Licenciatura en Seguridad Pública

TESINA

El Sistema de adquisición de comunicación electrónica del departamento de Asistencia Tecnológica y Apoyo Investigativo de la Dirección de Investigaciones de la Policía de Mendoza. Preservación y análisis de datos de mensajería digital, protocolo de identificación, resguardo y presentación de informes analíticos, durante el periodo del 2019 al 2021

Estudiantes: Mauricio Raúl Carmona

Jesús Darío Cepeda

Director de Tesina: Lic. José Víctor Vega

Coordinación de Tesina: Lic. Graciela Matricani

Mendoza, marzo 2022

Agradecimientos

Principalmente a nuestras familias, esposas e hijas, que saben del compromiso institucional que tenemos, y la vocación de servicio que a diario ejercemos, llevando incluso a estar mucho tiempo a disposición laboral, sin atender las necesidades del hogar.

Al equipo que integra el Departamento de Asistencia Tecnológica y Apoyo Investigativo, dado que a diario pone de manifiesto su compromiso con la función, tratando de llevar seguridad a la ciudadanía, y tratar de general justicia a las víctimas de los delitos que les ocupa investigar

A nuestro Director de Tesina que además es nuestro Superior diario, quien nos incita y provee de las herramientas para que podamos brindar respuestas.

A la Licenciada Graciela Matricani, y la Sra. Mónica Ferreira, quienes nos han apoyado compartiendo sus conocimientos, en este proceso de aprendizaje.

Al personal policial y judicial que constantemente se apoya en nuestros servicios, depositando su confianza, situación que nos reconforta plenamente.

A todos ellos muchas gracias por todo el aporte constante, la unidad y disposición.

Introducción

Las nuevas tecnologías, y en especial las relacionadas a las telecomunicaciones, han revolucionado el mundo de la comunicación en general, imponiendo adelantos a la sociedad, y exigiéndonos que debamos adaptarnos a nuevos, profundos y rápido cambios, para no quedar fuera de este sistema y sus tendencias.

Hoy se mantienen nuevas relaciones a través de redes sociales como Facebook, Instagram, Snapchat, Telegram, WhatsApp entre otras, donde se intercambian contenidos de todo tipo. Esto pone de manifiesto que las formas de comunicarse, han evolucionado y con ellas la modalidad de cometer delitos.

Con el advenimiento de las Tecnologías de la Información y la Comunicación (TIC), se modificaron los mecanismos de comunicación, mutando a todas las instancias sociales, incluida la de la seguridad. Esto ha favorecido la aparición de nuevos delitos, y nuevos métodos de interrelación entre criminales, a efectos de burlar y no ser atrapados por los organismos de seguridad.

En materia de persecución penal vinculadas a unidades especializadas, la historia nos permite conocer que el 7 de setiembre de 1898, el entonces Jefe de Policía de la Provincia de Mendoza Dr. Luis Lagomaggiore, a través de un decreto, da origen a la Comisaría de pesquisa, la que posteriormente se definiría como Dirección de Investigaciones, con el fin de llevar a cabo investigaciones profesionales de crímenes y conductas antisociales.

Su evolución ha sido constante y ha cambiado de acuerdo a la evolución de los eventos delictivos. Esto a su vez, implicó que se fuera profesionalizando el personal conforme a los avances científicos y tecnológicos, con el fin único de alcanzar el mayor grado de certeza, sobre los hechos que se ponen a consideración de la justicia.

Entendiendo esta dinámica, y vislumbrando la problemática, respecto del avance exponencial en materia tecnológica, dentro de dicho organismo se dio origen al Departamento de Asistencia Tecnológica y Apoyo Investigativo (D.A.T.A.I.), el cual está encargado de gestionar, centralizar, analizar e informar todo tipo de datos en materia tecnológica e informática para ser presentado en un proceso judicial.

Evidentemente, hemos pasado de una sociedad industrial a una sociedad de la información, en la cual existe todo un mundo de relaciones controlado por la tecnología, creando un escenario en el cual la implementación de las TIC ha creado nuevos hábitos, y también nuevas formas de cometer delitos. En este punto es importante realizar una distinción del uso de la tecnología como medio de comisión de hechos delictivos, pero también como objetivo del delito.

Las características particulares de las TIC, dificultan en gran medida, la detección, los procedimientos y las formas de encontrar pruebas. Además de ello, pensemos que algunas tecnologías se pueden programar a distancia, lo que permite borrar indicios o incluso, introducir pistas falsas que dificulten la identificación de autores, como también el lugar del ciberespacio en el cual se ha iniciado el hecho delictivo.

Frente a este contexto, el legislador ha debido reformular y crear nuevas normas legales logrando encontrar soluciones a algunas problemáticas, sin olvidar que, en materia penal, siempre se corre detrás del hecho delictivo, sobre todo en función de la naturaleza de los mismos. En el caso de las TIC, los cambios constantes, y la gran variedad de posibilidad de realizar hechos delictivos, profundizan aún más esta situación en cuanto a la creación de nuevos delitos.

Además del interés profesional que supone el gran inconveniente planteado, a nivel institucional, es decir, Policía de Mendoza, más precisamente Dirección Investigaciones en su punta de lanza, como lo es el Departamento de Asistencia Tecnológica y Apoyo Investigativo, surge como anticipación de sentido estudiar, analizar y encontrar de alguna manera mecanismos, para el tratamiento de esta situación, en procura de obtener herramientas que posibiliten la recolección de información para ser presentados ante los tribunales judiciales requirentes, a fin de ser un elemento de prueba eficiente y eficaz en un proceso legal.

En relación con lo expuesto, nos hemos planteado las siguientes preguntas de investigación:

- ¿Cómo afecta la falta de un protocolo de recuperación y recolección de datos digitales de un dispositivo electrónico, en la presentación judicial de

informes técnicos por parte del Departamento de Asistencia Tecnológica y Apoyo Investigativo de Dirección Investigaciones, entre el año 2019 y 2021, en la Provincia de Mendoza?

- ¿Cómo impacta la presentación de informes técnicos, por parte del Departamento de Asistencia Tecnológica y Apoyo Investigativo perteneciente a Dirección Investigaciones, en el proceso de investigación con el aporte de evidencia real y material, en el periodo comprendido entre el año 2019 y 2021, en la Provincia de Mendoza?
- ¿Qué son las tecnologías de la información y la comunicación (TIC)?
- ¿Cuáles son los protocolos de recolección de evidencia digital existentes en Argentina y en la provincia de Mendoza?
- ¿Qué marco regulatorio legal existe en Argentina y en la provincia de Mendoza respecto de la obtención de datos en dispositivos electrónicos como material probatorio en un proceso judicial?
- ¿Qué tipo de mecanismos se utilizan en la actualidad como cadena de custodia en la provincia de Mendoza en materia de evidencia digital?
- ¿Existe protocolo o guía para el proceso de análisis de datos y presentación de informe técnico, en la provincia de Mendoza?

El objetivo general que guía el presente trabajo es:

- Analizar el Sistema de Comunicación Electrónica que tiene el departamento de Asistencia Tecnológica y Apoyo Investigativo en cuanto a la, obtención de datos de redes de mensajería digital, protocolo de identificación, resguardo, análisis y presentación de informes analíticos de la Dirección de Investigaciones de la Policía de Mendoza, en el período 2019 al 2021, en la provincia de Mendoza.
- Visibilizar la importancia que tiene la implementación de un protocolo de recuperación y recolección de datos digitales de un dispositivo electrónico,

para la presentación judicial de informes técnicos, por parte del Departamento de Asistencia Tecnológica y Apoyo Investigativo perteneciente a Dirección Investigaciones de la Policía de Mendoza.

Los objetivos específicos son:

- Definir conceptualmente Tecnología de la Información y la Comunicación (TIC) y sus características generales.
- Conocer los protocolos de recolección de evidencia digital existentes en Argentina y en la provincia de Mendoza.
- Señalar el marco regulatorio legal existente en Argentina y en la provincia de Mendoza respecto de la obtención de datos en dispositivos electrónicos como material probatorio en un proceso judicial.
- Establecer los mecanismos que se utilizan en la actualidad como cadena de custodia en la provincia de Mendoza en materia de evidencia digital.
- Precisar cómo se lleva a cabo el proceso de análisis de datos y presentación de informe técnico del Departamento de Asistencia Tecnológica y Apoyo Investigativo perteneciente a Dirección Investigaciones de la Policía de Mendoza.

Metodológicamente, esta es una investigación decampo, con un diseño cualitativo y, por lo tanto, flexible ya que combina diferentes técnicas. El alcance es descriptivo, dado que busca dar cuenta de las formas como se obtienen los ciberdatos que permiten esclarecer diferentes hechos delictivos, cuál es su procesamiento y cuidado, y sobre todo, la utilidad que estos presentan para la justicia. Los estudios de alcance descriptivos buscan describir, como lo dice su nombre, este tipo de pruebas.

Los estudios descriptivos permiten identificar propiedades y características de los grupos de personas y/o fenómenos estudiados que son sometidos al análisis del investigador. Siguiendo a Montbrún Ruggiero (2013), las investigaciones de alcance descriptivo tienen como objetivo, dar cuenta de eventos o circunstancias que corresponden

a un mismo tipo de fenómenos, mediante procedimientos metódicos que muestren el objeto de análisis proveyendo una enrome cantidad de material que posibilita el acopio de datos.

Para su desarrollo nos hemos valido de estadísticas de intervenciones que se han realizado mediante la utilización de tecnología como cámaras de seguridad, investigación en dispositivos electrónicos y casos relevantes que puedan dar cuenta de los procedimientos. Se incluyen entrevistas realizadas a fiscales de la provincia de Mendoza.

Las fuentes primarias provienen de entrevistas realizadas a profesionales que desarrollan sus actividades en la Dirección se dio origen al Departamento de Asistencia Tecnológica y Apoyo Investigativo (D.A.T.A.I.).

El trabajo se organiza en cuatro capítulos:

En el capítulo I presentamos el contexto en el cual han nacido las TIC y como se han desarrollado dando lugar a la aparición de la Sociedad de la Información, la cual se caracteriza por un incremento significativo en las comunicaciones que han crecido notablemente en los últimos 20 años.

