecnología de registro distribuido que almacena transacciones en bloques enlazados y verificables, garantizando transparencia, trazabilidad e inmutabilidad de la información.

[5] UIF: organismo del Estado argentino encargado del análisis, tratamiento y difusión de inteligencia financiera para prevenir el lavado de activos, la financiación del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.

constituir un medio de intercambio, y/o una unidad de cuenta, y/o una reserva de valor, pero que no tienen curso legal, ni se emiten, ni se encuentran garantizadas por ningún país o jurisdicción. En ese sentido, la UIF diferenció a las monedas virtuales del "dinero electrónico", entendido este último como un mecanismo para transferir digitalmente monedas fiduciarias, es decir, mediante el cual se transfieren electrónicamente monedas que tienen curso legal en algún país o jurisdicción. Se define como activo virtual, a una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar con fines de pago o inversión, los cuales no incluyen representaciones digitales de monedas fiduciarias.

Las blockchains públicas y privadas se diferencian por su nivel de acceso y control. Las blockchains públicas —como Bitcoin o Ethereum— son redes abiertas, descentralizadas y transparentes, donde cualquier usuario puede participar, validar transacciones y auditar el registro histórico. En cambio, las blockchains privadas restringen el acceso a un conjunto limitado de nodos autorizados, generalmente bajo el control de una organización o consorcio, lo que permite mayor gobernanza, privacidad y eficiencia transaccional, pero reduce la descentralización y la verificabilidad pública de los datos.
Durante la última década, los activos virtuales, en especial las criptomonedas, han pasado a ocupar un lugar central como moneda de cambio en las transacciones ilícitas realizadas, sobre todo, en los mercados ilegales que operan en Internet.

Los principales rasgos que incrementan el riesgo de lavado de dinero y financiación del terrorismo son el anonimato asociado al diseño de los activos virtuales, la posibilidad de que una misma persona controle múltiples "monederos virtuales", el carácter descentralizado de la mayoría de las criptomonedas y el alcance global de muchas de ellas, entre otros. Esto derivó en que se recurriese a las criptomonedas para facilitar el surgimiento de mercados online en la "Dark Web" o "Red oscura" de Internet, en los que hasta el día de hoy se intercambian bienes y servicios (en su mayoría) ilegales a cambio de criptomonedas.

En este escenario de creciente digitalización y expansión de los activos virtuales, se vuelve esencial abordar su impacto desde una perspectiva integral que articule los planos tecnológico, jurídico y forense. El desarrollo del ecosistema cripto ha promovido la creación de nuevos instrumentos financieros y sistemas descentralizados de intercambio, pero también ha introducido desafíos relevantes para las instituciones encargadas de la regulación, la supervisión y la investigación del delito. La combinación entre anonimato, descentralización y alcance global genera un entorno complejo que demanda metodologías especializadas para garantizar la trazabilidad, integridad y validez probatoria de la evidencia digital asociada a estos activos.

La adopción de criptoactivos en Argentina y en el mundo continúa en crecimiento, expandiéndose más allá del uso financiero tradicional y generando nuevos desafíos en materia de trazabilidad, regulación y análisis forense digital. Su expansión trasciende el ámbito del resguardo o reserva de valor: los criptoactivos se utilizan como medio de pago para bienes y servicios, instrumento de inversión, canal de remesas internacionales, mecanismo de financiamiento descentralizado (*DeFi*)[6] y soporte tecnológico para la ejecución de contratos inteligentes[7] y la tokenización de activos digitales[8]. Este patrón, junto con la alta presencia de exchanges[9] centralizados en la región, impulsa la masificación de su uso y genera nuevas superficies de investigación y fuentes de información relevantes para la trazabilidad. Al mismo tiempo, su infraestructura puede ser explotada en esquemas ilícitos —como fraude, *ransomware*, lavado de activos y evasión fiscal— que demandan capacidades específicas de análisis forense digital y cooperación interinstitucional e internacional.

II. DESAFÍOS PERICIALES EN EL ANÁLISIS DE CRIPTOMONEDAS Y CRIPTOACTIVOS

A nivel nacional e internacional, aún no se han consolidado metodologías ni procedimientos específicos que faciliten el trabajo pericial o unifiquen criterios técnicos en el tratamiento de potenciales elementos de prueba digital asociados a criptomonedas y criptoactivos. En tal sentido, las evidencias vinculadas con el uso de criptoactivos se suman como una nueva categoría de elementos que se deben identificar, tanto en el lugar del hecho como en los laboratorios forenses donde se examinan computadoras, unidades de almacenamiento, teléfonos móviles y tabletas, entre otros, para luego poder realizar un análisis forense sobre los mismos.

La investigación criminal ligada a los criptoactivos cobra un rol preponderante. Investigar actividades delictivas relacionadas con criptoactivos puede resultar complejo, ya que muchos casos podrían estar vinculados con compras realizadas o fondos transferidos a través de la cadena de bloques. Por lo tanto, resulta vital comprender con precisión cómo se preparan, transmiten, procesan y almacenan estas transacciones.

Se plantean algunos de los siguientes desafíos: el análisis forense de billeteras físicas o digitales en el sitio (ubicación física), secuestro de criptoactivos, cómo encontrar evidencia en teléfonos móviles y computadoras portátiles y de escritorio, qué métodos aplicar para investigar y realizar análisis forenses de forma remota (usando conexión a Internet) de varias direcciones de criptomonedas maliciosas de la vida real,

[6] Financiamiento descentralizado (DeFi): conjunto de aplicaciones y servicios financieros basados en tecnología blockchain que operan sin intermediarios tradicionales (como bancos o entidades financieras) mediante contratos inteligentes (smart contracts). Permiten ejecutar préstamos, depósitos, intercambios y otros instrumentos financieros de forma automatizada y transparente.

[7] Contrato inteligente (smart contract): programas ejecutados en *blockchain* que automatizan y hacen cumplir condiciones pactadas entre partes sin intermediarios. Se despliegan como código inmutable, se activan ante disparadores definidos y registran sus resultados on-chain, aportando transparencia, trazabilidad y ejecución determinística

[8] Tokenización de activos digitales: proceso mediante el cual un activo físico, financiero o virtual se representa como un *token* dentro de una red *blockchain*. Este token digitaliza el valor o los derechos asociados al activo, posibilitando su fraccionamiento, transferencia y registro seguro en un entorno distribuido y trazable.

[9] Exchanges (casas de intercambio de criptoactivos): plataformas digitales que permiten la compra, venta, conversión y custodia de criptomonedas y otros criptoactivos. Pueden operar de manera centralizada (CEX) bajo la gestión de una entidad que intermedia las transacciones o descentralizada (DEX), donde las operaciones se realizan directamente entre usuarios mediante contratos inteligentes sobre blockchain.

permitiendo rastrear sus transacciones haciendo uso de software libre, entre otros.

Un obstáculo adicional a la hora de requerir información de empresas proveedoras de servicios de intercambio o compraventa de criptoactivos a través de internet es que, por la naturaleza y entorno digital de su negocio, esas empresas podrían estar constituidas y operar en jurisdicciones extranjeras, con lo cual el acceso a este tipo de información y evidencia digital puede resultar más complicado.

La naturaleza pública o privada de una blockchain tiene implicancias sustanciales en la investigación judicial y forense digital.

En las blockchains públicas, la información sobre transacciones y direcciones es abierta, verificable y accesible sin autorización judicial internacional, lo que facilita la trazabilidad de operaciones y el análisis de patrones de flujo mediante herramientas de recopilación y análisis de información disponible públicamente o plataformas de análisis y trazabilidad. No obstante, la pseudonimización de las direcciones impone el reto de vincularlas con identidades reales.

En las blockchains privadas, la visibilidad de los datos depende de los permisos definidos por la entidad administradora, por lo que el acceso a la información requiere cooperación directa con el operador o la autorización judicial correspondiente. Esto puede limitar la transparencia y dificultar la obtención de evidencia digital si la red no garantiza mecanismos auditables de registro y validación.

En síntesis, las blockchains públicas ofrecen mayor trazabilidad técnica, mientras que las privadas ofrecen mayor control institucional, lo que determina estrategias forenses diferenciadas para la recolección y validación de pruebas digitales.

III. Estado actual del conocimiento

En 2021, el Grupo de Acción Financiera de Latinoamérica (GAFILAT[10]) publicó la "*Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales*" [2], La misma tiene como propósito brindar a las autoridades de orden público herramientas para la recuperación de activos delictivos y la cooperación internacional, fortaleciendo sus capacidades para solicitar, investigar e identificar activos virtuales. Además, promueve el desarrollo de habilidades para la identificación, incautación y decomiso de activos ilícitos vinculados al lavado de dinero y la financiación del terrorismo en América Latina, por parte de unidades fiscales, fuerzas de seguridad y agencias de investigación. También advierte sobre las herramientas que utilizan los criminales para obstaculizar la acción de las autoridades y sus consecuencias. Aunque la guía no es de alcance nacional, sino regional —dado que GAFILAT reúne a 17 países de América del Sur, Centroamérica y América del Norte—, su aporte resulta de gran valor para todos los Estados miembros. La guía no profundiza sobre lo referido a análisis forense de las actividades delictivas con activos virtuales. Si bien facilita la cooperación internacional, necesita poder analizarse y adaptarse a marcos legales nacionales y a los avances tecnológicos.

En Argentina, se han producido avances regulatorios recientes, entre ellos la creación del Registro de Proveedores de Servicios de Activos Virtuales[11] (Registro PSAV) por parte de la Comisión Nacional de Valores (CNV), mediante la Resolución General 994/2024 [3] (artículo 4 de la Ley 27.739). Dicho registro está orientado a supervisar y transparentar las operaciones vinculadas con criptoactivos. La Resolución 994/2024 es de interés para que la Argentina pueda cumplir con los estándares fijados en "*Las 40 Recomendaciones de la GAFI*"[12] [4], en particular la Recomendación 15, en lo referente a la lucha contra el lavado de activos y el financiamiento del terrorismo en las transacciones con activos virtuales. Sin embargo, persisten desafíos significativos en materia de jurisdicción y cooperación internacional, especialmente cuando los exchanges o plataformas de intercambio operan desde el exterior y no están sujetos directamente a la normativa nacional.

En este marco, el Convenio de Budapest sobre Ciberdelito[13] [5], suscripto por Argentina, y su Segundo Protocolo Adicional [6] constituyen instrumentos fundamentales, ya que permiten requerimientos directos de información digital entre autoridades judiciales y empresas proveedoras radicadas en los Estados Parte del convenio. Dichos mecanismos garantizan la licitud del acceso a datos públicos, la preservación de la cadena de custodia digital, y fortalecen tanto la cooperación internacional como la eficacia de la investigación forense.

Como parte de los esfuerzos institucionales nacionales por abordar los desafíos vinculados a los criptoactivos, el Ministerio Público Fiscal (MPF[14]) de la Procuración General de la Nación publicó el 12 de mayo de 2023, la Resolución N.° 33/23, mediante la cual se dio a conocer la "*Guía Práctica*

[10] GAFILAT (Grupo de Acción Financiera de Latinoamérica): organismo regional intergubernamental que agrupa a países de América del Sur, Centroamérica y América del Norte, dedicado a promover la implementación de políticas contra el lavado de activos y la financiación del terrorismo, en coordinación con el GAFI.

[11] Las actividades incluidas en la definición de PSAV son i. intercambio entre activos virtuales y monedas de curso legal (monedas fiduciarias); ii. intercambio entre una (1) o más formas de activos virtuales; iii. transferencia de activos virtuales; iv. custodia y/o administración de activos virtuales o instrumentos que permitan el control sobre los mismos; y v. participación y provisión de servicios financieros relacionados con la oferta de un emisor y/o venta de un activo virtual.

[12] Las 40 Recomendaciones del GAFI son los estándares internacionales más reconocidos para combatir el lavado de activos y el financiamiento del terrorismo: https://www.gafilat.org/index.php/es/las-40-recomendaciones

[13] El Convenio de Budapest sobre Ciberdelincuencia es el primer tratado internacional que establece un marco jurídico común para combatir los delitos informáticos y las infracciones cometidas mediante sistemas informáticos o redes. Adoptado por el Consejo de Europa en 2001, promueve la armonización legislativa, el fortalecimiento de las capacidades de investigación y la cooperación internacional entre los Estados Parte para la obtención y preservación de evidencia digital. Los artículos 18 y 19 regulan la obtención, preservación y entrega de datos por parte de proveedores de servicios y autoridades competentes, mientras que el artículo 32 habilita la obtención transfronteriza de información informática cuando se trate de datos públicos o con consentimiento del titular.

[14] MPF (Ministerio Público Fiscal de la Nación): órgano autónomo del Estado argentino responsable de promover la acción de la justicia en defensa de la legalidad y los intereses generales de la sociedad.

para la Identificación, Trazabilidad e Incautación de Criptoactivos" [7], elaborada por la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI[15]). La resolución destaca diversas particularidades del entorno digital que dificultan el trabajo del MPF y las investigaciones penales, entre ellas el pseudoanonimato, la complejidad de los procesos informáticos y matemáticos empleados, la alta volatilidad del valor de las monedas virtuales, la localización de las operaciones con criptoactivos y sus actores, la escasa regulación existente, entre otros. Esta guía —una de las primeras de su tipo en Argentina— tiene como objetivo dotar a los organismos públicos de conocimientos y mecanismos actualizados para rastrear transacciones y confiscar activos virtuales que pudieran ser utilizados en actividades delictivas. Asimismo, busca ofrecer a los investigadores un material de referencia accesible para comprender el fenómeno de los criptoactivos y las tecnologías asociadas, con especial énfasis en los aspectos operativos de la investigación criminal, incluida la etapa de incautación. Sin embargo, no proporciona procedimientos específicos de investigación judicial ni aborda las tareas y análisis periciales que competen a los peritos informáticos en su labor. Como su título indica, se focaliza particularmente en la identificación, trazabilidad e incautación de criptoactivos para su investigación penal.

En una línea de acción más general, en marzo de 2023, el Ministerio de Seguridad de la Nación publicó el "*Protocolo para la Identificación, Recolección, Preservación, Procesamiento y Presentación de Evidencia Digital"* [8], elaborado por la Dirección de Investigaciones del Ciberdelito. Este Protocolo General de Actuación (PGA) tiene por objeto establecer las pautas y procedimientos que deben seguir los miembros de las Fuerzas Federales Policiales y de Seguridad durante las etapas de identificación, recolección, preservación, procesamiento y presentación de evidencia digital asociada a cualquier tipo de delito, y en particular a los ciberdelitos, ya sean ciberasistidos o ciberdependientes. El documento se enmarca en los objetivos de la Resolución N.° 86/2022 del Ministerio de Seguridad, dictada en el contexto del Programa de Fortalecimiento en Ciberseguridad e Investigación del Cibercrimen (ForCIC[16]). Su aplicación es de carácter obligatorio en todo el territorio nacional para el personal de la Policía Federal Argentina, Gendarmería Nacional Argentina, Policía de Seguridad Aeroportuaria y Prefectura Naval Argentina, quienes deben ajustar su accionar a la Constitución Nacional, las leyes penales, las normas procesales y los protocolos vigentes.

Este protocolo realiza una referencia general a los conceptos asociados a tecnología de blockchain y criptoactivos, estableciendo que, ante la posible presencia de Potenciales Elementos de Prueba digitales ("PEP digitales")[17] vinculados a los mismos, se coordine con la autoridad judicial los pasos a seguir. No detalla procedimientos de acción específicos, sino que se limita a definiciones y recomendaciones generales. Tampoco profundiza en cómo llevar adelante una investigación judicial o un análisis forense digital que incluya este tipo de evidencia. Definiciones relevantes incluidas en este protocolo:

- Tecnología de blockchain: Libro de contabilidad digital distribuido de transacciones firmadas criptográficamente que se agrupan en bloques. Cada bloque se vincula criptográficamente con el anterior después de su validación y de someterse a una decisión consensuada. A medida que se añaden nuevos bloques, los más antiguos se vuelven más difíciles de modificar (creando una resistencia a la manipulación). Los nuevos bloques se replican en las copias del libro mayor dentro de la red, y cualquier conflicto se resuelve automáticamente utilizando las reglas establecidas.
- Criptoactivos: Representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar con fines de pago o inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias.
- Rig de Minería: Conjunto de elementos de hardware instalados y configurados para el minado de criptoactivos.