En el capítulo II desarrollamos los conceptos de TIC, sus características, los medios de control social y el delito en la era digital. Para esto, recurrimos a presentar conceptualizaciones provenientes de la cibercriminología.

En el capítulo III presentamos la investigación policial en la era de la información, en la cual el cibercrimen ha generado nuevas formas de intervención legal y con ellas, también la creación de la prueba digital, en tanto método de comprobación y esclarecimiento de hechos delictivos.

En el capítulo IV presentamos el trabajo de campo, para lo que hemos seleccionado un caso particular de femicidio, que pudo ser resuelto gracias a los aportes de la prueba digital. Además, se incluyen las entrevistas y su posterior análisis. El trabajo finaliza con las conclusiones a las que hemos arribado y las propuestas que consideramos importantes para la temática estudiada.

Marco contextual

Capítulo I

Nuevas tecnologías de la información y comunicación.

Su desarrollo en el siglo XXI

El uso de las TIC (Tecnologías de la Información y la Comunicación) ha crecido en el presente siglo convirtiendo a internet en el medio más importante de comunicación para gran parte de los ciudadanos del mundo. El proceso generado por la sociedad de la información, nacida de la revolución tecnológica, ha contribuido a que esta forma de comunicación haya logrado un gran protagonismo.

La revolución tecnológica surgió como parte del proceso de transformaciones técnicas de desarrollo e innovación en las comunicaciones, trajo aparejado un cambio en la vida social y en las relaciones, marcando una época de progreso posterior a la tercera revolución industrial. En la era de las comunicaciones, la mayor herramienta tecnológica se refleja en las nuevas formas de almacenamiento de datos, constituidas por breves e invisibles espacios cibernéticos que movilizan, almacenan, cargan y re direccionan infinidad de archivos, documentos y datos con implicancia jurídica.

La sociedad de la información en la que nos encontramos inmersos, se caracteriza por la incorporación de las TIC en todos los ámbitos de la vida, produciendo grandes cambios que desarrollamos en adelante.

1.1Las nuevas tecnologías de la información y la comunicación

Las TIC, se han instalado en la sociedad mundial produciendo grandes modificaciones que contribuyeron, no solo con la mejora en las comunicaciones, sino también con nuevos aportes que benefician aspectos como la salud, la economía, la educación, cambios en la estructura social económica, laboral, jurídica y política, entre otros.

Como ha expresado Castell (1986)

> "Un nuevo espectro recorre el mundo: las nuevas tecnologías. A su conjunto ambivalente se concitan los temores y se alumbran las esperanzas de nuestras sociedades en crisis. Se debate su contenido específico y se desconocen en buena medida sus efectos precisos, pero apenas nadie pone en duda su importancia histórica y el cambio cualitativo que introducen en nuestro modo de producir, de gestionar, de consumir y de morir" (p.13).

Los avances tecnológicos, sociales y económicos que se han dado durante estos últimos años, ha llevado a denominar a la sociedad actual como "sociedad de la

información". Mattelart, (2002) refiere que "los orígenes de la sociedad de la información descansan sobre dos tipos de fenómenos interdependientes: el desarrollo económico a largo plazo y la evolución tecnológica" (p.12).

La globalización generó grandes cambios sociales, permitiendo una fuerte expansión de los países que traspasaron sus fronteras, y favorecieron el crecimiento de los mercados. La evolución tecnológica, contribuyó amplia y rápidamente, al desarrollo de un proceso económico diferente, sobre todo basado en las telecomunicaciones, las que han permitido incrementar notablemente la capacidad de tratamiento de la información, acelerando el crecimiento de otros sectores (Mattelart, 2002). Las tecnologías desarrollaron un papel decisivo en el cambio del dinamismo social, cultural y económico, siendo consideradas como una revolución de las comunicaciones y la información, ya que exceden el lenguaje oral, centrado en los hechos de la vida cotidiana del aquí y ahora. Pero, además, excede la escritura mediante signos y gráficos, como la imprenta, que fue hegemónica para transmitir los conocimientos durante siglos. Los medios de comunicación tradicionales del siglo XX como la televisión y la radio, han sido superados por la aparición de las TIC (Ontoria, 2006).

El funcionamiento de las nuevas tecnologías, se basa en el proceso de digitalización, y esto les ha permitido ingresar en el mundo de la economía, la educación, las relaciones sociales, el medio ambiente, la ciencia y la tecnología.

El desarrollo de las TIC ha conducido a una sociedad de la información, planteando un entorno diferente al que se vivía antes del siglo XX, momento histórico en el cual se han producido grandes cambios en el contexto social. Denominada sociedad de la información, caracterizada por un proceso de evolución profunda de la vida y las relaciones entre las personas, se destaca por un contexto en el cual las TIC, son protagonistas.

1.2 La sociedad de la información

El precursor de este concepto es Yoneji Masuda, quien en el año 1984 ya escribía sobre la sociedad de la información como sociedad post-industrial, la cual estaba sufriendo una silenciosa transformación centrada en la tecnología del ordenador, operando en conjunto con la tecnología de las comunicaciones. Sostenía que la tecnología de la información "se convierte en la fuerza latente de la transformación social, capaz de acarrear

una expansión en la calidad de información y un aumento a gran escala del almacenamiento de la información" (Masuda, 1984, p.26). Ya en el año 1984, el autor consideraba que el impacto que producirían las TIC, sería superior incluso, al generado por la revolución industrial, dado que el ordenador tiene como función, la de sustituir y amplificar el trabajo mental humano, mientras que la máquina a vapor buscó sustituir la amplificación del trabajo físico.

Al respecto Jeremy Rifkin, en su libro "El fin del trabajo", adhería a esta idea, mencionado que las TIC, no cumplirían la función de la Revolución Industrial, pues en ese momento de la historia, los grandes cambios puedieron sostener puestos de trabajo, e incluso ampliarlos. Sin embargo las nuevas tecnologías, si suplantan el trabajo humano, y "generan desempleo, y con esto el fin del trabajo como lo conocemos" (Rifkin, 1996 p.26).

Castells (1989) sostiene que los nuevos caracteres de este paradigma dieron lugar a la aparición de la era informacional, con internet como una herramienta fundamental para el nuevo modo organizacional de la sociedad, lo que impacta tanto en las relaciones personales como en las relaciones económicas y educativas. (Castells, 1989)

Por su parte, el sociólogo francés Alain Touraine (1996), en su libro "Sociedad posindustrial", señala la formación de nuevos tipos de sociedades: las sociedades de industrialización, que se han venido mezclando con las formas del capitalismo; las sociedades tecnócratas, designadas según el poder que las domina, y las sociedades programadas, apuntadas al modo de producción y de organización económica (Touraine, 1969).

En definitiva, los procesos de cambio registrados a lo largo del siglo XX han ido conformando un modelo social basado en la información, el conocimiento y la construcción de nuevas formas de comunicación que han transformado las formas de vivir, trabajar y divertirse, sin olvidar los peligros e inconvenientes que están asociados a estas nuevas formas de vida. La característica fundamental es que los cambios han sido mucho más vertiginosos que los ocurridos durante la Revolución Industrial, ya que la convergencia acelerada de las telecomunicaciones, la radiodifusión y la informática, han generado nuevos productos y servicios, así como nuevas formas de gestionar las organizaciones (Ortiz, 1995). Desarrollada de la mano de la globalización neoliberal, con la meta de instaurar un

mercado mundial abierto y autorregulado, el contexto en el cual creció la sociedad de la información, no siempre fue positivo, especialmente para los países débiles que no lograron incluirse en este mercado tan abierto como se suponía. En este sentido, las TIC se convirtieron en un factor clave para la aceleración de la globalización económica.

El rol que han adquirido las nuevas tecnologías en la sociedad actual, es el de facilitadoras de la sociedad de la información, dado que, gracias a las redes satelitales, la banda ancha o las redes de televisión y telefonía, la humanidad permanece conectada como nunca antes lo había estado, en consecuencia, esta sociedad presenta características que le son particulares.

1.2.1 Características de la sociedad de la información

Los rasgos que fueron configurando a la sociedad de la información son:

- *Exuberancia*: se distingue por la gran cantidad de información y datos que circulan actualmente en las TIC.
- *Omnipresencia*: el espacio preferido para la difusión de ideas e interacción social son las TIC, su universalidad implica mayor facilidad para la interacción social.
- *Irradiación*: la difusión de mensajes es prácticamente ilimitada gracias a que las distancias físicas se difuminan.
- *Velocidad*: la comunicación es inmediata e incluso simultánea con internet.
- Multilateralidad/Centralidad: existe la capacidad técnica de recibir información de todas partes, no obstante lo más probable es que la mayor parte de esta, surja de unos cuantos sitios.
- *Interactividad/Unilateralidad*: la comunicación contemporánea permite que sus usuarios sean productores de mensajes, sin embargo la mayoría de usuarios utiliza poco esa capacidad, son comunicadores pasivos.
- *Desigualdad*: existe un problema de falta de equidad social en la propagación e intercambio de información, en las naciones más industrializadas aumenta el acceso a la red, mientras los países más pobres son ajenos a internet.
- *Heterogeneidad*: en los medios de comunicación se multiplican las ideas, opiniones, comentarios y manifestaciones de toda índole.

- *Desorientación*: la sociedad de la información requiere de habilidades o técnicas para distinguir lo verídico de lo falaz, a partir de la gran cantidad de material que se comparte en internet (Alfonso Sánchez, 2016).

La transformación digital, protagonista de la sociedad de la información, ha afectado a todas las actividades de la sociedad humana, impactando en la banca, en las empresas y en la sociedad civil.

La posibilidad de conexión ha permitido el desarrollo de un nuevo espacio en el que se llevan a cabo millones de transacciones diarias que van, de un simple intercambio de la información, hasta la realización de actividades comerciales. Ileana Alfonso Sánchez, (2016) sostiene que a partir de la creación de internet, las comunicaciones fluyeron de manera constante, sobre todo en la transmisión de información ya que al contar con nuevas posibilidades de herramientas multimedias e hipertextuales, con acceso inmediato a volúmenes importantes de información, los receptores denominados usuarios, se fueron adaptando a las nuevas circunstancias técnicas y culturales. En la sociedad de la información, las *self media* (medios masivos), son personalizados y facilitan el establecimiento de relaciones desterritorializadas, multicrónicas, en red y en alguna medida interactivas.