En el mismo protocolo se establece que, al momento del allanamiento, deberá prestarse especial atención a los siguientes aspectos:

- Presencia de billeteras frías —dispositivos con aspecto similar a un pendrive—, así como a anotaciones que contengan palabras clave (semillas), códigos QR u otros datos que puedan estar asociados a wallets o monederos digitales. Ante la detección de indicadores o identificadores vinculados a actividades con criptoactivos, se deberá consultar de inmediato a la autoridad judicial, quien determinará el criterio de actuación correspondiente.
- Hallazgo de equipos de minería (rigs de minería). El primer interviniente deberá coordinar con la autoridad judicial y con el personal especializado en criptoactivos para definir el procedimiento a seguir. Los rigs de minería pueden presentar distintos aspectos según la tecnología utilizada; actualmente, los más comunes emplean placas de video (GPU) o hardware específico para algoritmos determinados (ASIC). Debe considerarse que algunos rigs representan un alto valor económico, por lo que su detección durante un procedimiento debe ser informada a la autoridad judicial para que evalúe su posible secuestro. El protocolo no detalla las acciones específicas a seguir, sino que en todos los casos recomienda la consulta a la autoridad judicial antes de proceder.

Las criptomonedas constituyen un tipo específico de criptoactivos. Son monedas virtuales de emisión descentralizada, sin respaldo de ningún gobierno o entidad en particular, basadas en la tecnología de blockchain. Funcionan como medios de pago y buscan reproducir las funciones esenciales del dinero. A diferencia del sistema financiero

[15] UFECI (Unidad Fiscal Especializada en Ciberdelincuencia): unidad del Ministerio Público Fiscal de la Nación Argentina encargada de investigar delitos informáticos y coordinar acciones vinculadas con la criminalidad digital y el uso de criptoactivos.

[16] ForCIC (Programa de Fortalecimiento en Ciberseguridad e Investigación del Cibercrimen): creado por el Ministerio de Seguridad de la Nación mediante la Resolución N.° 86/2022, publicada en el Boletín Oficial el 1 de marzo de 2022, orientado a establecer políticas, protocolos y capacidades técnicas para fortalecer la prevención, detección e investigación de delitos informáticos en Argentina.

[17] Potencial Elemento de Prueba (PEP): dispositivos susceptibles de contener información (representación física), los cuales almacenan potencial evidencia digital (representación lógica). Potencial Elemento de Prueba digital (PEP digital): se refiere a cualquier dato (registro y/o archivo) que puede ser generado, transmitido o almacenado por equipos de tecnología informática y que está constituido por campos magnéticos y pulsos electrónicos, los cuales pueden ser recolectados y analizados con herramientas y/o técnicas especiales.

tradicional —basado en la confianza y la intermediación de instituciones financieras—, las criptomonedas operan sobre un sistema de pago electrónico sustentado en pruebas criptográficas, lo que garantiza la autenticidad y seguridad de las transacciones sin necesidad de terceros o autoridades centrales. De este modo, dos partes pueden realizar transacciones directas entre sí mediante mecanismos de criptografía que aseguran la validez de las operaciones.

Actualmente no existe una guía o metodología que esté orientada a cómo proceder específicamente en una pericia informática basada en el análisis y resguardo de potenciales elementos de prueba digital de criptomonedas y criptoactivos para presentar ante la justicia.

Como antecedentes de la presente investigación, en el Departamento de Ingeniería e Investigaciones Tecnológicas (DIIT) de la Universidad Nacional de La Matanza se desarrollaron tres proyectos orientados al diseño de metodologías, procedimientos y a la implementación y gestión de Laboratorios de Informática Forense. Si bien estos trabajos no tuvieron un enfoque específico en criptoactivos o criptomonedas, constituyen el marco metodológico y operativo de referencia que permite avanzar en el desarrollo de la propuesta actual.

En primer lugar, se llevó a cabo el proyecto "*Análisis del Marco Normativo Técnico Legal del Ciclo de Vida de la Evidencia Digital*" en el cual se desarrolló un marco normativo y operativo de referencia para el tratamiento integral de la evidencia digital, incorporando los aspectos legales y procedimentales necesarios para su correcta gestión.

En el contexto del segundo proyecto, "*Implementación y Gestión de un Laboratorio de Informática Forense*" [9], se definió un modelo integral para la creación y gestión de un Laboratorio de Informática Forense (LabIF-UNLaM), abordando tanto la infraestructura tecnológica como los procesos y metodologías de trabajo. De este desarrollo surgió la metodología ForenseUDE [10], alineada con los modelos PURI[18] ("Proceso Unificado de Recuperación de Información") [11], [12] y EDRM[19] ("Electronic Discovery Reference Model") [13]. Su diseño incorpora, además, los lineamientos de la norma ISO/IEC 27037:2012 [14] y su versión traducida al castellano con observaciones, ISO/IRAM 27037:2022, adaptada al contexto nacional, garantizando la validez técnica y legal.

La metodología ForenseUDE fue desarrollada con el propósito de establecer un proceso universal, integral y detallado para el tratamiento de la evidencia digital. Estructura un conjunto de fases interconectadas que guían las actividades forenses desde la identificación hasta la presentación de resultados, garantizando trazabilidad, consistencia y validez técnica en cada etapa.

Como resultado del tercer proyecto impulsado por el DIIT, "*Diseño de un Sistema de Gestión de Calidad y Proceso de Acreditación del Laboratorio Informático Forense (LabIF-UNLaM)*", se logró diseñar, desarrollar e implementar un Sistema de Gestión de la Calidad aplicable al laboratorio, conforme a la norma ISO/IEC 17.025:2017, fortaleciendo la estandarización y la confiabilidad de los procesos periciales [15], [16].

IV. HERRAMIENTAS DE ANÁLISIS Y TRAZABILIDAD

Existe la idea de que, debido a su naturaleza seudónima, es imposible determinar el origen de las criptomonedas o rastrear el camino que han recorrido hasta llegar a la persona que las posee en un momento específico. Sin embargo, las criptomonedas de blockchains públicas son perfectamente trazables, ya que todas las transacciones realizadas están expuestas y son visibles para el público en general. Aunque la red opera de manera seudónima, ya que no hay registro en la blockchain sobre la identidad detrás de cada dirección pública, es posible combinar esa información con otros datos para asociar direcciones a personas y así reconstruir una cadena de tenencias de criptomonedas. Es decir, es viable llevar a cabo una investigación forense para identificar el origen o destino de una criptomoneda.

El análisis forense y la investigación judicial de operaciones con criptoactivos requieren el uso combinado de herramientas especializadas que permitan rastrear, visualizar y documentar transacciones en entornos blockchain.

El proceso investigativo requiere el uso combinado de software libre y plataformas comerciales especializadas en trazabilidad de criptoactivos —tales como Chainalysis [17] y TRM Labs [18] — con el fin de abordar el análisis de grandes volúmenes de transacciones en redes blockchain públicas.

Estas herramientas permiten identificar patrones de flujo financiero, detectar nodos relevantes y visualizar interacciones entre direcciones mediante heurísticas de agrupamiento, técnicas de atribución basada en OSINT (Open-Source Intelligence)[20] y algoritmos de análisis de grafos. OSINT complementa las técnicas de trazabilidad blockchain al permitir contextualizar direcciones, entidades o transacciones mediante información disponible en Internet o detectar infraestructura técnica asociada a actividades ilícitas (por ejemplo, servidores C2[21], exchanges no registrados o clusters de wallets[22]).

[18] PURI (Proceso Unificado de Recuperación de Información): es el resultado de un proyecto de una investigación iniciada en el 2011 en la Facultad de Ingeniería de la Universidad FASTA. El modelo es un esquema de las tareas involucradas en la aplicación forense de las ciencias de la información. Este esquema agrupa las tareas en actividades de mayor abstracción, y a éstas en.

[19] EDRM ("Electronic Discovery Reference Model"): modelo internacional de referencia del descubrimiento electrónico (e-discovery), que se refiere a cualquier proceso en el que se busca, localiza, asegura y examina datos electrónicos con la intención de usarlos como evidencia digital. Este modelo también menciona una serie de etapas o fases en las cuales se brindan mejores prácticas de manera global para el tratamiento de la evidencia.

[20] OSINT: se refiere a la obtención, análisis y correlación de información proveniente de fuentes abiertas y accesibles públicamente, tales como sitios web, redes sociales, registros públicos o foros en línea. Principales herramientas OSINT: Maltego, SpiderFoot, Shodan, Breadcrumbs y Bitquery, entre otras.

[21] Servidores C2 (Command and Control): son infraestructuras utilizadas por atacantes para dirigir, coordinar y controlar sistemas comprometidos o redes de equipos infectados (botnets).

[22] Clusters de wallets: son agrupaciones lógicas de direcciones de criptomonedas que, mediante técnicas de análisis heurístico y de comportamiento en la blockchain, pueden inferirse como controladas por un mismo usuario o entidad.

El empleo conjunto de entornos abiertos y soluciones propietarias fortalece la validez técnica y pericial del proceso, al combinar la transparencia del código abierto con las capacidades avanzadas de procesamiento, correlación y automatización que ofrecen las plataformas comerciales en investigaciones complejas.

Entre las soluciones más utilizadas a nivel internacional se destacan Chainalysis y TRM Labs, plataformas comerciales de inteligencia y trazabilidad blockchain que integran métodos de análisis de grafos, heurísticas de agrupamiento y atribución de direccione.

Chainalysis es una plataforma comercial de inteligencia blockchain diseñada para la trazabilidad y el análisis forense de transacciones con criptoactivos. Permite examinar el flujo de fondos a través de diferentes redes —como Bitcoin, Ethereum y otras blockchains públicas— mediante la aplicación de algoritmos de agrupamiento heurístico, análisis de grafos y técnicas de atribución de direcciones. En el ámbito judicial, su utilización posibilita vincular direcciones de criptoactivos con entidades o actores específicos, detectar operaciones sospechosas, y reconstruir esquemas de lavado de activos, fraude o ransomware. Asimismo, facilita la generación de reportes técnicos admisibles como evidencia digital, compatibles con los principios de trazabilidad y preservación de la cadena de custodia.

Desde una perspectiva forense, Chainalysis aporta capacidad analítica avanzada para el tratamiento de grandes volúmenes de datos y el seguimiento de fondos a través de mixers[23], exchanges o wallets distribuidas globalmente, constituyéndose en una herramienta de apoyo esencial para peritos informáticos y fiscales en investigaciones complejas relacionadas con criptoactivos.

TRM Labs es una plataforma de análisis e inteligencia blockchain orientada al monitoreo de riesgos, cumplimiento normativo y trazabilidad de criptoactivos. Su principal fortaleza radica en la integración de información on-chain[24] y off-chain[25], permitiendo a las autoridades judiciales y forenses identificar, rastrear y analizar transacciones sospechosas en múltiples redes y activos digitales. La herramienta combina modelos de aprendizaje automático con bases de datos de entidades verificadas, lo que posibilita asociar direcciones de billeteras con exchanges, plataformas de servicios financieros y actores ilícitos conocidos. En el contexto forense, facilita la visualización de flujos transaccionales, la detección de patrones de lavado de activos o financiamiento del terrorismo, y la elaboración de reportes probatorios que cumplen con los estándares internacionales de evidencia digital. El uso de TRM Labs en investigaciones judiciales fortalece la cooperación interinstitucional y la eficacia de la respuesta frente a delitos financieros basados en blockchain, al ofrecer un entorno analítico unificado, trazable y técnicamente verificable.

En síntesis, Chainalysis se orienta al análisis forense retrospectivo y judicial de operaciones, mientras que TRM Labs privilegia un enfoque preventivo y de cumplimiento normativo dentro del ecosistema financiero.

El uso conjunto de ambas herramientas —en sinergia con software libre y técnicas OSINT— amplía el alcance del análisis, fortaleciendo la validez técnica y jurídica de las investigaciones, y consolidando un enfoque estandarizado para la trazabilidad forense de activos digitales. Además, ofrecen una cobertura integral que abarca desde la detección temprana de operaciones sospechosas hasta la trazabilidad forense y presentación de evidencia digital.

La admisibilidad judicial de evidencia obtenida en estas herramientas ha sido validada en precedentes internacionales principalmente en los Estados Unidos, los cuales confirmaron su validez probatoria al considerarlas técnicamente confiables, utilizadas por agencias federales y sujetas a verificación pericial independiente. En United States v. Sterlingov [19], el tribunal del Distrito de Columbia admitió los informes de Chainalysis como evidencia válida para vincular direcciones de Bitcoin utilizadas en un servicio de mezcla (*mixer*) con el acusado, estableciendo la confiabilidad técnica de la herramienta y su uso por parte del FBI y el IRS-CI .Por su parte, en *U*.S. v. Harmon [20], la misma corte aceptó los resultados de trazabilidad de Chainalysis que demostraron operaciones ilícitas de lavado de dinero a través de un servicio de "mixing", sentando un precedente relevante para la utilización forense de estos sistemas en delitos financieros y cibernéticos.

Estos antecedentes internacionales sientan base para su aceptación en investigaciones judiciales y pericias forenses de criptoactivos, al demostrar que la trazabilidad basada en blockchain puede cumplir con los estándares de admisibilidad de evidencia digital en el proceso penal.

V. PLANTEO GENERAL DE LA METODOLOGÍA

Se plantea el diseño de una metodología de análisis y resguardo de potenciales elementos de prueba digital vinculados a criptomonedas y criptoactivos, aplicable a pericias informáticas que formen parte de procesos o investigaciones judiciales. El objetivo principal es fortalecer la eficacia, confiabilidad y validez técnica y legal de los procedimientos forenses en el ámbito de los criptoactivos.

La metodología propuesta, orientada al tratamiento de posibles elementos de prueba digital asociados a estos activos, busca asegurar la integridad y trazabilidad de la evidencia digital, promoviendo un desempeño eficiente y estandarizado

[23] Mixers (o tumblers): son servicios o protocolos diseñados para ofuscar el origen y destino de los fondos en una transacción de criptomonedas, mezclando múltiples entradas y salidas de distintos usuarios. Su objetivo declarado suele ser preservar la privacidad, pero en la práctica son utilizados con frecuencia para dificultar la trazabilidad y el rastreo de operaciones ilícitas, como lavado de activos o pago de ransomware. Desde el punto de vista forense, los mixers representan un desafío técnico, ya que rompen la correlación directa entre direcciones y flujos de valor, requiriendo análisis heurísticos avanzados y herramientas de trazabilidad especializadas (p. ej., Chainalysis o TRM Labs).

[24] Información on-chain: comprende todos los datos registrados directamente en la cadena de bloques, como transacciones, direcciones, hashes, bloques y contratos inteligentes. Esta información es pública, inmutable y verificable criptográficamente, lo que permite su análisis mediante herramientas de trazabilidad o inteligencia forense.

[25] Información off-chain: se refiere a datos externos o complementarios que no se almacenan en la blockchain, tales como registros de usuarios en exchanges, metadatos de dispositivos, comunicaciones, archivos, documentos, o datos personales asociados. Su obtención suele requerir órdenes judiciales, cooperación internacional o análisis técnico adicional, y resulta esencial para vincular identidades reales con transacciones pseudónimas.

por parte de los equipos periciales. Asimismo, favorece la cooperación interinstitucional, al propiciar la homologación de criterios y la aceptación de los resultados obtenidos entre diferentes laboratorios forenses.

El desarrollo de esta propuesta metodológica se alinea y especifica a partir de la metodología ForenseUDE, consolidando su adaptación al contexto tecnológico y jurídico de los criptoactivos. Además, se enmarcan en los lineamientos de las normas ISO/IEC 27037:2012 e ISO/IRAM 27037:2022, y sus normas complementarias, como también con las leyes, pautas procesales y protocolos vigentes a nivel nacional e internacional.

Etapa Preliminar de Actualización Metodológica y Tecnológica

Se propone una instancia preliminar y de actualización permanente orientada a fortalecer las capacidades técnicas, analíticas y operativas de los equipos forenses en el tratamiento de evidencia digital vinculada a criptomonedas y criptoactivos. Estas etapas constituyen un marco de referencia dinámico que sustenta la metodología general, asegurando su vigencia y adecuación frente a la evolución tecnológica y delictiva del ecosistema cripto-financiero.

1) Relevamiento y actualización de aspectos teórico-prácticos sobre criptoactivos y tecnología blockchain

Comprende el estudio y actualización de los principales fundamentos técnicos y operativos relacionados con los activos virtuales basados en tecnología blockchain. Incluye el análisis de las transacciones con criptomonedas y criptoactivos, los mecanismos de minería y validación, el funcionamiento de las billeteras virtuales y los métodos de almacenamiento y resguardo de claves privadas. Esta etapa proporciona el sustento conceptual necesario para comprender la naturaleza, estructura y trazabilidad de los criptoactivos en el contexto de la investigación y el análisis forense digital.

2) Investigación y formalización de procedimientos y herramientas para el seguimiento transaccional

Implica el estudio y la definición de procedimientos específicos y herramientas para rastrear y reconstruir el flujo de transacciones (on-chain y off-chain) que involucran criptomonedas y criptoactivos. Su finalidad es establecer criterios de actuación homogéneos que permitan mejorar la trazabilidad y correlación de operaciones a lo largo de la cadena de bloques.

3) Análisis e identificación de nuevas modalidades delictivas asociadas a criptoactivos

Orienta la investigación hacia la detección, clasificación y comprensión de las tipologías delictivas emergentes vinculadas con el uso de criptoactivos, como fraudes, estafas, esquemas de lavado de activos o financiamiento ilícito. Incluye la evaluación de técnicas, actores, patrones de comportamiento y dinámicas de operación que permitan fortalecer la detección temprana y la trazabilidad en el ámbito forense, contribuyendo a la formulación de protocolos de actuación y prevención.

4) Identificación y estudio de métodos antiforenses

Abarca la identificación, análisis y documentación de técnicas antiforenses utilizadas por los ciberdelincuentes para evadir o dificultar la acción de los investigadores. Se consideran herramientas de anonimización, uso de mixers, tumblers, servicios de ofuscación, entre otros mecanismos que alteran la visibilidad de las transacciones o la recuperación de evidencia digital. Incluye la actualización continua de repertorios de amenazas y tipologías antiforenses emergentes.

5) Definición y validación de procedimientos y herramientas forenses aplicables

Consiste en la revisión, selección y validación de metodologías y soluciones tecnológicas aplicables al análisis digital y la investigación de ciberdelitos y cibercrimen vinculados con criptoactivos. Incluye la evaluación comparativa de plataformas de trazabilidad blockchain, software de análisis forense y metodologías de investigación digital, promoviendo la estandarización y compatibilidad entre laboratorios e instituciones.

Tareas Principales de la Metodología

1) Identificación y clasificación de potenciales elementos de prueba digital (PEP) asociados a criptoactivos.

Consiste en la detección, reconocimiento y categorización de indicios o elementos digitales vinculados con criptoactivos que puedan constituir potenciales evidencias en una investigación judicial. Incluye el relevamiento de dispositivos físicos y virtuales —como billeteras frías o calientes, registros de transacciones, equipos de minería, aplicaciones de intercambio (exchanges), y documentación asociada a claves o frases semilla. Esta etapa permite establecer una primera delimitación del alcance de la evidencia, diferenciando entre datos on-chain y off-chain, y asegurando la preservación inicial de la integridad y trazabilidad de la información.

2) Análisis forense y trazabilidad de transacciones con criptoactivos

Tareas orientadas a la aplicación de técnicas de análisis forense digital y trazabilidad en redes blockchain, con el fin de reconstruir el flujo de operaciones y determinar el origen, destino y posible vinculación de los criptoactivos con actividades ilícitas. Se propone emplear una combinación de herramientas de software libre y plataformas comerciales de trazabilidad —como *Chainalysis Reactor* o *TRM Labs*— para el manejo de grandes volúmenes de datos, la detección de patrones transaccionales, la identificación de clusters de direcciones y el rastreo de fondos a través de mixers o servicios de ofuscación. Asimismo, se integran técnicas de OSINT y análisis de información on-chain y off-chain, garantizando la

consistencia metodológica, la documentación del proceso y la preservación de la cadena de custodia digital.

3) Resguardo, preservación y documentación de la evidencia digital.

Comprende el conjunto de procedimientos destinados a asegurar la integridad, autenticidad y trazabilidad de los potenciales elementos de prueba digital (PEP) vinculados a criptoactivos y criptomonedas. Se establecen pautas de recolección, etiquetado, almacenamiento y registro documental que garanticen la cadena de custodia digital durante todas las etapas del proceso forense. La preservación incluye tanto los datos *on-chain* como *off-chain*, así como la protección de metadatos y claves criptográficas asociadas a billeteras o transacciones.

4) Presentación y comunicación de resultados periciales.

Esta fase final se orienta a la elaboración y presentación de informes técnicos periciales que documenten de manera clara, precisa y verificable el proceso de análisis forense realizado sobre los criptoactivos y criptomonedas. Incluye la descripción de los procedimientos aplicados, las herramientas utilizadas, los hallazgos relevantes y las conclusiones obtenidas, en un formato que garantice su comprensión tanto por especialistas técnicos como por autoridades judiciales. El informe debe reflejar el cumplimiento de las normas y protocolos vigentes, mantener la trazabilidad de la evidencia y respaldar la validez técnica, jurídica y probatoria de los resultados.

A partir de la definición de esta metodología adecuada a ForenseUDE se plantea la actualización de los procedimientos y herramientas del Laboratorio Informático Forense (LabIF-UNLaM) para llevarse a cabo pericias informáticas de casos vinculados a criptoactivos y criptomonedas.

VI. Riesgos delictivos asociados al uso de Criptomonedas y Criptoactivos

Así como el mercado criptoactivos y criptomonedas ha crecido y continúa creciendo a pasos agigantados en todo el mundo, en forma paralela, desafortunadamente, también se optimizaron las maniobras delictivas en este innovador ámbito, donde su desregulación, su masiva proliferación o el uso de diversas tecnologías traen aparejados nuevos riesgos, al crear nuevas oportunidades de actividades ilícitas.

Por un lado, nos encontramos con usuarios atraídos, interesados en explorar sus posibles beneficios sociales y económicos, pero también con individuos que desnaturalizan su propósito y evalúan alternativas para explotar la tecnología en el marco de actividades ilícitas.

Las criptos presentan incontables casos de uso beneficiosos para nuestra sociedad. Sin embargo, también es importante destacar que pueden ser utilizadas para cometer distintos tipos de actividades ilícitas. El riesgo de ser víctima de fraude es muy alto, ya que los estafadores a menudo tienen la ventaja en este entorno digital.

Entre los principales delitos se encuentran: estafas con criptomonedas, evasión fiscal, lavado de dinero, coerción y chantaje, especulación, tiendas de dudosa reputación en la dark web, ataques de ransomware/malware, pornografía, fraudes en línea, identidades falsificadas, tráfico de drogas ilegales, financiamiento de organizaciones terroristas o criminales, criminalidad organizada, entre otros.

En todos estos casos los ciberdelincuentes suelen utilizar criptodivisas para dificultar el rastreo y anonimizar sus transacciones. El alto valor económico de estos activos digitales los hace atractivos para todo tipo de delitos, entre ellos los patrimoniales.

Dada su naturaleza digital, las "apropiaciones" de criptomonedas revisten la forma de ataques a los sistemas informáticos de sus tenedores, ya sean empresas o individuos, para lograr tomar el control del sistema y transferir estos bienes digitales a cuentas propias.

La capacidad de realizar operaciones transfronterizas rápidamente y a través de internet no solo permite a los criminales adquirir, mover y almacenar activos digitalmente, a menudo fuera del sistema financiero regulado, sino que también posibilita disfrazar el origen o destino de los recursos, dificultando que los sujetos obligados identifiquen de manera oportuna las actividades sospechosas. Estos factores añaden obstáculos a la detección e investigación de la actividad criminal.

Los casos más frecuentes de comisión de delitos que involucran a las criptomonedas son los de “Ransomware”. Estas son situaciones de ataques informáticos donde se encriptan todos o parte de los archivos de un ordenador o sistema informático de la entidad atacada, ya sea una persona física o una empresa, donde el atacante sólo desencriptará los archivos a cambio de un pago, generalmente en criptomonedas.

En línea con este tipo de ataques informáticos, otra táctica común es la introducción de malware en otros dispositivos. Esto permite que el dispositivo participe sin saberlo en un esquema de minería. Las criptomonedas generadas a través de este malware son dirigidas hacia el ciberdelincuente que infectó el dispositivo, resultando en una suerte de "hurto de uso", aprovechando el tiempo de procesamiento de los sistemas afectados. Además, las criptomonedas son utilizadas como medio para cometer delitos relacionados con la prevención de lavado de activos y el financiamiento del terrorismo, entre otros.

La investigación criminal ligada a los criptoactivos cobra un rol preponderante. Investigar actividades delictivas relacionadas con criptoactivos puede resultar complejo, ya que muchos casos podrían estar vinculados con compras realizadas o fondos transferidos a través de la cadena de bloques. Por lo tanto, resulta vital comprender con precisión cómo se preparan, transmiten, procesan y almacenan estas transacciones.

A esto se suma las “billeteras virtuales” o “monederos virtuales” (wallets) de las cuales existen una gran variedad de implementaciones y permiten almacenar las claves privadas para que los activos virtuales sean seguros y accesibles. Son aplicaciones o software que permite a los usuarios administrar sus criptomonedas y realizar transacciones. Una billetera virtual no almacena criptoactivos, pero sí hará referencia a cualquier transacción en la cadena de bloques que se pueda

vincular con las claves privadas gestionadas por intermedio de esta. En este sentido cabe distinguir las billeteras virtuales de las aplicaciones provistas por diferentes plataformas privadas que proveen servicios de arbitraje y/o compraventa de criptoactivos, conocidas comúnmente como "Exchanges".

Existen monederos con almacenamiento en frío (Cold storage), lo cual alude a los monederos que no están conectados a Internet, como los monederos físicos o de papel. La finalidad de las variantes de "almacenamiento en frío" es ofrecer protección contra el hackeo o robo de las criptomonedas. En contraposición, los monederos con almacenamiento en caliente funcionan online, es decir, con conexión a Internet. Debido a ello, esta forma de almacenamiento es más vulnerable a la piratería/robo que el almacenamiento en frío.

VII. CONCLUSIONES

Disponer de una metodología integral para el análisis y resguardo de posibles elementos de prueba digital asociados a criptomonedas y criptoactivos, fortalece la eficacia y la confiabilidad de los procedimientos forenses a aplicar en pericias informáticas, asegurando que se generen resultados técnica y legalmente válidos.

Dicha metodología puede ser aplicada en organismos judiciales, fuerzas de seguridad, por parte de peritos informáticos en sus diferentes roles y en otros laboratorios de informática forense nacionales e internacionales.

Asimismo, favorece la futura cooperación entre laboratorios de diferentes organismos y entidades, tanto nacionales como internacionales, al generar una mayor confiabilidad y aceptación del trabajo pericial y los resultados obtenidos.

REFERENCIAS

[1] Unidad de Información Financiera (UIF), *Resolución 300/2014 – Monedas* Virtuales, Buenos Aires, Argentina, 2014. [En línea]. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/230000-234999/231930/norma.htm

[2] Grupo de Acción Financiera de Latinoamérica (GAFILAT), "Guía sobre Aspectos Relevantes y Pasos Apropiados para la Investigación, Identificación, Incautación y Decomiso de Activos Virtuales". GAFILAT, 2021. [En línea]. Disponible en: https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guía-sobre-aspectos-relevantes-y-pasos-apropiados-para-la-investigación-identificación-incautación-y-decomiso-de-AV.pdf

[3] Comisión Nacional de Valores, "Resolución General 994/2024 – Registro de Proveedores de Servicios de Activos Virtuales (PSAV)", Boletín Oficial de la República Argentina, 25-Mar-2024. [En línea]. Disponible en: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-994-2024-397598

[4] Grupo de Acción Financiera Internacional (GAFI), *Las* Recomendaciones del GAFI – Estándares internacionales sobre la lucha contra el lavado de activos, el financiamiento del terrorismo y la proliferación (Feb. 2012). [En línea]. Disponible en: https://www.mpf.gob.ar/dafi/files/2017/03/GAFI-Recomendaciones.pdf

[5] Consejo de Europa, Convenio sobre Ciberdelincuencia (Convenio de Budapest), Budapest, 23 de noviembre de 2001. [En línea]. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[6] Consejo de Europa, Segundo Protocolo Adicional al Convenio sobre Ciberdelincuencia relativo a la mejora de la cooperación y la revelación de pruebas electrónicas, Estrasburgo, 12 de mayo de 2022. [En línea]. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/224

[7] Ministerio Público Fiscal de la Nación, "Guía Práctica para la Identificación, Trazabilidad e Incautación de Criptoactivos". Dirección de Comunicación Institucional, Buenos Aires, Argentina, 2023. [En línea]. Disponible en: https://www.fiscales.gob.ar/wp-content/uploads/2023/05/Informe_Criptoactivos-1.pdf

[8] Ministerio de Seguridad de la Nación, Dirección de Investigaciones del Ciberdelito, "Protocolo para la Identificación, Recolección, Preservación, Procesamiento y Presentación de Evidencia Digital", Resolución N.° 232/2023. Buenos Aires, Argentina, 2023. [En línea]. Disponible en: https://servicios.infoleg.gob.ar/infolegInternet/anexos/380000-384999/382307/res232.pdf

[9] C. V. Gioia, J. Eterovic, M. J. Krajnik y E. A. Zárate, "Marco de referencia para la implementación y gestión de Laboratorios de Informática Forense", en CADI 2021 – 5.º Congreso Argentino de Ingeniería, Universidad de Buenos Aires (UBA), Buenos Aires, Argentina, 2021.

[10] C. V. Gioia, E. A. Zárate, M. L. Giménez, M. J. Krajnik y J. E. Eterovic, "Metodología de Informática Forense Universal ForenseUDE", en VI Info-Conf 2022, Universidad FASTA, Mar del Plata, Argentina, p. 51, 2022. [En línea]. Disponible en: https://info-lab.org.ar/extension/info-conf;https://drive.google.com/file/d/1wKJqVbb3vD9ihLyHCWFDuq_km3GxbhQs/view

[11] A. H. Di Iorio, M. Castellote, C. Bruno y J. Waimann, El Rastro Digital del Delito. Mar del Plata, Argentina: Universidad FASTA, Info-Lab, 2017.