En esta nueva sociedad, la información y el conocimiento se convirtieron en los elementos centrales, en los cuales se sustenta la economía y las relaciones sociales que estructuran la sociedad actual, mediante el uso de las TIC. Sin embargo, es indiscutible que ha contribuido a aumentar la brecha ya existente entre los países en desarrollo y los desarrollados (Castano, 2008). Las características de la sociedad de la información, han permitido ofrecer una serie de retos que conducen a los gobiernos a preocuparse por el diseño de estrategias públicas que les permitan a los miembros de la sociedad, disfrutar de los posibles beneficios de la nueva transformación.

El vertiginoso avance de las TIC en la sociedad, ha facilitado el acceso de las personas a la información, la comunicación y el aprendizaje, acercando los contenidos educativos, pero también facilitando la creación de nuevos empleos, aunque estos no han sido suficientes para captar toda la población, ya que quienes no cuentan con conocimientos, quedan excluidos. La búsqueda de mayor interacción humana, de

integración entre comunidades del mundo, o el crecimiento de las transacciones mercantiles, mediadas por la tecnología no siempre ha logrado mejorar la calidad de vida de las personas, dado que quienes no tienen igualdad de oportunidades de acceso a internet o dispositivos adecuados, quedan excluidos. Esto se puso en evidencia durante el período de pandemia de Covid-19, momento en el cual las brechas entre los que tienen acceso y los que no, quedaron evidenciadas.

En las relaciones personales, el aumento del uso de estas tecnologías, ha conformado un nuevo paradigma en el cual es difícil separar con claridad el "yo real" del "yo digital", especialmente en los denominados nativos digitales, es decir quienes han nacido en la era digital adquiriendo todos los conocimientos de tecnología desde pequeños. Esta transformación hacia el ciberespacio ha generado los cambios culturales y sociales que no han sido igual en todo el mundo, e incluso no es el mismo hacia el interior de cada país. En los países desarrollados la mayoría de la población tiene a las TIC absolutamente incorporadas en su vida cotidiana, y es una población considerada "informáticamente alfabeta", pero no es así en todas partes. Alva de la Selva (2015) sostiene que en todo el mundo la informatización ha aumentado la distancia entre quienes tienen acceso a las TIC y quienes no, siendo estos últimos, claramente excluidos (Alva de la Selva, 2015). En Argentina la situación se ha modificado en los últimos años, permitiendo el acceso a las tecnologías de la comunicación a partir de fomentar políticas inclusivas. En el siguiente apartado presentamos el contexto en el cual se encuentra en la actualidad, la situación de los habitantes del país en relación con el acceso a TIC.

1.3 Argentina y las TIC

Como hemos mencionado, el producto más importante de estos cambios en la sociedad, es que han surgido oportunidades únicas en el mundo para avanzar en el camino del desarrollo económico y social, en referencia a la integralidad de las comunidades. Estas oportunidades, basadas en las nuevas tecnologías, han permitido mejorar la industria y el comercio. Pero además han facilitado el acceso a la información, aunque no a todos los ciudadanos por igual, ya que esto depende de factores políticos y económicos que condicionan la posibilidad de contar, tanto con dispositivos como con internet, para la conexión.

En relación con la heterogeneidad de la población argentina, el informe de la CEPAL del año 2021, en su análisis de las capacidades de las TIC para crear empleo, mejorar la educación y brindar mayores accesos a la información en un marco de equidad, puso de manifiesto que en el país se observa una gran diversidad de patrones de incorporación tecnológica a nivel empresarial, educativo y social. El informe sostiene que existe poca disponibilidad de dispositivos como computadoras y teléfonos inteligentes, en los sectores más vulnerables, lo que evidencia que muchos no han podido acceder a contenidos educativos, sobre todo durante el tiempo de pandemia de Covid-19. Esto último, generará una gran desigualdad social en referencia a la capacitación educativa de la población y su consecuente ingreso al mercado laboral en el futuro (Novick, 2021).

Sin embargo es notable destacar que en referencia a la región de América Latina, Argentina se encuentra en primer lugar en materia de innovación tecnológica. La plataforma educativa Coursera, refiere que el país posee una población talentosa en referencia a los usuarios educativos, de negocios y de vinculación con el mercado, encontrándose a niveles cercanos a Suiza, Bélgica, Austria y Suecia, gracias a la creación de Polos Tecnológicos en varias ciudades, y la factibilidad de acceso a internet de la población, en comparación con otras regiones (INDES, 2019).

El INDEC, en su 4° Informe de Ciencia y Tecnología del año 2020, advierte que durante el año 2019 el 60,9% de los hogares urbanos, poseían computadora, y el 82,9% a internet; 84 personas, de cada 100, emplean teléfono celular, y 80 de cada 100, utilizan internet en su teléfono, de acuerdo a los últimos datos obtenidos en la Encuesta Permanente de Hogares realizada en el año 2019, anterior a la pandemia de Covid-19 (INDEC, 2020).

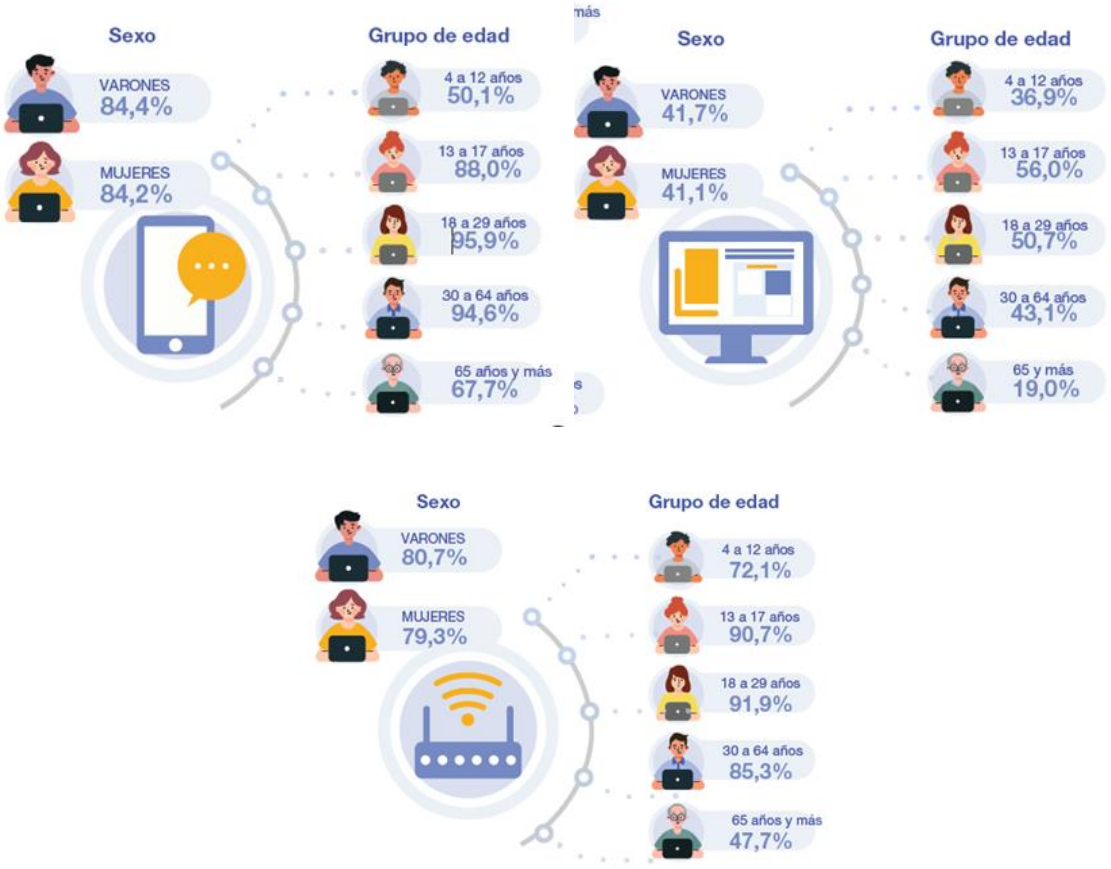
En comparación, el primer semestre del año 2021 refleja datos que presentan algunas variaciones: 63,8% de los hogares urbanos poseen computadoras; 90% de los hogares tienen acceso a internet, lo que significa que 88 de cada 100 personas, utilizan internet (INDEC, 201).

En referencia a la provincia de Mendoza, se registraron valores similares: el 61,3% de los hogares cuenta con computadora, el 85,6% posee internet y el 81% posee teléfono celular (INDEC, 2020).

Estos datos son tomados en hogares que tienen niños desde 4 años de edad, lo que significa que esos grupos tienen acceso a la tecnología desde edades tempranas.

Ilustración

Imagen 1. Dispositivos por grupo de edad en hogares argentinos primer semestre 2021



Fuente: INDEC (2021)

La ilustración N°1, demuestra la cantidad y disponibilidad de dispositivos electrónicos que poseen las familias argentinas, distribuidos por grupo de edad.

Con motivo de la pandemia de Covid-19, en el año 2020, a través del DNU N° 690/2020, el Poder Ejecutivo Nacional declaró los servicios regulados bajo la Ley Argentina Digital, como servicios públicos esenciales en competencia. A partir del mes de agosto de 2020, se modificó la norma a fin de permitir el acceso a toda la población, a internet. Esto significó un aumento en la contratación de este servicio, ya que el gobierno

nacional, creo nuevas formas de contratación con valores accesibles para personas de bajos recursos, mediante la Prestación Básica Universal y Obligatoria (PBU), para celulares, internet, televisión por cable y telefonía fija (PBU, 2021).

Los datos referentes al acceso a TIC en el sistema educativo, el cual ha demostrado la mayor brecha social en el país, ponen de manifiesto que el 76,9% de los hogares de niños que asisten a nivel primario, cuentan con computadoras, notebook o Tablet con las que pudieron acceder a clases virtuales (Hernández, 2021). Los datos más bajos se observaron en adolescentes que asistieron al nivel secundario donde el 60,5% contaba con un equipo informático y el 81,6% con acceso a internet, de alumnado de educación pública, mientras que quienes asisten a instituciones educativas privadas, las cifras son superiores dado que se corresponden con el 90,8% cuenta con equipamiento tecnológico y el 95,1% con acceso a internet (Hernández, 2021). Este puede ser el dato más importante respecto a la brecha de accesibilidad a tecnología, que demuestra la realidad del país.