[12] A. H. Di Iorio, Guía Integral de Empleo de la Informática Forense en el Proceso Penal, 1.ª ed. Mar del Plata, Buenos Aires, Argentina: Universidad FASTA, 2015. [En línea]. Disponible en: https://info-lab.org.ar/descargas/libros-y-guias

[13] Electronic Discovery Reference Model (EDRM), EDRM Model, 2020. [En línea]. Disponible en: http://www.edrm.net

[14] International Organization for Standardization (ISO), Sitio oficial de la Organización Internacional de Normalización. [En línea]. Disponible en: https://www.iso.org/home.html

[15] M. J. Krajnik, E. A. Zárate, y C. V. Gioia, Implementación de Laboratorios de Informática Forense en base a la norma IRAM/ISO/IEC 17025:2017, ReDDI – Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza, vol. 2, no. 1, ISSN 2525-1333, Univ. Nac. de La Matanza, Buenos Aires, Argentina, 2024. [En línea]. Disponible en: https://reddi.unlam.edu.ar/index.php/ReDDi/article/download/241/434/

[16] M. J. Krajnik, E. A. Zárate, y C. V. Gioia, Requisitos de Infraestructura Edilicia y Tecnológica de Base para la Implementación de Laboratorios de Informática Forense, ReDDI – Revista Digital del Departamento de Ingeniería e Investigaciones Tecnológicas de la Universidad Nacional de La Matanza, vol. 8, no. 2, ISSN 2525-1333, Univ. Nac. de La Matanza, Buenos Aires, Argentina, 2023. [En línea]. Disponible en: https://reddi.unlam.edu.ar/index.php/ReDDi/article/download/215/394/

[17] Chainalysis Inc., Blockchain Data Platform, [En línea]. Disponible en: https://www.chainalysis.com/

[18] TRM Labs Inc., Blockchain Intelligence for Stablecoin Risk Management / Crypto Investigation, Compliance & Risk Solutions, [En línea]. Disponible en: https://www.trmlabs.com/

[19] United States v. Sterlingov, Case No. 1:21-cr-00399, U.S. District Court for the District of Columbia, 2023. [En línea]. Disponible en: https://storage.courtlistener.com/recap/gov.uscourts.dcd.239226/gov.uscourts.dcd.239226.141.0.pdf

[20] United States v. Larry Dean Harmon, Case No. 1:19-cr-00395, U.S. District Court for the District of Columbia, 2021. [En línea]. Disponible en: https://www.justice.gov/opa/pr/operator-darknet-based-cryptocurrency-mixing-service-pleads-guilty

Ciberpatrullaje, Privacidad y Derechos

D. J. Romero, *Ingeniero en Informática e Ingeniero Electrónico* [1] y A. Grisolia, *Becario*[2]

[1]*Universidad Nacional de La Matanza (UNLaM) y Universidad Nacional del Oeste (UNO)*
djromero@unlam.edu.ar
[2]*Universidad Nacional del Oeste (UNO) dgrisolia@uno.edu.ar*

***Resumen*– En este trabajo se examinará el concepto de ciberpatrullaje, entendido como una actividad de vigilancia e investigación realizada por las fuerzas de seguridad en el ciberespacio, y se explorarán sus implicaciones en relación con la privacidad y la posible vulneración de los derechos de los ciudadanos. Para analizar este tema, se indagará, de manera pormenorizada, cada uno de los conceptos que tienen que ver con esta cuestión, como es el caso de la ciberseguridad, de la privacidad de los usuarios, y, también, de la protección de los derechos que se pueden ver vulnerados cuando se habla de ciberpatrullaje. A su vez, se tomarán en cuenta las leyes, así como las resoluciones internacionales y nacionales, que tratan sobre la seguridad de la información y la privacidad. También, se analizarán los riesgos y los desafíos que plantea el ciberpatrullaje para los derechos humanos, especialmente para la libertad de expresión y la privacidad de los usuarios, y se ahondarán las implicaciones éticas, políticas y sociales del ciberpatrullaje.**

***Abstract*– This work will examine the concept of cyberpatrolling, understood as a surveillance and investigative activity conducted by law enforcement in cyberspace, and will explore its implications regarding privacy and potential violations of citizens' rights. To analyze this topic, each relevant concept will be scrutinized in detail, including cybersecurity, user privacy, and the protection of rights that may be compromised with cyberpatrolling. Addiotinally, laws, international and national resolutions addressing information security and privacy will be considered. The risks and challenges posed by cyberpatrolling to human rights, particularly freedom of expression and user privacy, will also be analyzed, along with delving into the ethical, political, and social implications of cyberpatrolling.**

I. INTRODUCCIÓN

El ciberpatrullaje es una forma de vigilancia que implica la observación, análisis y recopilación de información de fuentes digitales abiertas, como las redes sociales, con el propósito de prevenir o investigar delitos. No obstante, esta práctica presenta riesgos y desafíos para los derechos humanos, en particular para la privacidad y la libertad de expresión de los usuarios de internet. Desde el punto de vista legal, el ciberpatrullaje debe estar regulado por normas claras, precisas y proporcionales, que establezcan los límites, las garantías y los controles necesarios para evitar abusos o arbitrariedades por parte de las autoridades En Argentina, en 2020, el Ministerio de Seguridad derogó la Resolución 31/2018, que habilitaba el ciberpatrullaje, y la reemplazó por la Resolución 144/2020 que buscaba establecer criterios más transparentes y participativos, con la intervención de organizaciones de la sociedad civil. Sin embargo, esta resolución no resolvió todas las cuestiones que plantea el ciberpatrullaje, y por este motivo es necesario una revisión y volver a configurar las bases de este tema.

Para comprender el ciberpatrullaje, es esencial examinar ciertos conceptos que permiten definir de manera más precisa este campo. Estos conceptos son: ciberseguridad, ciberespacio y, específicamente, dos conceptos impactados por el uso del ciberpatrullaje: la privacidad y, especialmente, los derechos humanos. En este trabajo se elaborará un examen acerca de estos conceptos para alcanzar una base sólida que permita indagar acerca de la problemática planteada en este trabajo.

II. CIBERSEGURIDAD Y PRIVACIDAD

No es posible discutir sobre ciberseguridad, ciberpatrullaje o la vulneración de derechos a través de la vigilancia sin abordar el ciberespacio, que es el entorno donde toda esta realidad ocurre. De esta forma, existe un escenario en el que las nociones de ciberseguridad y ciberespacio son familiares para todos los individuos. Sin embargo, no se posee un conocimiento completo sobre cómo estas pueden impactar la vida diaria de las personas, tanto en lo personal como en lo profesional. Los conceptos de ciberseguridad y ciberespacio son altamente complejos, dado que la ciberseguridad representa un nuevo modelo de seguridad global para los entornos afectados por la influencia y el uso del ciberespacio.

La Organización de Estados Americanos (OEA) dispone de un Programa de Seguridad Cibernética, cuyo principal objetivo radica en promover que los Estados miembros adopten estrategias nacionales de seguridad cibernética; no obstante, ese programa no brinda un concepto propio de ciberseguridad [1].

Para el caso argentino, la Resolución del JGM N° 580/11 que crea el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC), invoca el terminó ciberseguridad, pero no le reporta ninguna definición rigurosa. Por su parte, para la Unión Internacional de Telecomunicaciones (UIT), organismo especializado de la Organización de las Naciones Unidas (ONU), la ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno [2]. En resumen, la ciberseguridad asegura que se logren y se mantengan las propiedades de seguridad de los activos de la organización y de los usuarios frente a los riesgos asociados en el entorno digital. Estas propiedades de seguridad abarcan una o varias de las siguientes características: disponibilidad; integridad, que puede englobar autenticidad y no repudio; y confidencialidad. La UIT propone unos aspectos mediante los cuales se podría dividir el enfoque de la definición de ciberseguridad, que variará de acuerdo a los fines de quienes hacen uso del término. De esta manera, se podría concebir a la ciberseguridad como la misión de las fuerzas de seguridad para proteger o proteger la infraestructura, las redes, los datos y los usuarios nacionales, para, de esa manera, investigar, prevenir y abordar el delito digital (ciberdelito). También, puede definirse como una actividad de vigilancia realizada por una agencia de inteligencia. Se debe agregar, que el concepto ciberentorno aportado por la UIT resulta equivalente al de ciberespacio.

Además, para lograr una definición más sólida de la noción de ciberespacio que permita comprender y asimilar de manera eficaz las implicaciones mencionadas previamente, es crucial considerar el concepto de servicio, entendido como la prestación que un usuario o consumidor recibe de un proveedor. En consecuencia, el ciberespacio podría definirse como el conjunto de medios y de procedimientos basados en las tecnologías de la información y que se encuentran configurados para la prestación de servicios.

Una característica importante para examinar el tema del ciberpatrullaje, es la cuestión de la seguridad en sí. Este fenómeno posee una modalidad transnacional que suele soportar los procesos delictuales y/o criminales. En este sentido, la OEA ofrece una perspectiva sobre el progreso alcanzado desde su primera edición. Este organismo establece que las políticas de ciberseguridad son fundamentales para salvaguardar los derechos de los ciudadanos en el ámbito digital, tales como la privacidad, la propiedad, así como también, para aumentar y asegurar la confianza de los ciudadanos en las tecnologías digitales, y para permitirles sentirse confortables cuando acceden a dichas tecnologías [1].

Dada la temática escogida, resulta esencial discernir el concepto de seguridad en el ciberespacio. Por un lado, la seguridad se establece como una cualidad que percibe un determinado actor, respecto a una situación dada en su contexto. Por otro lado, la seguridad implica aquellas acciones llevadas a cabo por el actor en cuestión, a los efectos de alcanzar una situación ideal. En este sentido, la seguridad seria tanto una situación ideal que en forma simplificada podría caracterizarse como de ausencia de amenazas, o como el conjunto de medidas y políticas conducentes a ese objetivo [2]. De esta forma, al hablar de seguridad, es factible encontrar un conjunto de diversos términos, donde se destacan la seguridad informática, seguridad de la información y ciberseguridad. La información recopilada deberá limitarse estrictamente a lo necesario para caracterizar y gestionar los tipos de amenazas, evitando en particular la recopilación y procesamiento que puedan comprometer la privacidad de las personas. A tal efecto, se mantendrá una plataforma segura y confidencial de colaboración en materia de incidentes de ciberseguridad, con el objeto de agregar la información pertinente y, en conjunto con otros órganos públicos y privados, establecerá una red de trabajo.

Cuando se habla de ciberpatrullaje, entendido como la vigilancia y el monitoreo de actividades en el ciberespacio por parte de las fuerzas de seguridad, surgen diversas complejidades, dado que pueden vulnerarse ciertos derechos. Esta situación ha generado un intenso debate en Argentina.

Es importante indagar acerca de la constitucionalidad de estas prácticas de vigilancia por parte de las fuerzas de seguridad. En este sentido, se deben determinar las condiciones para comprender cómo se podrían establecer parámetros objetivos para construir una sospecha razonable que justifique la intrusión del Estado en la privacidad de los individuos a través de las tecnologías de la información y comunicación. Con el auge de la sociedad de la información y el uso intensivo de las tecnologías de la información y la comunicación (TIC), las distinciones sobre lo público, lo privado y lo íntimo se volvieron más ambiguas y difusas, y por ende, más problemáticas para el derecho, y, especialmente, para el derecho penal y la investigación del delito [4].

III. IMPORTANCIA DE LA REGULACIÓN

Para realizar una labor sólida y transparente sobre este tema, es crucial establecer una legislación que regule adecuadamente el ciberpatrullaje. Dicha normativa debe ser precisa y proporcionada, asegurando que las garantías procesales y los derechos humanos sean respetados. Es imprescindible, como se ha visto, una normativa asentada en una base que no vulnere los derechos de las personas, y para ello es vital observar las regulaciones que se han establecido a nivel internacional. En Estados Unidos, en la Unión Europea y en el Reino Unido, se ha constituido una serie de regulaciones sobre el tema analizado en este trabajo, que ha sido objeto de un pormenorizado análisis por

parte de muchos países del mundo. En los EE. UU. se han sancionado normativas como la "USA Patriot Act" en el 2001; ley Clarifying Lawful Overseas Use of Data Act (CLOUD Act) en 2018; la Ley de Protección de la Privacidad en Línea para Niños (Children's Online Privacy Protection Act, COPPA) en 1998. En la Unión Europea se sancionaron normativas como el Reglamento 2016/679 en 2018; este reglamento es conocido como el Reglamento General de Protección de Datos de la Unión Europea (General Data Protection Regulation, GDPR); mientras que en 2002 se promulgó la Directiva sobre Privacidad y Comunicaciones Electrónicas de la UE (ePrivacy Directive). Por su parte, en el Reino Unido se sancionó la Ley de Poderes de Investigación del Reino Unido de 2016 (Investigatory Powers Act 2016). En la región sudamericana, es importante mencionar el caso de Brasil, particularmente, la sanción en 2018 de la Ley General de Protección de Datos Personales de Brasil (LGPD), que fue aprobada por el Parlamento de Brasil como Ley N.º 13.709 en agosto de 2018.

Luego de lo presentado hasta aquí, parece relevante pensar una manera eficiente que permita indagar sobre el ciberpatrullaje, no para condenar su práctica, puesto que es una herramienta necesaria en estos tiempos, sino para velar por los derechos de las personas, que en muchas ocasiones se ven vulneradas debido al incorrecto manejo que hacen las fuerzas de seguridad mediante este tipo de vigilancia.

Por lo tanto, a partir de lo analizado en la primera parte de este trabajo, se puede sintetizar una idea de lo que se podría esperar de una sociedad en la que exista un ciberpatrullaje sólido y efectivo, pero que respete y se ajuste a una serie de reglas que garanticen la privacidad de las personas. De este modo, es menester pensar una regulación que podría ser implementada por cualquier país que desee constituir una legislación segura que vele por los derechos de las personas en los casos de monitoreo por ciberpatrullaje.

Argentina podría inspirarse en las normativas internacionales y regionales como base, y luego desarrollar métodos apropiados y específicos que se ajusten a su realidad, para asegurar que el ciberpatrullaje no afecte de manera negativa los derechos personales y la privacidad de los individuos. En este sentido, por ejemplo, se podría tomar lo esgrimido por el CLOUD Act para permitirle a las autoridades nacionales que obliguen a las empresas tecnológicas con sede en el país para que suministren los datos solicitados que se encuentran almacenados en los servidores, independientemente de si estos datos se encuentren almacenados en el país o, en su defecto, en el extranjero.

En Argentina, el ciberpatrullaje no está legislado específicamente, pero las actividades de prevención están amparadas bajo el "Protocolo General de Actuación para las Fuerzas de Seguridad y Policiales en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos" creado en 2016 y que ha quedado efectivo a partir de la Resolución 144/2020. Además, el Ministerio de Seguridad de Argentina ha propuesto un protocolo de ciberpatrullaje que se desarrolló en consulta con organizaciones de derechos humanos y sociales [5]. El ciberpatrullaje desempeña un papel fundamental en la seguridad del ciberespacio. No obstante, su implementación debe realizarse de manera que se respete y proteja la privacidad de las personas. Las leyes internacionales como el Patriot Act y el CLOUD Act, así como las regulaciones argentinas, proporcionan un marco dentro del cual se puede lograr este equilibrio. Sin embargo, es crucial que se mantenga un diálogo continuo y se realicen modificaciones según sea preciso para asegurar la protección tanto de la seguridad como de la privacidad.

Como se ha señalado anteriormente, un buen ejemplo para ser tomado como modelo es el Reglamento General de Protección de Datos europeo, la ley GDPR de la UE. Adaptando esta ley a la realidad de Argentina, se podrían proteger los datos personales y la forma en la que las organizaciones los procesan, almacenan y, finalmente, destruyen, cuando esos datos dejan de ser útiles. Una de las peculiaridades de esta ley es el principio de *accountability* (o responsabilidad proactiva) que sostiene que el responsable del tratamiento de datos no sólo debe cumplir con la normativa de protección de datos, sino que también debe poder demostrarlo y rendir cuentas de su proceder [5].

A pesar de la importancia del ciberpatrullaje, es fundamental que se lleve a cabo respetando la privacidad de las personas. La privacidad es un derecho humano fundamental que debe ser protegido, incluso en el ciberespacio. Por lo tanto, las actividades de ciberpatrullaje deben estar sujetas a regulaciones que garanticen el respeto a la privacidad. Para alcanzar un equilibrio entre la seguridad y la privacidad, es crucial establecer normativas claras y transparentes para el ciberpatrullaje. Estas normativas deben determinar qué información puede recopilarse, cómo puede utilizarse y cuándo debe eliminarse. Además, es fundamental que aseguren que todas las actividades de ciberpatrullaje estén sujetas a supervisión y rendición de cuentas.