1.4 Brecha digital y vulnerabilidad en el uso de las TIC

En el 2003 la Unión Internacional de Telecomunicaciones, organizó en Ginebra la Cumbre Mundial sobre la Sociedad de la Información. En ella se buscó reunir a diferentes países para lograr acordar algunos principios que contribuyeran a esta nueva sociedad, en la cual las TIC son las protagonistas. Allí se establecieron los principios que buscaron acabar con la brecha digital, y garantizar un desarrollo armonioso, justo y equitativo para todos.

Varios estudios han analizado el origen del término brecha digital (Gunkel, 2003; Castaño, 2008; van Dijk, 2017), quienes certeramente han señalado que existen en este tema, una brecha social, la cual se constituye en la diferencia en el acceso a la información entre los pobres y ricos en cada país; la brecha global, como la diferencia entre países desarrollados y en desarrollo en el uso de tic; y la brecha democrática, como la diferencia entre quienes utilizan las tic para movilizarse y participar en la esfera pública.

Alva de la Selva, (2015) ha sostenido que el uso de las TIC, en definitiva se refiere a la capacidad que tienen ciertos grupos sociales, de acceder a las mismas, y en este sentido estos usuarios dependen de sus propias habilidades, las que son necesarias para el uso de estas tecnologías. Esto lleva a definir a la brecha digital como aquella existente “entre

individuos, hogares, negocios y áreas geográficas en diferentes niveles socioeconómicos con respecto a sus oportunidades de acceso a las TICs y su uso para una amplia variedad de actividades" (Alva de la Selva, 2015, 267).

La inequidad en el acceso ha generado una nueva forma de exclusión social, de manera que ciertos sectores de la población quedan marginados de las ventajas que genera el uso de las TIC, tales como las oportunidades de empleo, la interacción y la integración social. Además, el término se relaciona con la desigualdad en capacidades y habilidades de los individuos para participar y desarrollarse en las "sociedades de la información y el conocimiento" (Castaño, 2008, p.28).

Una de las definiciones más importantes para comprender esta brecha digital es la de alfabetización digital, el cual es "un proceso de aprendizaje que permite a una persona adquirir competencias para entender y aprovechar el potencial educativo, económico y social de las nuevas tecnologías" (Fernández, 2019 p.33). Su objetivo es el de enseñar y evaluar los conceptos y habilidades básicos de la informática para que las personas puedan utilizar la tecnología informática en la vida cotidiana y desarrollar nuevas oportunidades sociales y económicas para ellos, sus familias y sus comunidades.

El acceso digital es cada vez más importante en tanto un diferenciador competitivo de capacidades para la inserción social, particularmente la inserción laboral. Dentro de esta brecha existen otras como la *brecha digital de género*, la *brecha de acceso* que se encuentra vinculada a la de disponibilidad de dispositivos, la *brecha de uso*, la cual hace referencia a las competencias digitales que las personas presentan, y la *brecha de calidad de uso,* la cual se refiere a los conocimientos disponibles para hacer un buen uso de la red y sacarle el mayor partido posible (Galperín, 2017).

La brecha digital implica también, la discriminación tecnológica, la cual constituye una forma de pobreza y exclusión social, al privar a una parte de la ciudadanía de recursos esenciales para desarrollarse y generar riqueza. Durante el período de pandemia de Covid-19, esto quedó en evidencia, dadas las grandes dificultades que, sobre todo que los estudiantes, debieron enfrentar. La desigualdad, medida en relación a la disponibilidad de dispositivos, o el acceso a internet, no siempre refleja la realidad, puesto que una persona

puede poseer uno o más dispositivos en su haber. Si bien los datos obtenidos del INDEC (2020) permiten inferir que la disponibilidad de dispositivos en la sociedad es alta, al igual que el acceso a internet, los estudios sólo analizan zonas urbanas, dejando fuera a muchas regiones que no cuenta ni siquiera, con acceso a electricidad.

La importancia de poseer acceso a las TIC se refleja no solo en la educación, sino también en el trabajo y en la ocupación del tiempo libre, el cual puede desarrollarse en interacción con otras personas. Las redes sociales cumplen un importante rol en la sociedad actual, para esta interacción.

1.5 Uso de redes sociales en Argentina y Mendoza

Las redes sociales, en el mundo de la virtualidad, son sitios y aplicaciones que operan en diferentes niveles, permitiendo el intercambio de información entre personas y/o empresas. Estas comunidades formadas por diferentes usuarios, organizaciones, empresas, entre otras, son plataformas que se relacionan entre sí, mediante la utilización de internet. En ellas se puede interactuar en forma individual, grupal y hasta comunitaria, dado que las posibilidades de relacionarse son amplias y variadas.

Cada red social tiene sus propios objetivos y usos particulares, y en relación a esto, son los contenidos que se publican y las formas de interacción que se desarrolla. Facebook, la más antigua de todas, es una red social que surgió para contactar amigos, conocer gente con los mismos intereses, e intercambiar conversaciones, conocimientos, eventos, hasta llegar a contenido de imágenes y videos (Wasserman, 2013). En la actualidad continúa realizando este funcionamiento, al igual que Instagram. Twitter, es una red que nació con la finalidad de competir en el mercado con Facebook, sin embargo hoy es un espacio de interacción diferente en el que la política ha encontrado un lugar para expresar sus ideas, e interactuar con ciudadanos.

Una de las utilidades más importantes de las redes sociales, es la interacción económica manejada por grandes mercados internacionales que invierten en ellas en publicidad y promoción de productos. Esto también es utilizado por pymes o emprendedores individuales, ya que en ellas pueden compartir las ofertas de sus bienes y/o servicios. Facebook, la red más popular, posee un espacio denominado Marketplace en el

cual se realiza una interacción comercial en la que todos pueden participar, independientemente si se trata de una mega empresa comercial o si se trata de usuarios que simplemente, buscan intercambiar o vender mercadería, nueva o usada, como también ofrecer sus servicios. Esta red, brinda a usuarios que realizan ventas permanentes, una herramienta de estadísticas en las que se observan las interacciones más importantes que tienen sus productos, así como también la cantidad de personas que han realizado vistas, cuantas personas pusieron Me Gusta, los usuarios que hicieron clic en ocultar, reportar como spam o ya no me gusta, de cada publicación (Facebook, s.f.). Esto le permite al vendedor, identificar el público objetivo al que puede dirigir sus productos, además de marcar tendencias en las ofertas. De esta forma, la red social se ha convertido en un espacio para operaciones de mercado más. También en ellas hay lugares para la recreación y el esparcimiento ya que cuentan con aplicaciones asociadas de juegos.

Instagram y Twitter, no cuentan con espacios de venta gratuita, sin embargo los usuarios pueden crear sus propias publicaciones que dependerán de las interacciones que cada red tenga entre sus usuarios. En este sentido, se destaca que Instagram por ejemplo, es la red social en la que los famosos publican artículos de marcas que los contratan en los espacios de historias, o bien en sus publicaciones. En la red social Twitter sólo realizan publicaciones los usuarios para que estas sean vistas por sus seguidores, quienes pueden compartirlas o no, lo que limita la llegada a mayor cantidad de público.

Las ventajas de las redes sociales radican en que incluyen la rápida comunicación, un espacio de oportunidad laboral y/o comercial, ocio y recreación, pero también sirven para compartir información, vender productos y promocionarlos. En función de estas ventajas, del mismo modo existen los problemas a los que los usuarios muchas veces deben enfrentarse como las estafas en redes sociales, los robos, la violación de privacidad, el robo de datos e imágenes, los escraches y la difamación, y un grave problema de salud pública como es el de la adicción a las redes sociales (Wasserman, 2013).

En Argentina la población asciende aproximadamente a 45 millones de personas, de las cuales el 92,2% habita en zonas urbanizadas (Kemp, 2021), los que tienen mayores posibilidades de acceder a servicios de internet. Los datos estadísticos que brinda el INDEC, en sus informes del año 2020 y 2021, han mostrado un crecimiento en el acceso a

dispositivos como computadoras, tablets y smartphones, y también a internet. El Digital 2021 Global Overview Report, realizó un estudio en el país, durante el período de confinamiento, entendiendo que Argentina fue uno de los más estrictos, demostrando que en el país existen 55,19 millones de celulares, lo que representa un número mayor a la población total del país.

Por su parte el INDEC, sostiene que el 80% de la población accede a internet y de estos, el 79,3% usa redes sociales activamente como Facebook, Instagram, TikTok, YouTube, lo que permite inferir que todos los usuarios de internet tendrían perfiles en estas plataformas (Kemp, 2021).

En la siguiente imagen se muestran los indicadores de crecimiento digital correspondientes al mes de enero de 2021

Imagen 2 Crecimiento digital en Argentina

Fuente: https://datareportal.com/reports/digital-2021-global-overview-report (Consultado el 15 de febrero de 2022)

En referencia a los dispositivos que más utilizan los usuarios de internet, se observa que la telefonía móvil es la más frecuente, los Smartphone (teléfonos inteligentes) siguen en la lista, luego continúan las laptops, Tablets, TV inteligente que permite ver contenido en línea, consola de videojuegos, entre otros.