Ahora bien, el tema tratado en este trabajo es un tema que está en constante progreso, dado que la tecnología evoluciona de manera cotidiana. Por esta razón, es crucial fortalecer continuamente los mecanismos de control, ya que los delitos ocurren a velocidades rápidas y requieren nuevas herramientas para abordarlos.

Con respecto a esta cuestión, algo que debe ser tenido en consideración en lo que respecta al ciberpatrullaje tiene relación con nuevas tecnologías como la *big data* y la inteligencia artificial (IA), puesto que actualmente se utilizan estos instrumentos para asuntos de ciberseguridad. Es primordial, que se implementen abordajes legales que aseguren la transparencia y el control sobre estas tecnologías para minimizar los riesgos a los derechos de las personas, y esto incluye, claro está, a la privacidad. Es imprescindible que se prevenga sobre el riesgo de dependencia acrítica en los algoritmos, que, a lo largo del tiempo, podría conducir a una

peligrosa vigilancia masiva y, tal vez, a la discriminación [6]. Es crucial enfatizar sobre la transparencia de los mecanismos utilizados para abordar los problemas derivados del ciberpatrullaje, garantizando así un pleno respeto de los derechos humanos sin comprometerlos.

El último informe de Freedom House (organización no gubernamental con sede en Washington D. C., que conduce investigaciones y promociona la democracia, la libertad política y los derechos humanos.), indicó que las democracias han registrado un monitoreo masivo de la población a través de las agencias gubernamentales que se están utilizando para nuevos propósitos sin las garantías adecuadas [5]. Esto significa que los organismos gubernamentales han hecho un uso abusivo con respecto a las libertades civiles y también indica una marcada reducción del espacio en línea para el activismo cívico.

De este modo, se puede observar como el derecho a la privacidad contemplado en el artículo 12 de la Declaración Universal de los Derechos Humanos se ha visto desafiado por diversas conductas que los gobiernos, las empresas y los propios particulares han realizado con las fuentes abiertas, ámbito en el cual la frontera entre lo público y lo privado no se encuentra claramente delimitada [5]. En este sentido, es imprescindible una educación ciudadana con respecto a sus derechos relacionados con los datos personales y el ciberespacio, puesto que en ciertas ocasiones los mismos ciudadanos entregan su propia privacidad cuando, por ejemplo, se crean un perfil en alguna red social.

Por lo tanto, es fundamental que cada ciudadano fortalezca su responsabilidad activa y dinámica. Cada persona debe tomar el control de manera proactiva y decidir cómo actuar en cada situación, anticipándose a los eventos que puedan surgir. ¿Por qué es importante esto? Porque las herramientas tecnológicas se han instalado en la sociedad y se quedarán instaladas allí, arraigadas. De este modo, es importante que se incremente la consciencia de cada ciudadanos, pero también debe consolidarse la eficiencia y la transparencia de las distintas agencias de control del Estado. Para ello, como se pudo advertir a lo largo de este trabajo, es necesario crear una legislación vigorosa que regule el uso de herramientas de monitoreo de redes sociales por parte de los privados, los Estados y, especialmente, por sus fuerzas de seguridad. En definitiva, se debe indicar que el ciberpatrullaje es una herramienta esencial para mantener la seguridad en el ciberespacio. No obstante, su implementación debe realizarse de manera que se respete y se proteja la privacidad de las personas [6].

IV. VIGILANCIA Y VULNERACIÓN DE DERECHOS

Aparte de las normativas establecidas, es crucial abordar ciertos problemas, dado que actualmente algunas prácticas de monitoreo y vigilancia en el ciberespacio no están reguladas por los Estados debido a la falta de leyes y normativas estrictas que protejan los derechos humanos en materia de ciberseguridad. Principalmente, es imperioso destacar el rol sustancial que debe tener el Estado valiéndose de la ética, para hacer frente a estas problemáticas.

La ética en ciberseguridad y privacidad es un tema emergente en la ética como campo de estudio, y por lo tanto requiere una profunda reflexión por parte de los expertos en este país. Comprender estos problemas podría contribuir significativamente a mejorar la regulación del ciberpatrullaje y proteger los derechos individuales.

Es esencial sugerir un enfoque renovado para entender y reflexionar sobre los dilemas éticos relacionados con las tecnologías de la información, buscando así generar recomendaciones prácticas para la acción. Las sociedades que se encuentran interconectadas son las que han exigido su nacimiento y actuación, son ellas las que precisan y demandan un saber interdisciplinar para su acción en la vida pública, siendo un bien de primera necesidad para determinar la altura moral de una sociedad [7].

Por su parte, es perentorio profundizar sobre el tema de la privacidad, dado que la aceleración de la tecnología implica poder gestionar grandes cantidades de datos, así como también, de informaciones y conocimientos, lo que a su vez lleva consigo importantes problemas de seguridad y privacidad [8]. Si la tecnología de la información acelera sus pasos a un ritmo vertiginoso y se debe mantener la atención sobre la privacidad, también se debe priorizar la cuestión de la privacidad cuando se habla de ciberpatrullaje. Esta problemática debe ser planteada de esta manera, puesto que si bien es imprescindible que el Estado de un país coloque sus focos en asegurar los derechos sobre los datos de los usuarios del ciberespacio, y muchas veces, como se vio en este trabajo, esta tarea se realiza a través del ciberpatrullaje, esa protección no debe vulnerar la privacidad de los ciudadanos.

Lo esencial en este caso, es indagar no solo en las regulaciones sino en cómo se vulneran los derechos de las personas en cuanto a su privacidad, dado que ha quedado en manifiesto que a pesar de una normativa establecida, se pueden llevar a cabo ciertas acciones que vulneran los derechos de la privacidad de las personas. Esta situación, en muchos casos, puede llevar a una vulneración de los derechos humanos de la sociedad civil que se puede ver perjudicada por leyes que violenten la manera en que se ejecute el ciberpatrullaje.

En este sentido, las fuerzas estatales que se ocupan de la seguridad informática presentan herramientas cada vez más específicas para perseguir delitos que también se comportan bajo herramientas cada más modernas, transformándose en una suerte de competencia o carrera tecnológica, como sucede con el caso de la IA

En consecuencia, en el marco de la persecución policial contra problemáticas como la pedofilia o contra el *grooming* (acoso sexual de una persona adulta a una niña, un niño o un

adolescente por medio de internet), las fuerzas se valen de la IA para construir perfiles falsos que, con el objetivo de ser atrayentes para determinados tipos de criminales, son utilizados como señuelos. Algo similar sucede con los conocidos como *honey pots* o *honey monkeys*, aunque en estos casos el reclamo es el propio sitio web, creado ad hoc con idéntica finalidad [6]. Se debe aclarar, que los *honey pots* (o *honey monkeys*) son herramientas de seguridad informática implementadas en una red o sistema para ser el blanco de un potencial ataque informático, con el fin de detectarlo y recabar información tanto sobre el ataque como sobre el atacante. En los dos supuestos se corre el riesgo de que el margen con la provocación policial se desdibuje en un exceso y se frustre el proceso.

Hay un punto que es central en toda esta cuestión, y es el de la protección de los derechos de las personas con respecto al ciberpatrullaje. Es sustancial atender el tema de los derechos humanos, porque son derechos que se encuentran protegidos, es decir, son derechos inalienables y fundamentales que todo individuo detenta por el mero hecho de ser humano y no pueden ser vulnerados con motivo de ciertos monitoreos específicos en materia de ciberseguridad. Cuando se llevan a cabo tareas de ciberpatrullaje, los integrantes de las fuerzas de seguridad monitorean de forma masiva e indiscriminada palabras claves en publicaciones de usuarios de redes sociales con la supuesta finalidad de "anticiparse a la comisión de delitos". Tales prácticas, que implican la observación de lo que las personas publican sin definir previamente qué se busca y a quienes se observa, son conocidas como "excursiones de pesca" y están estrictamente prohibidas por leyes locales e internacionales. Estas prácticas no cumplen salvaguardias básicas de derechos humanos tales como la legalidad, la necesidad y la proporcionalidad [9].

Estas acciones se encuadran en el marco de lo que se conoce como inteligencia de fuentes abiertas (*open-source intelligence*, OSINT) e inteligencia en redes sociales (*social media intelligence*, SOCMINT). ¿En qué medida corre riesgo la libertad de una persona cuando las fuerzas de seguridad realizan este tipo de operaciones? Cuando se realiza el monitoreo de, por ejemplo, las redes sociales por parte del gobierno implica importantes riesgos para la privacidad y la libertad de expresión de los usuarios [9]. Aquí se plantea una disyuntiva evidente: las normativas que se legislen sobre estos temas deben ser claras de manera manifiesta, puesto que la línea que delimita a la vigilancia de la protección es muy difusa. Este reparo ya fue planteado por el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) cuando examinó el tema del Protocolo de la Resolución Nº 144/2020 del Ministerio de Seguridad de la Nación. Sobre este aspecto, es necesario mencionar que el protocolo propicia otra discusión relativa al encuadre debido a estas actividades: ¿son tareas de prevención del delito o tareas de inteligencia? Atento al impacto de estas prácticas en nuestros derechos fundamentales, en particular la afectación a los derechos de libertad de expresión y privacidad, es necesario que la naturaleza jurídica de la actividad esté claramente establecida [10].

Si no queda delimitada categóricamente esa división, la vulneración de los derechos humanos se volvería muy evidente. En el caso de Argentina, la Constitución y los tratados internacionales de los derechos humanos, establecen una serie de garantías procesales que protegen a los individuos frente a la acción del Estado. Entre estas garantías se encuentran: el derecho a la privacidad, la presunción de inocencia y el debido proceso. El ciberpatrullaje, por su naturaleza, puede entrar en tensión con estos derechos, puesto que implica una forma de vigilancia que podría considerarse invasiva.

Para profundizar sobre este aspecto importante del tema analizado en este trabajo, es fundamental reparar en la trascendencia de la inteligencia de fuente abierta (OSINT), que es una práctica que se encuentra generalizada y que es incompatible con el estado de derecho. Es fundamental indicar, que la inteligencia de fuente abierta vulnera dos aspectos elementales. Un aspecto que se ve vulnerado es la privacidad de las personas. Puesto que las personas, por más que saben que sus expresiones en la esfera pública pueden llegar a ser monitoreadas, como pueden ser las redes sociales, tienen una expectativa de privacidad en la que esperan que no se haga seguimiento de sus expresiones, ni se recolecte ni se haga un tratamiento de esa información porque eso constituye tareas de inteligencia. Otro aspecto que podría verse vulnerado, se evidencia claramente cuando la inteligencia de fuente abierta ejerce una forma de condicionamiento del discurso público, puesto que esto posee un impacto sobre el derecho de libertad de expresión de las personas. Como ejemplo de este punto, se pueden mencionar acciones de ciberpatrullaje que conllevan a allanamientos y a detenciones de personas por sus expresiones de "violencia política" en ciertas redes sociales [11].

Lo que los organismos de defensa de los derechos de las personas reclaman, es que en la realidad se impone una notoria diferencia, y es que las autoridades "parecen desaparecer" cuando las personas se hallan vigiladas a través del ciberpatrullaje. En concreto, las personas no saben que son vigiladas ni cómo son vigiladas. ¿Por qué sucede esto? Porque no se puede advertir, observar, percibir lo que hacen los que vigilan, ni tampoco cómo lo hacen. Las personas no conocen, tampoco, qué hacen con la información que las fuerzas de seguridad toman de sus redes sociales cuando son vigiladas, ni cómo utilizan esa información.

Es por estos motivos que se cree necesario regular de manera eficiente el ciberpatrullaje para que se lleve a cabo de manera protegida y respetando los derechos humanos, para que las personas puedan conducirse en internet de manera segura, conociendo los límites y certezas. Asimismo, lo más importante es establecer que si la persona comete un delito,

sepa cuáles son las penas por ese delito cometido.

La posibilidad de cometer abusos sobre los derechos humanos está latente constantemente mediante el uso del ciberpatrullaje, y por este motivo es imprescindible elaborar procedimientos de vigilancia que deberán permanecer abiertos al escrutinio público y ser revisados regularmente. Sin esta condición, la confianza de la sociedad en el gobierno puede verse seriamente afectada [9]. Además, es insoslayable comprender, que si bien es necesaria la vigilancia dada la cantidad de delitos que se cometen en las redes con cada vez mayor asiduidad, no deben utilizarse mecanismos en base a engaños. En definitiva, las autoridades no pueden obtener acceso a información usando perfiles falsos como señuelo [9].

Para prevenir este tipo de abusos, los programas para el monitoreo de redes sociales no se pueden implementar o llevar a la práctica de facto. Por el contrario, deben ser puestos a prueba, probados, sometidos a un estricto examen de forma generalizada. Las fuerzas que realicen el ciberpatrullaje deben ser entrenadas y capacitadas, y deben estar preparadas para generar reportes cotidianos sobre el empleo y la competencia de esa clase de programas. Dichos programas de vigilancia deberán, al mismo tiempo, ser sometidos a auditorías de rutina y el resultado final deberá estar disponibles para el público para su revisión [9]. Sería relevante atender los requerimientos del CELS, que propone una serie de observaciones que pueden llegar a aportar una eficiente política de seguridad en materia de seguridad informática, que se establezca en consonancia con los valores democráticos y tipificados de los derechos humanos. Este organismo, recomienda que las fuerzas federales de seguridad dejen de llevar a la práctica actividades de vigilancia de carácter indiscriminado en fuentes abiertas. A su vez, se cree imperioso que se constituya una sólida y contundente normativa general que discuta los protocolos para todas las policías provinciales [12].

En el mundo de las leyes, las autoridades solo pueden obrar de acuerdo a lo que les está deliberadamente permitido. Esta regla es el principio de legalidad y es una de las bases más elementales de los sistemas jurídicos democráticos modernos [13]. El ciberpatrullaje parece ser una medida de vigilancia estatal, la cual sería algo que se encontraría prohibido de hecho sin un marco que la regule. De este modo, la Ley de Inteligencia Nacional (25.520) es clara en su artículo 4° (incisos 2 y 3) en prohibir exactamente el tipo de actividades que se realizan por medio del ciberpatrullaje [13]. Siguiendo este tema, se puede indicar que dado que la vigilancia en internet se engloba dentro del ámbito de la ciudadanía y de la libertad de expresión, debe ser razonable y apropiada para ser considerada una restricción adecuada.

Actualmente, más allá de las regulaciones que se establecieron en países puntuales y que se han mencionado en este trabajo, hay un marco internacional que garantiza que la vigilancia respete los derechos humanos. Particularmente, se hace referencia a los *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones*, un texto creado por asociaciones ciudadanas de todo el mundo para determinar cómo las normas y estándares internacionales de derechos humanos se aplican en el contexto de la vigilancia de las comunicaciones Estos fundamentos sostienen que la vigilancia debe ajustarse a un conjunto de principios para respetar los derechos humanos. Entre los más destacados se deben destacar los principios de necesidad y proporcionalidad, según los cuales, la vigilancia debe ser la única forma para conseguir un objetivo legítimo y proporcionada con el objetivo pretendido [14].

Esto es un imperativo para los Estados, dado que no hay nada más importante que la libertad de expresión en la base de las naciones, aun en momentos de crisis de las mismas. Es por motivos como estos, que Amnistía Internacional ha indicado que a pesar de que los Estados estén atravesando tiempos extraordinarios o de crisis, el derecho de los derechos humanos sigue siendo aplicable. En efecto, el marco de los derechos humanos tiene por objeto garantizar un cuidadoso equilibrio de los distintos derechos para proteger a las personas y las sociedades en general [15].

El ciberpatrullaje es un mecanismo importante de las fuerzas de seguridad, para tener el control de ciertos delitos que se han visto generalizados a partir de internet. Sin embargo, ese mecanismo de monitoreo no puede violentar las garantías de los derechos de las personas, sino que deben ser empleados de manera cautelosa, profesional y sin un exceso del poder estatal. En su accionar, este poder debe limitarse a combatir el delito. No debe infringir los derechos humanos de tal manera que las personas sientan amenazada su libertad y se auto-censuren excesivamente por temor a ser vigiladas por dicho mecanismo de vigilancia.