Imagen 3 Posesión de Dispositivos

Fuente: https://datareportal.com/reports/digital-2021-global-overview-report (Consultado el 15 de febrero de 2022)

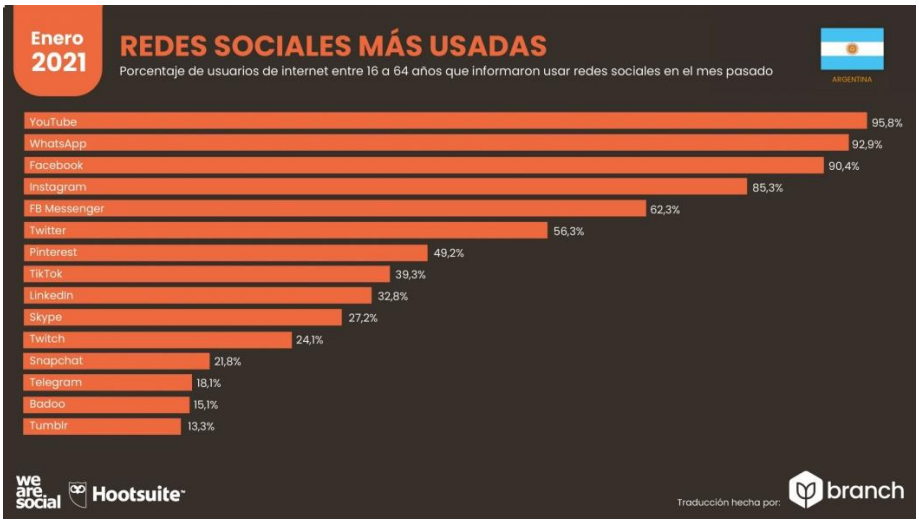
El tiempo invertido en forma diaria en las plataformas y dispositivos se describe en la imagen N°3. Al día, los argentinos le dedican 9 h y 39 minutos de tiempo conectados a internet; 3 h mirando TV (*broadcast* o *streaming*); 3 h y 22 min usando redes sociales; 1 h y 32 min leyendo noticias; 1 h y 54 min escuchando música a través de servicios de streaming, 1 h y 15 min escuchando radio y 1h y 6 min al día jugando videojuegos de consola (Kemp, 2021), en promedio.

Imagen 4. Tiempo diario invertido en plataformas y dispositivos

Fuente: https://datareportal.com/reports/digital-2021-global-overview-report (Consultado el 15 de febrero de 2022)

Las redes sociales y apps de mensajería instantánea más usadas fueron YouTube, WhatsApp, Facebook, Instagram; Messenger; Twitter; Pinterest; TikTok, Linkedin, tal como se observa en la imagen siguiente.

Imagen 5. Redes sociales más usadas



Fuente: https://datareportal.com/reports/digital-2021-global-overview-report (Consultado el 15 de febrero de 2022)

Una de las características más importantes es que el flujo de tráfico web se origina a través de dispositivos que poseen el sistema operativo Android, el cual es el más usado por los argentinos con un porcentaje de 91.9%, seguido, con una alta diferencia, por iOS con el 7.8%.

En este contexto, la provincia de Mendoza, se sitúa entre las más avanzadas en cuanto a generación de TIC, dado que cuenta no solo con una amplia variedad de acceso a ellas, sino que además, en el territorio se encuentra el Polo Tecnológico, el cual ha representado un gran avance en materia de tecnología, para la provincia.

1.6 Parque Tecnológico. Polo TIC

El Polo TIC, parque tecnológico de la provincia de Mendoza, fue creado en el año 1997, por un pequeño grupo de empresas TIC de Mendoza, quienes iniciaron este camino a partir de constituir en ese año, la Cámara de Empresas de base Tecnológica. En el año 2002 incluyeron sectores productivos, académicos y representantes del Estado provincial con la finalidad de consolidar la idea del Polo TIC. Esta articulación fue la que dio origen al

conjunto de acciones que se fueron consolidando en los últimos 20 años para la construcción de un edificio en un terreno municipal, ubicado en la calle Cubillos 2056 del departamento de Godoy Cruz, donde se instaló el Parque Científico y Tecnológico especializado en TIC, inaugurado en el año 2017.

Se trata de un modelo único en la República Argentina, constituido como una organización mixta en la que intervienen universidades, empresas vinculadas a las TIC y el sector público, con la misión de insertar a Mendoza en el nuevo paradigma de la revolución digital (TIC, 2021). Este parque cuenta con un plan de estratégico basado en el desarrollo de recursos humanos calificados en TIC que busca impulsar la promoción de I+D[1], a fin de alcanzar los estándares de calidad y competitividad internacionales.

Las investigaciones que se desarrollan en esta institución, le han permitido a Mendoza la construcción de drones creados exclusivamente en el Polo TIC, que son destinados a la sanitización ambiental, utilizados especialmente durante el año 2020, y que en la actualidad funcionan en el departamento de Godoy Cruz, desinfectando diferentes sectores.

Cuenta con inversiones de 18 empresas: Inamika Interactive, Omnitronic, Globalis, Col SA, Tiempo Soft, Case, Kerberos, Grupo Oeste, Arlink, ITC Soluciones, Softnuvo, Vial Siep, TMS Group, Big media, Foca, Silice, Sequre, R link, y Universidad del Aconcagua, UNCuyo, Fundación UNCuyo y UTN, además de aportes estatales. La estructura edilicia es de última generación, al igual que el material tecnológico destinado a la investigación y producción de recursos TIC.

Dado el gran crecimiento que las Tecnologías de la Información y la Comunicación han desarrollado en los últimos 50 años, se ha requerido la construcción de un conjunto de normas legales que regulen su funcionamiento, desde las telecomunicaciones, hasta la regulación de la circulación de datos. En el siguiente apartado presentamos el contexto legal en el cual se inscriben las TIC, y las normas que regulan el tráfico de datos, y la privacidad de los usuarios.

[1] Investigación y Desarrollo

1.7 Contexto legal en el uso de las TIC

Dado el gran crecimiento en la utilización de estas tecnologías, los Estados debieron responder creando normativas legales que las regulen, a fin de proteger tanto a usuarios, como a las empresas que ofertan servicios. A continuación se presenta las normas legales que regulan la utilización de TIC en Argentina.

1.7.1 Convenio de Budapest

El Convenio de Budapest es el primer instrumento internacional que trata de manera específica aspectos relacionados con el ciberdelito. El mismo fue sancionado en noviembre de 2001 por el Consejo de Europa y entró en vigencia en 2004. En 2017, mediante la sanción de la Ley Nro. 27.411, la Argentina lo incorporó como parte de su legislación. El Convenio, además, ya contaba con un Protocolo del año 2003 sobre delitos racistas a través de sistemas informáticos. Natalia Sergi (2018) sostiene que

> "En el año 2008 el Poder Ejecutivo Nacional conformó a una comisión integrada por representantes del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto, del Ministerio de Justicia, Seguridad y Derechos Humanos, de la Oficina Nacional de Tecnologías de Información dependiente de la Subsecretaría de Tecnologías de Gestión de la Secretaría de Gestión Pública de la Jefatura de Gabinete de Ministros, del Ministerio Público Fiscal de la Nación, expertos del sector académico y de las empresas privadas a fin de analizarla y determinar si sus principios y normativa se adecúan a los principios constitucionales de nuestro sistema penal" (p.58).

Esta Comisión, destacó la importancia de la incorporación de este Tratado en la normativa legal, como herramienta de cooperación en materia de delitos informáticos a nivel internacional. El Convenio permite que se investiguen no sólo los delitos informáticos, sino que además se investigue en cooperación internacional, ubicando a Argentina en un sistema de cooperación especializado junto a los países más importantes a nivel mundial y con los que el país tiene una tradición de vínculos cooperativos.

Es el primer Tratado Internacional creado con el objetivo de proteger a la sociedad frente a los delitos informáticos y los delitos en internet, mediante la elaboración de leyes adecuadas, la mejora de las técnicas de investigación y el aumento de la cooperación internacional. En el año 2019 este Convenio ha sido ratificado por 62 países en todo el mundo. Es el único acuerdo internacional sobre este tipo de delitos, que hace hincapié en

las infracciones de: derechos de autor, fraude informático, la pornografía infantil, los delitos de odio y violaciones de seguridad de red. La prevención de estos delitos es de vital importancia a nivel internacional ya que los mismos pueden poner en peligro “la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos” (Sergi, 2018, p. 60). (Temperini, 2018)

El Convenio de Budapest tuvo en cuenta los convenios existentes complementándose para incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos, así como para permitir la obtención de pruebas electrónicas, siendo el instrumento internacional vigente, más importante de la actualidad, para abordar el cibercrimen (Consejo de Europa, 2001).

1.7.2 Ley 19.798/72. Telecomunicaciones. Normativa aplicable

La norma del año 1972 define a la telecomunicación como “Toda transmisión, emisión, o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos"

Crea el Consejo Nacional de Telecomunicaciones (CONATEL), cuyas competencias incluyen la proyección de leyes referentes a telecomunicaciones, promover el desarrollo de industria de telecomunicaciones, participar en el fomento de la investigación y asistencia técnica para el progreso y perfeccionamiento de las telecomunicaciones, entre otros.

Uno de los problemas que presenta la norma se encuentra en su artículo 45, en el cual se pondrían en riesgo los datos personales. Esto ha sido subsanado por la ley 25.326 de Protección de datos Personales. En referencia a la norma, la doctrina ha establecido que justamente estos datos filiatorios son datos personales, sin embargo no son sensibles, por lo que pueden estar incluidos en bases de datos públicas como privadas (INFOLEG, 1972).

1.7.3 Ley 25.326/2000 de Protección de datos personales

El objeto de esta ley es la de protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al

honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional (INFOLEG, 2000).

1.7.4 Ley 25.891/2004. Servicios de comunicaciones móviles

Esta ley establece que, la comercialización de los servicios móviles, podrá realizarse únicamente a través de las empresas legalmente autorizadas para tal fin, por lo tanto prohíbe la reventa de líneas de comunicación. El órgano de contralor es el Registro Público Nacional de Usuarios y Clientes de Servicios de Comunicaciones Móviles.

Establece que las ventas de equipo o terminales móviles deberán registrar y sistematizar los datos personales, filiatorios, domiciliarios que permitan una clara identificación de los adquirientes. En caso que los adquirentes sean personas distintas del usuario, o personas jurídicas, u organismos del Estado, se deberá indicar la identificación del usuario final.

En el Art. 3° la ley expresa la obligación de las empresas de informar las terminales que se denuncian como robadas, hurtadas o extraviadas en forma diaria, y a negarse a otorgar servicios a quienes lo soliciten mediante la utilización de terminales incluidas en las bases de datos que hayan sido reportadas. Los licenciatarios pondrán a disposición de las fuerzas de seguridad nacionales y provinciales, un asterisco de llamada gratuita, a toda hora y todos los días del año, a fin de corroborar si un determinado equipo terminal se encuentra registrado en la base de datos a que alude el presente.