CONCLUSIONES

Como se ha visto reflejado en este trabajo, la privacidad en el ciberespacio es un tema de creciente importancia en la era digital actual. Con el incontenible avance de la tecnología, y a partir de la omnipresencia de internet en la vida de los ciudadanos, las actividades en línea están cada vez más expuestas a la vigilancia y a la recopilación de datos por parte de diversas entidades, incluidas empresas, gobiernos y, también, por los ciberdelincuentes.

Para abordar estas preocupaciones y proteger la privacidad en el ciberespacio, es necesario adoptar un enfoque multidisciplinario que involucre a diferentes actores, incluidos los ciudadanos, las empresas, los gobiernos y las organizaciones internacionales. A nivel individual, es importante que las personas estén informadas sobre los riesgos para la privacidad en línea y tomen medidas para protegerse,

como utilizar contraseñas seguras, habilitar la autenticación de dos factores, actualizar regularmente el software y las aplicaciones, y ser selectivos sobre qué información comparten en línea. La privacidad en el ciberespacio es un tema complejo y multidimensional que requiere la atención tanto de académicos como de legisladores. Es crucial encontrar un equilibrio entre la innovación tecnológica y la protección de los derechos individuales para garantizar un entorno en línea seguro y respetuoso de la privacidad.

Asimismo, el ciberpatrullaje en Argentina presenta tanto oportunidades como desafíos. Mientras que puede ser una herramienta valiosa para prevenir el crimen y proteger a la sociedad, también es imperativo que su implementación no vulnere las garantías procesales y los derechos humanos que son fundamentales en una sociedad democrática. La clave está en la creación de políticas que armonicen la seguridad con el respeto a la dignidad y la libertad de las personas. El ciberpatrullaje en Argentina requiere de una legislación cuidadosamente elaborada que equilibre la seguridad y la privacidad.

REFERENCIAS

[1] Organización de Estados Americanos, Documentos claves de la OEA sobre ciberseguridad. Banco Interamericano de Desarrollo, 2020.
[2] M. C. Bartolomé, La seguridad internacional en el siglo XXI, más allá de Westfalia y Clausewitz, ANEPE, 2006.
[3] Unión Internacional de Telecomunicaciones (UIT). Recomendación X.1205. Aspectos generales de la ciberseguridad. Aprobada en 18 de abril de 2008.
[4] M. Monte y S. I. Sánchez, "Tensiones constitucionales entre el derecho a la intimidad y el ciberpatrullaje en la investigación criminal. Análisis del Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas", Revista Pensamiento Penal, 2021.
[5] N. Ybañez, "Ciberpatrullaje: ¿cuál es el límite de las fuerzas de seguridad?", El Economista, 2020.
[6] P. Martín Ríos, "Empleo de big data y de inteligencia artificial en el ciberpatrullaje: de la tiranía del algoritmo y otras zonas oscuras", Revista de los Estudios de Derecho y Ciencia Política, N.º 36, 2022.
[7] J. Romero Muñoz, "CiberÉtica como ética aplicada: una introducción". Dilemata, N.º 24, pp. 45-63, 2017.
[8] P. R. Palos-Sánchez, R. Robina Ramírez y L. Cerdá Suárez, "Ética de la reputación online, marca personal y privacidad en el cloud computing: protección de los usuarios frente al derecho al olvido", Biblios, N.º 71, pp. 17-31, 2018.
[9] G. Pisanu, "Ciberpatrullaje en Argentina: los riesgos del monitoreo de redes sociales para los derechos humanos". Access Now, 2023.
[10] Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), "Protocolo de Ciberpatrullaje en fuentes abiertas", CELE. Observatorio Regional, 2020.
[11] D. De Amo, "Ciberpatrullaje: los expertos creen que es una práctica peligrosa y que pone en riesgo la libertad de expresión", Fundación Vía Libre, 2020.
[12] Centro de Estudios Legales y Sociales (CELS), "Sobre el «Proyecto de protocolo de ciberpatrullaje»", CELS, 2020.
[13] V. Chorny, "Detenido por tuitear: el ciberpatrullaje contra los derechos humanos en Argentina", R3D: Red en Defensa de los Derechos Digitales, 2020.
[14] Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, "13 Principios", 2013.
[15] Amnistía Internacional, "Los Estados deben respetar los derechos humanos al emplear tecnologías de vigilancia digital para combatir la pandemia", Amnesty, 2020.

Protección de datos personales: Aspectos, panorama actual y su implementación en las Universidades Nacionales

Sequeira, Martin Julián

UNLaM (sequemartin1999@gmail.com)

***Resumen*— Este trabajo explora las implicancias del derecho a la protección de datos personales desde su inclusión en la reforma constitucional de 1994 y la Ley 25.326 hasta la situación actual. Asimismo, se analizará la figura del Delegado de Protección de Datos Personales, que, aunque no esté implementado legislativamente, es reconocido por la Agencia de Acceso a la Información Pública y en diversos proyectos de reforma. Por otro lado, se evaluará la viabilidad de implementar esta figura en universidades nacionales, teniendo en cuenta la Ley de Educación Superior y la Resolución 40/2018.**

***Abstract*-- This paper explores the implications of the right to personal data protection from its inclusion in the 1994 constitutional reform and Law 25.326 to the present situation. It will also analyze the role of the Data Protection Officer, which, although not legislatively established, is recognized by the Agency for Access to Public Information and various reform projects. Additionally, the feasibility of implementing this role in national universities will be assessed, considering the Higher Education Law and Resolution 40/2018.**

I. INTRODUCCIÓN:

El avance de las nuevas tecnologías de la información y la comunicación ha traído consigo una serie de desafíos significativos que las organizaciones deben enfrentar en términos de ciberseguridad y protección de datos. La expansión del uso de herramientas digitales y la creciente dependencia de bases de datos para gestionar actividades en diversos sectores han intensificado la necesidad de abordar de manera efectiva las nuevas formas de criminalidad informática y garantizar la seguridad de la información almacenada.

A medida que las tecnologías evolucionan, también lo hacen las tácticas de los ciberdelincuentes, quienes explotan vulnerabilidades en los sistemas de información para llevar a cabo ataques que pueden comprometer la integridad, confidencialidad y disponibilidad de los datos personales. Esta situación ha llevado a un aumento en la preocupación por la protección de datos personales, un aspecto crítico dado que gran parte de la información gestionada por las entidades públicas y privadas se clasifica como datos personales.

Las universidades, en particular, se enfrentan a desafíos únicos en este contexto. Estas instituciones no solo manejan grandes volúmenes de datos personales relacionados con el alumnado, el personal docente y no docente, y las actividades de investigación, sino que también tienen la responsabilidad de garantizar la seguridad y privacidad de esta información. La naturaleza sensible de los datos que gestionan hace que la protección adecuada sea esencial para preservar la integridad de las operaciones académicas y administrativas.

Para abordar estos desafíos de manera efectiva, es crucial contextualizar tanto las normativas que regulan el funcionamiento de las universidades como el marco legal de protección de datos personales. Este análisis buscará propiciar una comprensión integral del derecho a la protección de datos personales. La protección de datos busca garantizar que la información personal sea gestionada de manera segura y respetuosa. Desde su incorporación en la Constitución Nacional en 1994, este derecho ha evolucionado, pasando de una visión centrada en la intimidad a una perspectiva más amplia que permite a los individuos controlar la información personal que sobre ellos se almacena y utiliza.En este contexto, la figura del Delegado de Protección de Datos Personales juega un papel crucial. Esta figura actúa como un nexo entre la autoridad de protección de datos y la organización, asegurando el cumplimiento de las regulaciones y políticas de privacidad. Además, entre otras tareas asesora sobre la correcta implementación de prácticas de protección de datos, supervisa los procedimientos internos, realiza auditorías y gestiona incidentes de seguridad relacionados con los datos personales.

Finalmente, es fundamental considerar el panorama actual y la implementación de estas prácticas en el ámbito universitario. Las universidades deben evaluar cómo integrar la figura del Delegado de Protección de Datos Personales en sus políticas de protección de datos. Aunque la legislación vigente en Argentina, no menciona explícitamente la figura del Delegado de Protección de Datos Personales, las resoluciones de la Agencia de Acceso a la Información Pública y los proyectos de reforma legislativa sugieren la incorporación de esta figura para asegurar una gestión adecuada de los datos personales.

A razón de lo expuesto es que en el presente trabajo se propone realizar un análisis de estos temas con el objetivo de compatibilizar el derecho a la protección de datos personales con la normativa que regula las universidades. Se examinará el alcance de las responsabilidades del Delegado de Protección de Datos Personales de datos personales y cómo estas pueden ser adaptadas al contexto universitario en Argentina.

[*] Revista Argentina de Trabajos Estudiantiles. Patrocinada por la IEEE.

II. PROTECCIÓN DE DATOS PERSONALES.

El derecho de protección de datos personales surge en nuestro ordenamiento jurídico con su incorporación en el artículo 43 de la Constitución Nacional en la reforma de 1994. La incorporación del instituto del amparo especial de protección de datos Personales o habeas data ampara desde su génesis el derecho a la Protección de datos Personales, la misma fue incorporada bajo el nombre de amparo especial, debido a la falta de habilitación expresa en la ley declarativa de reforma. Como menciona Oscar R. Puccinelli *para evitar impugnaciones constitucionales, se la guaresció bajo el molde de amparo, que era una de las figuras habilitadas para su incorporación en el artículo…pese a que su génesis se la vinculaba directamente con la otra figura habilitada, de la que tomó su nomen iuris: el habeas corpus.*[1]

Es importante mencionar que el alcance de la protección que brinda este instituto en principio estaba vinculado al derecho a la intimidad. Autores como el Dr. Quiroga Lavié han sostenido *que la reforma de 1994 incorporó en el artículo 43, párrafo 3° la acción de hábeas data que, en alguna de sus especies, funciona como medio de protección tanto de la intimidad como de la privacidad (remitimos al estudio especial del amparo como género de tutela dentro del subprincipio de control)*[2]. Hoy en día a 30 años de la reforma constitucional de 1994, dicho instituto es visto desde una mirada amplia y superadora. Ya no se vincula únicamente a la intimidad o la privacidad de las personas titulares de los datos personales, sino que, esto se modificó como resultado del gran procesamiento de datos que se dio inicialmente desde una perspectiva más analógica debido a el perfeccionamiento de la burocracia administrativa estatal y las entidades privadas encargadas de recopilar información, hasta el punto en que al día de hoy nos encontramos inmersos en un mundo completamente atravesado por el gran procesamiento de datos o mejor conocido como la "big data"[1]. En este contexto, la irrupción de la informática ha implicado una revisión del derecho a la intimidad debido a la creación de extensas bases de datos de naturaleza personal y la capacidad de cruzar la información contenida en ellas. Como bien señala el Dr. Molina Quiroga *el derecho a la intimidad no podía seguir considerándose simplemente la ausencia de información acerca de nosotros en la mente de los demás (el "déjenme solo"), sino que debía adquirir el carácter de un control sobre la información que nos concerniera, o sea la facultad del sujeto de controlar la información personal que sobre él figurara en los bancos de datos* [3]. Por esta razón es que la mirada actual para la doctrina de este derecho supera la concepción tradicional de la protección vinculada a la intimidad, debido a que actualmente la vulneración de este tipo de información abarca no solamente a los datos públicos sino a el honor, la identidad, la libertad, derechos de carácter económico, entre otros derechos. Por lo tanto, es reconocido como un derecho autónomo producto de la posibilidad de controlar la información de carácter personal que tiene el titular de los datos personales, mediante el uso de esta garantía constitucional como medio.

[1] El término "Big Data" se refiere al procesamiento de una gran cantidad de datos e información mediante el uso de herramientas digitales. Estas herramientas procesan Macrodatos que son una gran escala de información, de carácter compleja que precisa de un software informático específico para su procesamiento.

III. ¿QUÉ ES LA PROTECCIÓN DE DATOS PERSONALES?

Para comprender adecuadamente el alcance y la importancia de la protección de datos personales como un derecho fundamental, es esencial comenzar por definir qué constituye un dato personal en sí mismo. Los datos personales según el art. 2 de la ley 25.326 son aquella información de cualquier tipo referida a personas físicas o de existencia ideal, tanto determinadas como determinables. Por tanto, cuando nos referimos a un segmento de la realidad que constituye información, es decir, un dato, y este dato hace alusión a una persona física o jurídica, nos encontramos frente a lo que se denomina un dato personal. En este contexto, resulta relevante destacar que cualquier tipo de información que pueda estar relacionada con una persona, ya sea de forma directa o indirecta, se considera como dato personal. Es por esto que este tipo de información que suele ser almacenada por entidades públicas y privadas es de gran importancia a la hora de garantizar la protección de la información que almacenan. Aún más, la legislación al respecto establece que no es necesario que la persona esté completamente individualizada para que la información se considere como un dato personal, con el simple hecho de tener la posibilidad de poder identificarla mediante algún mecanismo técnico cumple con los requisitos para ser catalogada como tal. Podemos tomar como ejemplo una imagen de una persona, su dirección física o electrónica, número de teléfono, una nota de voz o cualquier otro tipo de información que pueda ser vinculada directa o indirectamente a un sujeto. Todos estos elementos debido a su vinculación o posible vinculación a un individuo son considerados datos personales. Es fundamental comprender que en la actual era digital, una gran cantidad de datos ya no se almacena en soportes analógicos. Estos datos están ampliamente dispersos y se guardan en una variedad de sistemas digitales alojados en servidores, que para el ordenamiento jurídico pueden ser considerados como bases de datos o bancos de datos, ya sea públicos o privados, dependiendo de la entidad o individuo que posea la titularidad de la información. Estos datos pueden ser utilizados para una amplia gama de propósitos, desde la prestación de servicios hasta la realización de análisis de mercado o incluso la prestación de servicios educativos como en el caso de las entidades educativas.

IV. PANORAMA ACTUAL DE LA PROTECCIÓN DE DATOS PERSONALES.

Si bien contamos con la consagración constitucional de la protección de datos personales esto no implica que la legislación actual que busca regular este derecho se encuentre

totalmente actualizada o alineada con los estándares internacionales, ni mucho menos adaptada a las cambiantes dinámicas que acompañan los avances vertiginosos de la tecnología. Es crucial reconocer que el mundo digital en el que vivimos está en constante evolución. Cada día, surgen nuevas tecnologías, aplicaciones y plataformas que transforman la manera en que interactuamos y compartimos información en sociedad. Este dinamismo tecnológico no solo nos brinda beneficios y oportunidades, sino que también plantea desafíos significativos en términos de protección de datos y privacidad. En este contexto, la legislación existente puede quedar rezagada o insuficiente para abordar los complejos escenarios que surgen del uso masivo de datos personales en línea, la proliferación de dispositivos conectados a internet, el desarrollo de tecnologías disruptivas como la inteligencia artificial y el aprendizaje automático e incluso las problemáticas que conlleva la cibercriminalidad. Es importante tener presente que la legislación que rige la protección de datos personales en argentina fue promulgada a fines del año 2000, lo que implica que ha estado en vigencia por más de 20 años. Asimismo, es oportuno mencionar que la Constitución cumplió 30 años desde su última reforma, momento en el cual se incorporó este instituto a nivel constitucional. A la luz de este marco normativo, se percibe una proximidad temporal en su promulgación, pero en lo que respecta al avance tecnológico, se observa una distancia considerable.

Nos encontramos en un contexto que la vertiginosa realidad digital nos enfrenta con desafíos impensados. Podemos tomar como ejemplo los diversos casos de filtraciones de datos personales, como lo fue la reciente filtración del RENAPER, en donde se publicó una base de datos con 65 millones de registros de datos personales[4]. Estos tipos de delitos perpetrados son realizados por la ciberdelincuencia que opera de manera organizada y sofisticada, realizando ciberataques a organismos públicos y privados con el objetivo de exponer las vulnerabilidades de los países y poner la información obtenida al alcance del público. Estos acontecimientos eran algo impensado en el momento en que la argentina decidió consagrar constitucionalmente la protección de datos personales. En aquel entonces, la Constitución y la posterior sanción de la Ley 25.326 no anticiparon la posibilidad de que los registros de todos los ciudadanos del territorio argentino pudieran quedar expuestos a cualquier persona con un solo click. Estos incidentes de filtración de información personal han suscitado un llamado de atención significativa por parte de los organismos públicos y privados que se ven afectados, así como también una consideración jurídica respecto a la responsabilidad estatal en este ámbito. Además, han intensificado el cuestionamiento sobre la idoneidad de la legislación vigente, reflejando la creciente preocupación entre los ciudadanos.

Es por esto que la actual ley de protección de datos personales se encuentra en un proceso de reforma llevado adelante por la Agencia de Acceso a la Información Pública que inició un proceso de debate participativo, abierto y transparente para la reforma de la Ley de protección de datos personales. Este proceso involucró la realización de mesas preparatorias y mesas de diálogo con diversos sectores de la sociedad. Como resultado de este proceso de participación y debate, se elaboró una Propuesta de Anteproyecto. Posterior a esto se le dió inicio a la fase de consulta pública a raíz de la resolución 119/2022 y la posterior resolución 145/2022 que postergó el plazo del periodo de consulta.

En cuanto a los avances que si se pudieron lograr podemos mencionar la sanción de la ley 27.483, la cual tuvo por objeto la adhesión de la Argentina al Convenio 108 del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. Este convenio representa un acuerdo internacional que establece pautas y principios para proteger los datos personales en el ámbito del tratamiento automatizado. Al ratificar este convenio, Argentina asume el compromiso de incorporar en su ordenamiento jurídico interno las disposiciones y principios estipulados en el mismo, con el fin de garantizar la protección de datos personales conforme a estándares internacionales reconocidos.

En lo que respecta a el objetivo del proceso de reforma legislativa es importante destacar que la finalidad principal es alinear las normativas nacionales de protección de datos personales con los estándares establecidos en normativas que son vanguardia como el caso del Reglamento General de Protección de Datos (GDPR) en Europa y la Ley General de Protección de Datos (LGPD) en Brasil. Estos marcos legales, reconocidos internacionalmente, establecen principios de protección robustos y mecanismos efectivos para garantizar la privacidad y seguridad de la información personal. Al lograr reformar nuestro marco jurídico y adecuar la legislación argentina a estos estándares, se lograría fortalecer la protección de datos de los ciudadanos.

V. Delegado de Protección de Datos Personales.

Una vez conceptualizado el alcance de la protección de datos personales y su panorama actual es importante profundizar en cuanto a la figura del Delegado de Protección de Datos Personales[5].

El Delegado de Protección de Datos Personales es el elemento central del cumplimiento de las disposiciones de protección de datos personales[6]. En el caso de Argentina, contamos con la ley 25.326, que, si bien no contempla en su articulado esta figura, su reconocimiento surge en base a distintas resoluciones emitidas por la Agencia de Acceso a la Información Pública, autoridad de aplicación de dicha ley. Además, está contemplada esta figura por el Proyecto de Ley de Protección de Datos Personales como obligatoria para todo aquel que realice tratamiento de datos, más aún como sostiene en su art. 44 inc a) “Si se trata de una autoridad u organismo público”[7].

En cuanto a sus funciones es aquel responsable que tiene a su cargo ser un nexo entre la autoridad de protección y la organización en la que convive. Su labor consiste en ser el encargado de llevar adelante el programa de privacidad del organismo, el cumplimiento de la regulación de datos personales y facilitar que las organizaciones cumplan con

dichas regulaciones. Además de ser un asesor de opiniones jurídicas, analizar la manera en que se transfieren datos personales intencionalmente, realizar un registro activo del tratamiento de datos que se realice, etc. Dentro de sus funciones principales encontramos aquellas relacionadas a realizar monitoreo de riesgo, llevar adelante un inventario y acompañar el desarrollo de las evaluaciones de impacto sobre los datos personales. Llevan adelante constantes auditorias y monitoreos para ver si existen desvíos en el programa de protección que lleven adelante.

En cuanto a si surge alguna problemática con los datos que se traten como puede ser una filtración de datos alojados en una base de datos, el delegado y la organización tienen que llevar adelante un reporte de incidente de seguridad, debido a que esto puede afectar los datos personales de distintos particulares. Es necesario que se realice un reporte ante la autoridad de protección de datos y se comunique a todas las personas afectadas por el incidente de seguridad, incluso si este incidente no haya producido aun daño alguno. Se le debe explicar al afectado cuales son los pasos que adoptar para que el titular evite que se produzca un daño a causa de la filtración de datos. Por ejemplo, si una empresa pierde datos de una tarjeta de crédito se debe dar aviso para que se comuniquen con la empresa y realicen las gestiones necesarias para cambiar los datos.

Si bien estas cuestiones no son obligatorias en Argentina, son resultado de la aplicación de los estándares internacionales provenientes del GDRP (Reglamento de Protección de Datos Personales) y la ley de Brasil LGPD (Ley General de protección de Datos Personales), siendo este un punto a seguir que se ve hoy en día plasmado en nuestro proyecto de reforma de la ley 25.326 y las distintas resoluciones que emite nuestra autoridad de aplicación de la ley.

VI. Implementación del Delegado de Protección de Datos Personales en las Universidades.

Es reconocido que el Delegado de Protección de Datos Personales es una figura que suele predominar en el sector privado, a razón de que es un elemento esencial para actores que se de dediquen al tratamiento masivo de datos, sin embargo, debemos tener en cuenta la **Resolución 40/2018** de la Agencia de Acceso a la información Pública. Dicha resolución en sus considerandos sostiene que: "para la eficacia de la política de tratamiento de datos personales es conveniente recomendar a los organismos estatales que posean bases de datos, la designación de un agente de planta permanente como "delegado de protección de datos personales" a fin de que cumpla la tarea de acompañar la implementación y control del cumplimiento de la política de protección de datos personales que se diseñe". Es por esto por lo que en su Art. 3 recomienda la designación de un agente bajo estos supuestos y aún más en el ANEXO 1 utilizado como "POLÍTICA MODELO DE PROTECCIÓN DE DATOS PERSONALES PARA ORGANISMOS PÚBLICOS" contempla en su modelo la posibilidad de contar con una línea directa de contacto con estos agentes para que pueda cumplir con su tarea. Debemos tener en cuenta entonces que si bien hoy en día en nuestro ordenamiento jurídico no es de carácter obligatorio la figura del Delegado de Protección de Datos Personales y tampoco lo es realizar tareas preventivas ante un incidente de seguridad sobre una base de datos personales, podría implementarse dicho actor en las políticas de protección de la información que diagramen los organismos públicos.

A la luz de esta resolución, resulta pertinente cuestionar si es adecuado implementar esta figura en las universidades nacionales. Por ende, es fundamental referirse a la Ley de Educación Superior, que regula la educación superior en Argentina. Dicha ley define los niveles y modalidades de la educación superior, incluyendo universidades, institutos universitarios y establecimientos de formación técnica y profesional. Asimismo, en su artículo 29 garantiza y consagra la autonomía de las universidades nacionales en cuanto a la gestión académica, administrativa y económica, permitiendo a su vez a las universidades definir sus planes de estudio, políticas de investigación y designación de autoridades.

En relación con este asunto, es importante señalar que las universidades, en virtud de su autonomía, tienen la capacidad de decidir si desean adaptarse a la resolución mencionada e implementar la figura del Delegado de Protección de Datos Personales. Esta decisión les permitiría establecer un agente encargado de velar por el cumplimiento de las normativas de protección de datos, garantizando así la seguridad y confidencialidad de la información sensible que manejan, tanto del alumnado como del personal universitario.

Aunque es sabido que en muchos organismos ya existen responsables designados para la seguridad de la información, esto no significa que sus funciones y responsabilidades se equiparen a las de un Delegado de Protección de Datos Personales. Los encargados de seguridad de la información suelen centrarse en la protección técnica y operativa de los sistemas, es decir, en garantizar que la infraestructura tecnológica sea segura y que los datos estén resguardados frente a amenazas externas, como ciberataques o fallos en la seguridad informática. Sin embargo, un delegado de protección de datos tendría un alcance más amplio y responsabilidades específicas que van más allá de la simple seguridad técnica. Este agente estaría encargado de asegurar el cumplimiento de las normativas sobre protección de datos personales, supervisando que los procesos de recolección, almacenamiento y tratamiento de la información se realicen de acuerdo con la legislación vigente. Además, tendría la obligación de velar por los derechos de los titulares de los datos, garantizando que se respeten principios como la confidencialidad, el consentimiento informado y el derecho a la rectificación o eliminación de la información cuando sea necesario. En este sentido, si en el futuro se llevara a cabo una reforma legislativa que incorporara formalmente la figura del Delegado de Protección de Datos Personales, y esta se convirtiera en una obligación derivada de una ley nacional, las responsabilidades de este agente estarían claramente definidas por dicho marco legal. Esta normativa podría establecer de manera precisa los alcances de su actuación, incluyendo las medidas de protección a implementar, las sanciones aplicables por el incumplimiento de sus obligaciones y la relación directa que tendría con las

autoridades de control en materia de datos personales. Este tipo de regulación podría cambiar sustancialmente el panorama actual, exigiendo a los organismos públicos y privados, incluidas las universidades y otras instituciones educativas, la designación de un Delegado de Protección de Datos Personales con funciones específicas y detalladas. De esta manera, se fortalecería el marco de protección de los datos personales, asegurando un tratamiento más riguroso y transparente de la información en diversos ámbitos, particularmente en aquellos que manejan grandes volúmenes de datos sensibles como el sector educativo.

Un ejemplo claro de esta situación se observa en España, donde universidades como la Universidad Autónoma de Madrid (UAM) han implementado la figura de un responsable para el tratamiento de datos personales en todas las actividades y servicios que brindan. Esto se enmarca en lo establecido por el Reglamento General de Protección de Datos, el cual exige que las instituciones que gestionan información personal adopten medidas de protección adecuadas.

Siendo así que en cumplimiento de lo dispuesto en el artículo 37.5 del Reglamento General de Protección de Datos, la UAM designó a Jesús Larena Millán como Delegado de Protección de Datos el 21 de diciembre de 2021[8]. El Delegado de Protección de Datos Personales desempeña un rol crucial dentro de la universidad, con responsabilidades que abarcan desde asesorar e informar a la institución sobre las mejores prácticas en el tratamiento de datos personales, hasta supervisar que los procedimientos internos cumplan con la normativa vigente en materia de protección de datos.

Además, el Delegado de Protección de Datos es un punto de referencia esencial para toda la comunidad universitaria. Su papel incluye atender las consultas de estudiantes, docentes y personal administrativo en lo que respecta a la protección de datos, así como facilitar el ejercicio de los derechos que otorga el RGPD, tales como el derecho al acceso, rectificación, supresión y oposición al tratamiento de datos. Asimismo, el Delegado de Protección de Datos Personales tiene la misión de concientizar y formar al personal de la universidad, fomentando una cultura de protección de la privacidad y la seguridad de la información dentro de la institución. Por último, es importante destacar que dicha figura colabora activamente con la Agencia Española de Protección de Datos (AEPD), actuando como enlace entre la universidad y la autoridad de control, lo que asegura que la UAM no solo cumpla con las normativas nacionales e internacionales, sino que también responda adecuadamente ante cualquier incidencia relacionada con la gestión de datos personales. Este ejemplo pone de manifiesto cómo las universidades pueden adaptarse a las normativas internacionales para proteger eficazmente la información de su comunidad.

VII. CONCLUSIONES:

En virtud de lo expuesto es destacable mencionar que la protección de datos personales se ha afirmado como un derecho fundamental en Argentina, especialmente desde su inclusión en el artículo 43 de la Constitución Nacional durante la reforma de 1994. Inicialmente asociado con el derecho a la intimidad, este derecho ha evolucionado significativamente con el avance tecnológico y la expansión de la "big data". La necesidad de proteger la información personal ha adquirido una dimensión más amplia, abarcando no solo la privacidad sino también la seguridad y el control de la información en un entorno digital en constante cambio. El concepto de protección de datos personales ha sido impulsado por la creciente sofisticación del procesamiento de información y la formación de grandes bases de datos, lo que ha llevado a una revisión de cómo entendemos la privacidad. Hoy en día, la protección de datos personales no abarca solamente la protección de la intimidad, sino que se extiende hasta incluso la capacidad de controlar cómo se recopilan, almacenan, y utilizan los datos personales. Esta evolución se refleja en el reconocimiento del derecho a controlar la información personal en una era de procesamiento masivo y tecnologías avanzadas. En este contexto, el Delegado de Protección de Datos Personales juega un rol crucial. Aunque la Ley 25.326, no menciona explícitamente esta figura, su importancia ha sido reconocida a través de diversas resoluciones de la Agencia de Acceso a la Información Pública y el Proyecto de Ley de Protección de Datos Personales. Según estas normativas, el Delegado de Protección de Datos Personales es una figura clave para asegurar el cumplimiento de las regulaciones de protección de datos y facilitar la implementación de políticas adecuadas en la organización. El Delegado de Protección de Datos Personales actúa como un puente entre la organización y la autoridad de protección de datos, gestionando el programa de privacidad de la entidad y supervisando el cumplimiento de las normativas. Además, el Delegado de Protección de Datos Personales debe facilitar el ejercicio de derechos por parte de los titulares de los datos y colaborar estrechamente con la autoridad de protección para resolver cualquier incidencia relacionada con la gestión de la información personal. A nivel internacional, el papel del Delegado de Protección de Datos Personales ha sido adoptado con éxito por diversas instituciones. Un ejemplo destacado es la Universidad Autónoma de Madrid (UAM), donde se ha implementado un Delegado de Protección de Datos Personales para asegurar el cumplimiento del Reglamento General de Protección de Datos. En el ámbito argentino, aunque la figura del Delegado de Protección de Datos Personales no es actualmente obligatoria, la Resolución 40/2018 de la Agencia de Acceso a la Información Pública, autoridad de aplicación de la ley 25.326, recomienda su designación para organismos públicos con bases de datos. Esta recomendación refleja la importancia de contar con un profesional especializado en la protección de datos, especialmente en un contexto donde las filtraciones de datos y los incidentes de seguridad son cada vez más comunes. La posibilidad de implementar un Delegado de Protección de Datos Personales en las universidades nacionales debería alinearse con la autonomía que les otorga la Ley de Educación Superior. Esta ley permite a las universidades definir sus políticas internas y gestionar de manera efectiva la protección de la información que manejan. La inclusión de un Delegado de Protección de Datos Personales podría no solo reforzar la seguridad de los datos personales de estudiantes y personal, sino también mejorar el cumplimiento de los

estándares internacionales en protección de datos. En conclusión, la implementación de un Delegado de Protección de Datos Personales en las universidades nacionales representa una posibilidad de lograr alinear a las casas de estudio con las mejores prácticas internacionales. Aunque no es una obligación legal en Argentina en este momento, la adopción de esta figura podría fortalecer significativamente el marco de protección de datos, garantizando una gestión más rigurosa y transparente de la información personal. Esta medida sería un paso hacia una mayor protección de la privacidad en el ámbito educativo, reflejando un compromiso con los derechos de los individuos y adaptándose a los desafíos contemporáneos en el manejo de datos personales.

REFERENCIAS

[1] Palazzi Pablo. Protección de Datos Personales: Doctrina y Jurisprudencia. Tomo 1. Oscar R. Puccinelli. La ley N° 25.326, de cara a su reforma integral: el proyecto elaborado en el marco del Programa Justicia 2020. CDYT. Buenos Aires. (2021). Pag 56.