Por otro lado, obliga a los clientes a informar de inmediato si su terminal ha sido robada o extraviada, como también prohíbe la reactivación de los equipos reportados.

La ley crea el Registro Público Nacional de Usuarios y Clientes de Servicios de Comunicaciones Móviles, en el que se encuentran todos los datos filiatorios de los titulares.

Las sanciones por alteración, reemplazo, duplicación o modificación en los números de línea o cualquier modificación de identificación en las terminales, incluyen desde 1 mes a 6 años de prisión. Igual sanción corresponde para quienes alteren o roben tarjeta de

telefonía o “accediere por cualquier medio, a los códigos informáticos de habilitación de créditos de dicho servicio” (Art. 11). (INFOLEG, 2004)

1.7.5 Ley 25.992/2004 Ley de promoción de la industria del software

Esta ley consiste en promover la creación de empresas que tengan, como actividad principal la creación de software a través de importantes beneficios impositivos. Esta normativa se ha visto actualizada por el importante proceso evolutivo que atraviesa la industria del software, dando acogida a aspectos novedosos dentro del abanico de prestaciones promovidas tales como la incorporación de actividades de desarrollo de productos y servicios de software, aplicados a actividades tales como “e-learning”, marketing interactivo, “e-commerce”, Servicio de Provisión de Aplicaciones (ASP), edición y publicación electrónica de información, y otros, siempre que se encuentren formando parte integrante de una oferta informática integrada y agreguen valor a la misma. (INFOLEG, 2011)

1.7.6 Ley 26.522/2009 Servicios de comunicación audiovisual

Esta norma regula los servicios de comunicación audiovisual en todo el ámbito del territorio nacional, siguiendo los parámetros de la Comisión Europea publicados el 13 de diciembre de 2005, para la Televisión sin Fronteras, la cual se constituye en una evolución de la directiva actual a una directiva de servicios de medios audiovisuales, independiente de la tecnología implementada.

En el mismo sentido, dicen los fundamentos de la Directiva, en su considerando Nº 27:

> “El principio del país de origen debe seguir siendo el núcleo de la presente Directiva, teniendo en cuenta que resulta esencial para la creación de un mercado interior. Por lo tanto, debe aplicarse a todos los servicios de comunicación audiovisual a fin de brindar seguridad jurídica a los prestadores de tales servicios, seguridad que constituye un fundamento necesario para la implantación de nuevos modelos de negocio y el despliegue de dichos servicios. También es esencial el principio del país de origen para garantizar la libre circulación de la información y de los programas audiovisuales en el mercado interior”.

Prevé la implementación de comunicación adecuada a la diversidad e identidad cultural, la diversidad lingüística y el contenido local. Regula la creación de políticas y

legislaciones nacionales para garantizar el acceso a contenidos audiovisuales en todos los ámbitos educativos, de salud, economía y finanzas, agricultura, entre otros, a la información. (INFOLEG, 2009)

1.7.7 Ley 26.388/2008. Modificación al Código Penal

Esta ley introduce los delitos informáticos en el Código Penal, sancionando los delitos contra la integridad sexual, especialmente la pornografía infantil. Agrega además, la violación de secretos y la privacidad, los que incluye el acceso a sistemas informáticos y a bancos de datos. Sanciona además el fraude informático, el daño informático y los delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

En su artículo 1° incorpora al artículo 77 del Código Penal, a los siguientes párrafos:

- El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
- Los términos "firma" y "suscripción", comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
- Los términos "instrumento privado" y "certificado" que comprenden el documento digital firmado digitalmente.

El artículo 2° sustituye el art. 128 del Código Penal por el siguiente:

> Artículo 128: Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
>
> Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.
>
> Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años.

Art. 3° sustituye el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, estableciendo el denominado “Violación de Secretos y de la Privacidad”.

En el artículo 4°, se sustituye el Art. 153 del Código Penal estableciendo que será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica, carta, pliego cerrado, despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido o se apodere indebidamente de alguna de ellas. En esta pena se incluyen a quienes intercepten o capten comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. Si el autor, además, publica los contenidos, la pena será de 1 mes a 1 año.

La ley también sanciona a quienes accedan por cualquier medio, y sin autorización o excediendo la que posee, a un sistema o dato informático de acceso restringido. Incorpora como delitos al uso ilegítimo de contraseñas sin autorización del propietario; si se produce alguna infracción al copyright de bases de datos sin autorización; interceptación de e-mail; pesca de claves secretas; estafas electrónicas; juegos de azar y transferencia de fondos no autorizados. Incluye los delitos en los que medie el uso de internet, de espionaje, espionaje industrial, terrorismo, narcotráfico y fraude. (INFOLEG, 2008)

1.7.8 Ley 27.078/2014. Tecnologías de la Información y las Comunicaciones. Argentina Digital

El objeto de esta norma es de declarar de interés público el desarrollo de las TIC, las Telecomunicaciones y sus recursos asociados, estableciendo y garantizando la completa neutralidad de las redes.

Esta norma busca garantizar el acceso a la totalidad de los habitantes de la República Argentina, a los servicios de la información y las comunicaciones en condiciones sociales y geográficas equitativas, con los más altos parámetros de calidad. Asimismo, su finalidad es la de garantizar el derecho humano a las comunicaciones, reconociendo a las TIC como un factor preponderante en la independencia tecnológica y productiva y productiva de la Nación. Busca promover el rol estatal en tanto planificador de

políticas públicas, incentivando la función social de las tecnologías, la competencia y la generación de empleo.

Establece las definiciones vinculadas a la comunicación definiendo a las TIC como "el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permitan la compilación, procesamiento, almacenamiento y transmisión de información, como por ejemplo voz, datos, texto, video e imágenes, entre otros" (Art. 6, inc. i).

Incluye el concepto de acceso como aquel que se encuentra "a disposición de parte de un prestador a otro de elementos de red, recursos asociados o servicios con fines de prestación de Servicios de TIC, incluso cuando se utilicen para el suministro de servicios de contenidos audiovisuales" (Art. 7, inc. a), entre otros, incorporando las características que adquieren las redes de telecomunicaciones y la interconexión. (INFOLEG, 2014)

1.7.9 Ley 27.411/2017 Convenio sobre Ciberdelito. Aprobación

Esta norma, en su Art. 1° aprueba el Convenio sobre Ciberdelito del Consejo de Europa, conocido como Convenio de Budapest, el cual consta de 48 artículos. Las reservas de la ley son las siguientes:

- El art. 6.1.b. manifiesta que no regirá en su jurisdicción ya que en el mismo se observa un supuesto de anticipación de la pena mediante la tipificación de actos preparatorios, lo que va en contra de la legislación jurídico penal argentina.
- Art. 9.1.d; 9.2 y 9.2.c no regirán en la jurisdicción argentina por entender que son supuestos incompatibles con el Código Penal vigente.
- Reserva parcial al art. 9.1.e. no regirá en la jurisdicción por entender que el mismo es solo aplicable cuando la posesión, allí referida, fuera cometida con "inequívocos fines de distribución o comercialización", lo que se encuentra definido en el art. 128, párr. 2° del Código Penal vigente.
- Reserva del art. 22.1.d. el cual no regirá en la jurisdicción dado que su contenido difiere de las reglas que rigen la definición de la competencia penal nacional.

- Reserva del art. 19.4 el que no regirá en la jurisdicción por entender que el requisito de la doble incriminación es una de las bases fundamentales de la Ley de Cooperación Internacional en materia penal 24.767 para el tipo de medidas de cooperación previstas en artículo y numeral citados. (INFOLEG, 2017)

1.7.10 Decreto 267/2015 Ente Nacional de Comunicaciones (ENACOM). Creación. Ley N° 26.522 y N° 27.078. Modificaciones

Mediante este Decreto se crea el Ente Nacional de Comunicaciones (ENACOM) en tanto ente autárquico y descentralizado, en el ámbito del Ministerio de Comunicaciones, y como autoridad de aplicación de las Leyes N° 26.522 y 27.078 y sus normas modificatorias y reglamentarias.

El artículo 10 sustituye el art. 10 de la Ley 27.078 estableciendo que se incorpora como servicio que podrán registrar los licenciatarios de TIC, al servicio de Radiodifusión por suscripción, mediante vínculo físico y/o mediante vínculo radioeléctrico. El servicio de Radiodifusión por suscripción se regirá por los requisitos que establecen los artículos siguientes de la presente ley y los demás que establezca la reglamentación, no resultándole aplicables las disposiciones de la Ley N° 26.522. Se encuentra excluida de los servicios de TIC la televisión por suscripción satelital que se continuara rigiendo por la Ley N° 26.522. (INFOLEG, 2015)

1.7.11 Decreto 798/2016 Plan nacional para el desarrollo de condiciones de competitividad y calidad de los servicios de comunicaciones móviles. Aprobación

Este Plan tiene como eje estratégico, el de favorecer una mayor eficiencia en el mercado con servicios de calidad y a precios justos y razonables. Este plan comprende los Servicios de Telefonía Móvil, de Radiocomunicaciones Móvil Celular, de Comunicaciones Personal y de Comunicaciones Móviles Avanzadas y su evolución tecnológica. (INFOLEG, 2016)

1.7.12 Decreto 1.340/2016. Ministerio de Comunicaciones. Normas básicas. Implementación

Implementa las normas básicas para alcanzar un mayor grado de convergencia de redes y servicios en condiciones de competencia, promover el despliegue de redes de próxima generación y la penetración del acceso a internet de banda ancha en todo el territorio nacional, de conformidad a lo dispuesto por las leyes N°. 26.522 y 27.078.

Este Decreto define:

Banda Ancha: como los servicios de acceso con velocidades del orden de megabits por segundo (Mbps).

Red NGN: red basada en paquetes que permite prestar servicios de telecomunicaciones y en la que se pueden utilizar múltiples tecnológicas de transporte de banda ancha propiciadas por la calidad de servicio, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionados con el transporte.

LTE: acceso de datos inalámbricos de banda ancha de alta eficiencia espectral que utilizando OFDM (acceso múltiple por división de frecuencias ortogonales) permite gran cantidad de usuarios simultáneos a altas velocidades por canal de radio. Arquitectura totalmente basada en conmutación de paquetes, con baja latencia, gestión y control de los recursos radioeléctricos para mejorar la calidad del servicio de banda ancha que cumple los requisitos de la UIT para IMT Advanced, también referido como 4G.