[2] Quiroga Lavié, Derecho Constitucional Argentino. Rubinzal-Culzoni. (2001). Pág. 150.

[3] Eduardo Molina Quiroga. Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material. SAIJ. (2003). Pag 3.

[4] Disponible en: https://www.clarin.com/tecnologia/filtraciones-datos-personales-demandan-responsabilidad-discuten-ley vigente_0_2g8DEGGLMa.html. Último acceso 30/8/2024.

[5] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. ARTÍCULO 29: Directrices sobre los delegados de protección de datos (DPD). Pag 4.

[6] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS Creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995. ARTÍCULO 29: Directrices sobre los delegados de protección de datos (DPD). Pag 4.

[7] https://www.argentina.gob.ar/sites/default/files/proyecto_de_ley_de_proteccion_de_datos_personales_-_febrero_2023.pdf

[8] Disponible en: https://www.uam.es/uam/proteccion-datos/delegado-proteccion-datos. Ultimo acceso en 30/8/2024.

¿Cómo trabajar con un perito? El ABC para abogados y peritos

Autora: Silvina Ocampo, abogada UBA

SECURETIA, socampo@securetia.com

***Resumen*—El presente trabajo intenta ser una guía práctica y de referencia para los profesionales tanto del ámbito judicial como para los técnicos, analistas y/o ingenieros que deseen explorar las competencias de su título en las prácticas forenses.**

Para esto, en primer lugar, se evidenciará cuál es la importancia de conectar ambos saberes en un mundo cada vez más informatizado. En segundo lugar, se analizarán las similitudes y diferencias desde la mirada técnica y jurídica. Es decir, ¿qué aporta cada disciplina en torno a un proceso judicial? Estableciendo los límites y las formas de actuación. Y por último, se mostrará a partir de casos prácticos cómo trabajar en conjunto.

***Abstract*--This work attempts to be a practical and reference guide for professionals in both the judicial field and for technicians, analysts and/or engineers who wish to explore the competencies of their degree in forensic practices.**

For this, first of all, the importance of connecting both knowledges in an increasingly computerized world will be evident. Secondly, the similarities and differences will be analyzed from a technical and legal perspective. That is, what does each discipline contribute to a judicial process? Establishing limits and forms of action. And finally, it will be shown through practical cases how to work together.

I. INTRODUCCIÓN

El presente trabajo busca ser una referencia para los profesionales que, desde el ámbito jurídico, buscan comprender por qué la prueba pericial informática, que hoy en día incluye básicamente todas las nuevas formas de comunicación, tiene un rol crucial. En este sentido, es preciso saber: ¿Cómo debemos solicitarla?, ¿Qué preguntas son las apropiadas para que el perito pueda trabajar correctamente según el medio tecnológico disponible como prueba? y, ¿Cuáles son las preguntas pertinentes para que efectivamente la prueba sea útil?

Así mismo, el presente trabajo será de gran utilidad para aquellos que deseen incursionar en el sistema judicial como peritos porque se explicará brevemente cómo es el proceso judicial desde su aspecto procesal, la relevancia de la prueba pericial y qué es efectivamente lo que buscan los abogados al preguntar de tal o cuál forma.

Es importante destacar que el fin del trabajo es que sirva como un conector entre ambas disciplinas generando puentes para facilitar la comunicación entre saberes que a primera vista parecen ser contradictorios. Nos referimos principalmente a que en muchos procesos judiciales los letrados suelen pedir en forma general que se analicen por ejemplo “todos los correos electrónicos de casilla XXX” y esto es algo que termina demorando enormemente la prueba pericial además de ser inútil para los plazos del proceso judicial y para la claridad con el que juez podrá analizar la prueba. Debemos comprender que el saber en el caso de los peritos informáticos es técnico, preciso y conciso, y esto atenta contra las lecciones que aprendemos en la carrera de derecho, ya que, desde que ingresamos nos enseñan: siempre presenten toda la prueba. Bueno lo que debemos entender, es que en el caso de la prueba informática esto es completamente contraproducente y, en lugar de ayudarlo, ralentiza al punto de volverlo inoficioso.

A esto se suman otras dificultades que si bien son materia de futuros trabajos, es menester mencionarlas porque tienen una importancia crucial. En primer lugar, tenemos un código procesal que si bien intenta actualizarse, en el momento en que se creó no existían los medios digitales. En segundo lugar, el avance de las comunicaciones en las sociedades actuales es vital y prácticamente la mayoría de las pruebas está contenida en un soporte digital. Por último, por más que nos pese, los abogados estamos sesgados en la prueba física descrita por nuestro código procesal y lo que debemos entender es que el mundo cibernético tiene otras reglas completamente distintas y debemos debatir cómo darle un marco preciso para que efectivamente sea útil a los procesos judiciales. Creo que el principal problema es tratar de pensar con nuestras categorías un lenguaje que es radicalmente distinto y que necesita de nuevas reglas pero para hacer dichas reglas debemos entender cómo funciona. Los subtítulos del presente trabajo son expresiones típicas de mi labor entre ambos saberes que reflejan parte de la realidad de ambos mundos.

II. LO OBSOLETO DEL SISTEMA JUDICIAL Y EL CÓDIGO PROCESAL DESDE LA MIRADA TÉCNICA

Desde la mirada de los peritos y sus saberes específicos, la definición de nuestro código procesal en torno a la prueba pericial carece de completo sentido.

Incluso la forma en que los letrados solemos presentar la prueba pericial, por ejemplo, a través de conversaciones de Whatsapp o impresiones de mails resultan completamente inadecuadas para la labor pericial informática precisamente porque el lenguaje técnico tiene un lenguaje específico.

El inconveniente radica principalmente en que nuestro Código Procesal Civil Y Comercial De La Nación incluye a la prueba pericial dentro de la prueba documental y en su en su artículo 387 exige: "Las partes y los terceros en cuyo poder se encuentren documentos esenciales para la solución del litigio, estarán obligados a exhibirlos o a designar el protocolo o archivo en que se hallan los originales. El juez ordenará la

exhibición de los documentos, sin sustanciación alguna, dentro del plazo que señale"[1]. Obviamente si pensamos la cuestión en el momento que nuestro código procesal introdujo la prueba documental esto tiene sentido porque se refería a una prueba tangible, donde el debate era probar la veracidad de ese documento y, en tal caso, probar su validez. Ahora bien, si intentamos trasladar esto al mundo informático lo que vamos a descubrir es que ”La prueba digital es extremadamente volátil, sensible e intangible” [2]. Y que poco importa si presentamos el original o la copia porque se puede duplicar infinitamente el mismo archivo. Por otra parte, no tendríamos que llevar porque la información no es material o física sino que está almacenada en un dispositivo que es físico. Por este motivo, presentarle al perito las impresiones de las conversaciones de whatsapp o los mails para que analice no tiene ningún valor y es similar a querer respirar debajo del agua. La información que el perito puede y debe analizar es la información codificada en los diferentes lenguajes informáticos que no es el papel impreso que nosotros presentamos a fin de que el experto determine su autenticidad.

En mi experiencia como asesora de los letrados a la hora de pedir la prueba pericial informática muchas de las demandas suelen decir por ejemplo: Para el caso que la demandada niega explícita o implícitamente la veracidad de los aumentos que informa por el portal web, solicito se designe perito único de oficio a fin de expedirse sobre la autenticidad acompañados como prueba documental. Desde el punto de vista del Código Procesal Civil Y Comercial De La Nación esto tiene toda razón de ser, pero desde la mirada técnica es simplemente un papel impreso.

La función del perito es analizar la información codificada en diferentes lenguajes de programación y su labor consiste en primer lugar en obtener o adquirir esa prueba, peritarla y posteriormente conservarla a través de la cadena de custodia siguiendo los lineamientos de la norma ISO/IEC 27037:2012. Para poder cumplir con dicha finalidad el letrado deberá transmitir con claridad a dónde tendrá que dirigirse el perito. De más está decir, que esto no es a un papel impreso con imágenes sino que por el contrario es individualizar el dispositivo electrónico o la URL donde se encuentra alojado nuestra prueba.

Sin embargo, mientras que la prueba pericial informática esté contenida dentro de la sección documental, imprimir las conversaciones, imágenes o fotos, etc. va a seguir siendo válido desde el punto de vista del proceso judicial pero inútil a los fines de que el perito obtenga, perite y custodie la prueba que nosotros necesitamos para el proceso.

Cabe aclarar, que se vienen haciendo esfuerzos considerables por tratar de armonizar ambas disciplinas sobre todo desde el ámbito penal como la ley de protección del software, la ley de datos personales, la adecuación al Convenio de Budapest en torno a delitos informáticos a partir de la modificación del Código Penal en el 2008, la introducción de la ley de Grooming en 2013 o la adecuación del artículo 128 del Código Penal sobre tenencia de pornografía infantil, donde en todos los casos buscan garantizar un mayor acceso a la justicia a partir de comprender los nuevos paradigmas tecnológicos pero estás modificaciones aún están en deuda en las otras ramas del derecho y principalmente en nuestro Código Procesal. Incluso desde nuestro país se viene abordando el tema desde varias provincias y universidades que tienen como fin generar equipos de trabajo multidisciplinarios enfocados en trabajar colaborativamente.

III. ¿POR QUÉ ES TAN DIFÍCIL QUÉ EL PERITO ME ENTIENDA?

Simplemente porque no hablamos su idioma. A la hora de presentar la prueba en una demanda judicial los abogados solemos solicitar un perito informático a fin de que se expida sobre la validez de la prueba que adjuntamos como documental. Pues bien, aquí radica todo el inconveniente, tal como explique en el punto anterior las pruebas informáticas no son cosas son datos, o mejor dicho información almacenada en un lenguaje codificado que está alojada en un dispositivo electrónico. Por lo tanto, no es visible de forma clara para individuos que no tienen conocimientos técnicos. Entonces, ¿cómo podemos pedirle al perito que analice la prueba pericial si no hablamos su lenguaje? Muchas veces los abogados por temor a perder el proceso solicitan que se analice toda la prueba documental de la casilla XXX, o todas las conversaciones de whatsapp del número, o la página web de XXX, y qué respuesta obtenemos de los peritos: “No se puede acceder a la información solicita porque el sitio web no se encuentra disponible"

Y esto es precisamente porque no estamos preguntando lo que el perito puede efectivamente respondernos. En este aspecto, la ISO 27037 describe los procesos de actuación pericial para identificar, recolectar, adquirir y custodiar la prueba desde su aspecto técnico pero la norma no hace ninguna referencia a requisitos específicos de cada jurisdicción que se refieren a cuestiones como la admisibilidad, la ponderación probatoria, la pertinencia y otras limitaciones que controlan el uso de la evidencia digital en los tribunales de justicia [3].

Un ejemplo típico de esta situación es que el Portal del Poder Judicial sólo permite la carga de archivos en formato PDF y si el perito necesita subir un audio, un vídeo, una base de datos, una imagen no puede salvo que modifique el formato. Esto desde el aspecto jurídico ¿no sería alterar la integridad de la prueba que tanto buscamos custodiar?.

Otro ejemplo es cuando al perito le solicitamos que indique si tal individuo envió un correo electrónico a tal casilla, como si el perito pudiera analizar las acciones de los individuos. El perito nos podrá decir si de tal casilla se envió a otra casilla un mail, nos informará de la hora, la fecha, los servidores involucrados, y otros datos que se encuentren en las cabeceras de los correos electrónicos pero de ninguna manera nos podrá brindar información sobre el sujeto que realizó la acción.

Es importante que a la hora de armar nuestros puntos de pericia contemos con la opinión de los expertos porque en definitiva ellos podrán analizar lo que nosotros realmente necesitamos solicitar.

En síntesis, sin ir más lejos, el perito va a extraer los datos para analizarlos en relación a nuestros puntos de pericia. Si nosotros como letrados esperamos entender sus respuestas necesitamos saber manejar su lenguaje, de lo contrario nuestra prueba pericial se transformará en un montón de vocablos indescifrables y no sabremos qué hacer con esa información desperdiciando recursos, tiempo y dinero.

No debemos exigirle al perito que interprete los datos sacando conclusiones que son interpretativas y puntuales de nuestra disciplina sino pedirle la obtención de esos datos con la finalidad que sea útil al proceso. Por eso nuestras preguntas deben ser concisas, puntuales y en torno a la prueba específica.

IV. CONCLUSIÓN

Para obtener una prueba pericial que nos sea de utilidad en una demanda judicial debemos enfocarnos en preguntar de forma correcta y en el lenguaje correspondiente, de lo contrario sólo forzaremos categorías sin ningún resultado útil desperdiciando recursos, tiempo y dinero. Por eso es crucial que nos capacitemos y entendamos sobre las nuevas tecnologías.

En este aspecto, el presente trabajo busca generar puentes que nos inviten a lograr una buena comunicación donde prime el enfoque multidisciplinario principalmente teniendo en cuenta la importancia primordial que adquiere está prueba en las sociedades actuales. Para esto no debemos forzar a los peritos a que interpreten los datos como nos exige el sistema judicial sino que por el contrario, debemos comprender cuáles son sus funciones y qué nos pueden ofrecer en su actuación como la mano informática de la justicia.

REFERENCIAS

[1] Código Procesal Civil y Comercial de la Nación, Texto actualizado de la ley n° 17.454 (t.o. 1981). Buenos Aires: Honorable Cámara de Diputados de la Nación

[2] Carlos Christian Sueiro, El Derecho Penal en la era digital, Primera edición., A&C Ediciones Jurídicas S.A.C., Jr. Camaná N° 1043 - Of. 604 Plaza Francia - Cercado de Lima, 2018, pp.161.

[3] Santiago Roatta, María Eugenia Casco y Martín Fogliato "El tratamiento de la evidencia digital y las normas ISO/IEC 27037:2012¨ XXI Congreso Argentino de Ciencias de la Computación, Junín, 2015 http://sedici.unlp.edu.ar/handle/10915/50586

Agradecimientos

Queremos expresar nuestra sincera gratitud a todos los que hicieron posible la realización de la VIII Conferencia Nacional de Informática Forense, **InFo-Conf 2024**:

- A la Universidad Nacional de La Matanza (UNLaM), al Departamento de Ingeniería e Investigaciones Tecnológicas (DIIT), por su compromiso, organización y apoyo logístico.
- A la Red Universitaria de Informática Forense (Red UNIF), por impulsar este espacio de encuentro, difusión e intercambio entre profesionales, investigadores, docentes y estudiantes.
- A los disertantes, autores de trabajos, evaluadores, moderadores y asistentes que participaron activamente en las jornadas, contribuyendo con sus experiencias, conocimiento y participación al éxito del evento.
- A todas las instituciones, organismos y empresas que auspiciaron y patrocinaron esta edición, así como a aquellos que colaboraron en forma técnica, académica o logística.
- A los equipos de apoyo, voluntarios y personal administrativo que, detrás de escena, garantizaron el funcionamiento fluido del evento presencial e híbrido.
- Al equipo técnico, comunicaciones y difusión, y a todas las personas que compartieron materiales, hicieron posible la transmisión híbrida, coordinaron las aulas, la agenda y todos los detalles organizativos.
- A cada participante —ya sea en persona o en modalidad virtual— por su interés, compromiso y aporte. Su presencia y participación hacen que conferencias como esta tengan sentido y generen valor compartido.
- Finalmente expresar un agradecimiento muy especial al Ing. Alfredo Vázquez, quien durante años formó parte del DIIT-UNLaM y acompañó esta edición de la InFo-Conf 2024 como evaluador, siempre con una mirada rigurosa, dedicada y generosa, que resultó fundamental para fortalecer la calidad académica de nuestra producción. Nos dejó físicamente, pero su legado, su ética profesional y su pasión por la investigación continúan siendo una guía y un ejemplo.

Estamos convencidos de que gracias a la colaboración de todos los involucrados, **InFo-Conf 2024** logró su objetivo de fortalecer los lazos entre las disciplinas de informática forense, investigación criminal informática, ciberseguridad y derecho.

ISBN 978-631-6611-69-7