Red de Última Milla: la red que conecta a los usuarios con las redes de los prestadores de servicios de telecomunicaciones, también conocida como red de acceso local. (INFOLEG, 2016)

1.7.13 Resolución 98/2010. Régimen de portabilidad numérica. Aprobación

Esta Resolución le permite al usuario titular de servicios portables, mantener su número cuando cambie de prestador de servicios portables, de conformidad con las disposiciones del Plan Fundamental de Numeración Nacional.

Así mismo, incluye definiciones de dispositivo terminal; prestador; reclamo; roaming; Servicio de Comunicaciones Móviles; Servicio Prepago; SMS (servicios de mensajerías simples); Servicio de Acceso a Internet; Servicios de Tecnologías de la Información y las Comunicaciones, entre otras. (INFOLEG, 2010)

1.7.14 Resolución 733/E/2017 del Ministerio de Modernización

Esta resolución se basa en el Art. 42 de la Constitución Nacional, donde se establecen los derechos de los consumidores, protegiendo sus intereses económicos y el de acceso a una información adecuada y veraz. En este sentido, reglamenta los Servicios de TIC en consideración al abono, la adquisición de contenidos y aplicaciones de información y entrenamiento, las licencias y, sobre todo, regula la baja de la relación contractual, siendo este punto uno de los más importantes puesto que viene a restituir un derecho de los consumidores, como el de renunciar a la prestación de un servicio. Además establece la confidencialidad de las claves creadas por los usuarios, así como también cualquier dato vinculado con sus datos personales. (INFOLEG, 2017)

1.7.15 Resolución 1.291/2019 Ministerio de Justicia y Derechos Humanos. Unidad 24/7 de Delitos Informáticos y Evidencia Digital

En relación a la adhesión de la República Argentina a la Ley N° 27.411/17 al Convenio sobre Ciberdelito del Consejo de Europa, conocido como Convenio de Budapest, el país buscó mejorar el sistema penal tanto en la persecución de los delitos informáticos, como también en la investigación de cualquier delito para el que se requiera de obtención de pruebas en formato digital. Este gran avance legislativo nacional, fortalece la cooperación internacional en materia penal, ubicando a Argentina en un sistema de cooperación especializado, junto a los países más importantes con los que tenemos vínculos de cooperación.

De acuerdo a esta Resolución, Argentina se compromete a designar un punto de contacto localizable las 24 horas del día, los 7 días de la semana, el cual es denominado Red 24/7, con la finalidad de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recolección de pruebas electrónicas de una infracción penal. De esta forma se crea la Unidad 24/7 de Delitos Informáticos y Evidencia Digital, que asume las funciones previstas

en el artículo 35 del Convenio sobre Ciberdelito del Consejo de Europa. (Boletín Oficial, 2019)

1.7.16 Ley 8.916/2016. Creación del Registro Provincial de Huellas Genéticas Digitalizadas.

Esta ley provincial, autoriza a la provincia de Mendoza a contar con un Registro Provincial de Huellas Genéticas Digitalizadas a fin de contar con conocimientos sobre personas que han cometido delitos.

A los fines de la ley, el art. 2 realiza las siguientes definiciones:

a) Huella Genética Digitalizada: Se entenderá por huella genética digitalizada el registro alfanumérico personal elaborado exclusivamente sobre la base de la información que comprenda un mínimo de veinte (20) marcadores STRs autosómicos según el set extendido del CODIS (Expanded CODIS core) del FBI; marcadores de cromosoma Y (haplotipo mínimo de 11 marcadores según la Y-STR Haplotype Referente Database: YHRD); marcadores STRs del cromosoma X; ADN mitocondrial (HVRI y HVRII) validados a nivel internacional, que carezca de asociación directa con ADN de genes codificantes, que aporte sólo información identificatoria y que resulte apto para ser sistematizado y codificado en una base de datos informatizada, sin perjuicio de la utilización más amplia de la muestra biológica que pudiera disponerse en el marco de una investigación judicial, previa autorización fundada de la autoridad jurisdiccional interviniente y dentro de los límites establecidos por la legislación vigente.

b) ADN: Acido Desoxirribonucleico.

c) Marcadores Polimórficos: secuencias de ADN que presentan variación de un individuo a otro dentro de la población.

d) Impacto Identificatorio Positivo: es la coincidencia entre un patrón genético ingresado con otro/s previamente ingresados en el Registro Provincial de Huellas Genéticas Digitalizadas.

e) Huellas genéticas de persona imputada, procesada o condenada en un proceso penal y/o huellas que se encontraren asociadas a la identificación de las mismas, así como de menores cuya responsabilidad penal haya sido declarada y de personas a quienes no se condenó por mediar una causa de inimputabilidad.

f) Huellas genéticas del personal perteneciente a la Policía de la Provincia de Mendoza, Servicio Penitenciario de Mendoza, Policía Judicial, funcionarios y/o personal del Poder Judicial y/o del Ministerio Público que intervengan en la

> investigación penal, incluyendo contratados, y demás fuerzas de seguridad que operen en el territorio provincial.
>
> h) Huellas genéticas de directivos, propietarios, socios, asociados, personal e individuos cuya actividad principal o secundaria fuere el servicio de seguridad privada en el territorio provincial". (SAIJ, 2016)

En función de la normativa vigente, se han incluido un conjunto de nuevas terminologías en el Derecho Penal, las que presentan actualmente, una diversidad de conceptualizaciones. En el siguiente capítulo, presentamos los conceptos más relevantes que permiten comprender el impacto que las TIC han generado en el ámbito penal y policial.

Marco Conceptual

Capítulo II

Alcance de las nuevas tecnologías de la información y la comunicación en la Seguridad Pública

La digitalización mundial, también ha contribuido para crear espacios adecuados para la conformación de nuevas formas delictivas y que reciben el nombre de ciberdelitos, como también delitos informáticos. A fin de poder identificarlos y conocerlos, en el presente capítulo, explicaremos que son las TIC y sus características, lo que nos permitirá demostrar que estos nuevos espacios permitieron la aparición de nuevos delitos en los cuales ya no serán las armas de fuego las herramientas más utilizadas, sino que la estrategia se dirige hacia otras formas de interacción que requieren de un poco más de conocimientos, sobre todo en informática y programación, pero además, requieren de la elaboración de nuevas estrategias de captación de víctimas.

2.1 ¿Qué son las TIC?

La conceptualización de las TIC ha evolucionado, desde las proposiciones realizadas por Castells en 1986, quien las entiende como "una serie de descubrimientos científicos y desarrollos tecnológicos que afectan a los procesos de producción y gestión, en mayor medida que la afectación que se produce en los productos" (p 32), pasando por otras definiciones como las de Cabero (2001) o Majó y Marqués (2002), quienes comprenden que las TIC se desarrollan en torno a la informática, la microelectrónica, los multimedia y las telecomunicaciones. Mientras que autores más contemporáneos como Cacheiro (2014) y Roblizo y Cózar (2015) (citados por Grande, 2015), las entienden como tecnologías que permiten transmitir la información en cualquier momento y en cualquier lugar, y por lo tanto es un fenómeno revolucionario, impactante y cambiante. Estos autores subrayan la inmediatez y la omnipresencia de los avances de la sociedad que han ocasionado las TIC en sus definiciones.

Desde la última década del siglo XX la informática y las telecomunicaciones han recibido los beneficios de los componentes tecnológicos, los cuales siendo cada vez más pequeños y potentes, permitieron la creación de aparatos multifuncionales, muchos de los cuales tienen hoy precios accesibles como la telefonía celular, o los dispositivos de GPS, en los que pueden asociarse no solo palabras, sino también imágenes y texto, en una comunicación sin cables (Álvarez Ventura, 2018). Estas modificaciones permiten a varios autores como Sunkel (2016), redefinir las TIC como:

> "Herramientas y procesos para acceder, recuperar, guardar, organizar, manipular, producir, intercambiar y presentar información por medios

> electrónicos; estos incluyen hardware, software y telecomunicaciones en la forma de computadores y programas tales como aplicaciones multimedia y sistemas de bases de datos" (p. 8).

O las definiciones aportadas por Ana Rivoir y María Morales (2019):

> "un conjunto de herramientas, soportes y canales desarrollados y sustentados por las tecnologías (telecomunicaciones, informática, programas, computadores e internet) que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones en forma de voz, imágenes y datos, contenidos en señales de naturaleza acústica, óptica o electromagnética a fin de mejorar la calidad de vida de las personas". (p. 21)

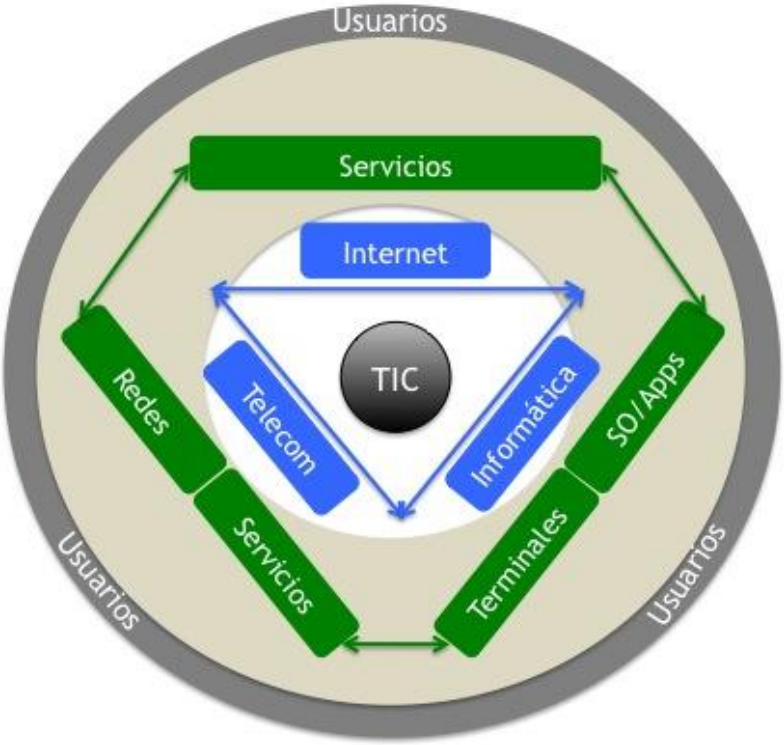
De esta forma entendemos que las concepciones de las TIC, son amplias y variables, ya que en sus génesis se elaboraban diferentes ideas que incluían las comunicaciones y los avances tecnológicos, hasta llegar a la actualidad en la que ya hablamos de herramientas, canales de comunicación, diferentes registros, incorporando diversos tipos de equipamientos tecnológicos denominados *hardware* y programas informáticos, denominados *software*.

Se componen de los siguientes elementos:

- Servicios de telecomunicación, como telefonía e internet, que se utilizan combinados con un soporte físico y lógico que permite construir la base de otros servicios, como correo electrónico, transferencia de archivos, video conferencias, video llamadas, chats, foros de discusión, entre otros.
- Las tecnologías precursoras de la radio, la telefonía y la televisión, que en la actualidad se refieren a comunicaciones móviles, dado que las mismas tecnologías que se utilizan para transmitir datos, videos digitales, video llamadas, entre otras.
- Las redes que son aquellas que utilizan cables de cobre, fibra óptica, cable coaxial, conexiones inalámbricas, telefonía celular, UTP, enlaces satelitales, entre otros.
- Los equipos se comprenden del hardware, presentando una gama muy amplia de variedades. Ejemplos de ellos son los ordenadores, smartphones, entre oros y todos los equipos que se utilizan para la conectividad de la red y la comunicación.

- El software son los programas que alimentan a cada uno de estos componentes
- El internet es una red de computadoras interconectadas a nivel mundial, en forma de tela de araña. Consiste en servidores, o nodos, que proveen información a aproximadamente 100 millones de personas que están conectadas entre ellas, a través de redes de telefonía y cable.
- La robótica, que es la ciencia y la técnica involucrada en el diseño, la fabricación y la utilización de robots, el cual es una máquina que puede programarse para que interactúe con objetos.
- El dinero electrónico es un valor o medio de pago que se almacena en un soporte electrónico, así por medio de este sistema es posible hacer transacciones sin que necesariamente intervenga un banco u otra entidad financiera. Incluye cualquier sistema de pago que involucre un medio digital por lo que engloba las tarjetas de prepago, tarjetas de crédito o monederos electrónicos, entre otros. Todos estos medios utilizan software, y en algunos casos hardware y conexión a internet para realizar las transacciones. (Guzmán Flores, 2008)

Imagen 6 Componentes de las TIC



Fuente: Guzmán Flores (2008)

2.1.1 Características de las TIC

Las Tecnologías de la Información y Comunicación como la microelectrónica, informática, telecomunicaciones, inteligencia artificial e ingeniería genética han contribuido al desarrollo social y económico, favoreciendo la combinación con otras formas de comunicación social, lo que posibilitó incluir contenidos de producción propia que permitan a todos, acceder a la información de utilidad. Para lograr estos cometidos, las TIC presentan características que les son propias y que se han ido modificando con el correr del tiempo. Belloch Ortí (2020), en su trabajo de investigación sobre las TIC, ha recopilado las características descriptas por otros autores que se ajustan a las formas actuales de estas tecnologías:

Inmaterialidad: En líneas generales podemos decir que las Tecnologías de la Información y la Comunicación, realizan la creación (aunque en algunos casos sin referentes reales, como pueden ser las simulaciones), el proceso y la comunicación contenidos de información, la

cual es básicamente inmaterial y puede ser llevada de forma transparente e instantánea a lugares lejanos.

Interactividad. La interactividad es posiblemente la característica más importante de las TIC para su aplicación en el campo educativo. Mediante las TIC se consigue un intercambio de información entre el usuario y el ordenador. Esta característica permite adaptar los recursos utilizados a las necesidades y características de los sujetos, en función de la interacción concreta del sujeto con el ordenador.

Interconexión. La interconexión hace referencia a la creación de nuevas posibilidades tecnológicas a partir de la conexión entre dos tecnologías. Por ejemplo, la telemática es la interconexión entre la informática y las tecnologías de comunicación, propiciando con ello, nuevos recursos como el correo electrónico, los IRC, etc.

Instantaneidad. Las redes de comunicación y su interacción con la informática, han posibilitado el uso de servicios que permiten la comunicación y transmisión de la información de forma rápida entre lugares alejados físicamente.

Elevados parámetros de calidad de imagen y sonido. El proceso y transmisión de la información abarca todo tipo de información: textual, imagen y sonido, por lo que los avances han ido encaminados a conseguir transmisiones multimedia de gran calidad, lo cual ha sido facilitado por el proceso de digitalización.

Digitalización. Su objetivo es que la información de distinto tipo (sonidos, texto, imágenes, animaciones, etc.), pueda ser transmitida por los mismos medios al estar representada en un formato único universal. En algunos casos, por ejemplo los sonidos, la transmisión tradicional se hace de forma analógica y para que puedan comunicarse de forma consistente por medio de las redes telemáticas es necesario su transcripción a una codificación digital, que en este caso realiza bien un soporte de hardware como el MODEM o un soporte de software para la digitalización (Belloch Ortí, 2020).

2.1.2 Internet en las TIC

La evolución de los sistemas de búsqueda de información, se encuentra ligada estrechamente con los diferentes servicios que se han profundizado mediante el uso de Internet. Su historia nos remonta a los motores de Alta Vista, Allthe Web y otros, que

fueron apareciendo a fines del siglo XX y consistían en la creación de índices o guías, que permitían rastrear diferentes contenidos disponibles en la red. El acceso a estos contenidos dependía de la posibilidad de contar con un ordenador, un *router* y acceso a internet.

Surgida como una necesidad del Departamento de Defensa de los Estados Unidos, se creó una red de comunicaciones que fuera capaz de operar desde diferentes sitios de manera segura, recibiendo el nombre de ARPA, conectando computadoras ubicadas en distintos lugares, aunque trabajaran con diferentes sistemas operativos (De Pablos, 2016). Para esto, se debieron crear unos códigos denominados protocolos, los que luego se destinarían a la educación e investigación, para llegar a dar origen, en 1990, a la *World Wide Web* (www), el cual es un sistema interconectado de páginas web públicas accesibles a través de Internet, y se constituyen en una de las muchas herramientas construidas sobre internet.

Ya en el siglo XXI, tras la aparición de la Web 2.0, pudimos observar como la comunicación se fue extendiendo, especialmente por la aparición de las redes sociales, y la utilidad que la web comenzó a brindar para la educación, la economía, las ciencias y la transformación del conocimiento. Es importante tener en cuenta a autores como Cacheiro, (2017); García-Peñalvo y Seoane (2015) Roig (2015), Santiago (2018), pusieron de manifiesto la inmediatez y la velocidad con la que se produjeron estos grandes avances en las TIC en el nuevo milenio, lo que se vio reflejado en la aparición de un número cada vez mayor de dispositivos de comunicación, que superaron a las tradicionales computadoras, como los smartphones, las tablets y notebook las cuales, por su fácil portabilidad y accesibilidad a internet, han permitido acceder en forma permanente a la red y mantenerse en constante comunicación. Esto se vio reflejado en la relevancia que las TIC han adquirido durante el periodo de pandemia de Covid-19, momento en el cual millones de usuarios han accedido al uso de internet para sus comunicaciones.

Sin lugar a duras su influencia es importante en la sociedad, lo que le ha permitido a las TIC ejercer un control social informal, a partir de la generación de tendencias, compartir hábitos y costumbres y contribuir a la cultura. Pero además, aportando una gran cantidad de datos que son útiles para el ejercicio del control social formal, ya que son una importante fuente de pruebas ante hechos delictivos, además de ser un nuevo espacio para el desarrollo

de los mismos. A continuación, presentamos las formas como las TIC, funcionan como herramientas del control social.

2.2 TIC y control social

El control social es entendido como "el proceso mediante el cual, los miembros de una entidad social son influenciados para adherirse a los valores y principios de comportamiento que se considera apropiado para esa entidad social" (Aguilar Avilés, 2010, p. 127).

Estos organismos de presión, mediante los cuales la sociedad mantiene el orden social y la cohesión, se conforman en mecanismos que hacen cumplir un estándar de comportamiento para los miembros de una sociedad, incluyendo una variedad de componentes como los prejuicios, los valores, las creencias, la coerción, la fuerza, la restricción o la persuasión, entre otros.

Entre los medios de control social encontramos las normas sociales, las instituciones, la religión, las leyes, las jerarquías, los medios de represión, los medios de comunicación, las redes sociales, los comportamientos generalmente aceptados, y los usos y costumbres, los que conforman el control social informal. Las leyes, las sanciones, el Sistema Policial, el Sistema Penal y el Sistema Penitenciario, conforman los medios de control social formal.

2.2.1 Medios formales de control social

Este es el control ejercido por el Estado, el cual tiene un poder coactivo legitimado a través de las instituciones estatales que integran el Sistema Penal, como el Sistema Policial, el Poder Judicial y el Sistema Penitenciario, cada uno de los cuales cumple una función previamente determinada de control social formal.

Autores como Gilbert Ceballos (1997) o Aguilar Avilés, (2010) refieren que el control social formal descansa en el aparato represivo del Estado. Se trata de una "organización formal encargada de responder a los quebrantamientos de las leyes establecidas a través de las cortes de justicia mediante el uso de la fuerza pública y la emisión de sentencias para castigar los crímenes cometidos por las personas" (Aguilar Avilés, 2010 p. 132). Este tipo de control, se caracteriza por tener al Estado como

autoridad política, el cual a través del marco jurídico promulgará que acciones, y cuáles no, se deberán realizar a fin de garantizar el orden social.

El control social formal se fundamenta en dos premisas: la aceptación de las conductas o comportamientos que se establecen en el marco legal de cada país, y otra que se refiere a las respuestas, respecto al cometimiento de conductas o actividades que afectan el orden social y que son reprimidas o juzgadas, a través de las instituciones del Estado. Dentro de esta instancia, se encuentran aquellos organismos que, regulados mediante una disposición legal, se encargan de regular sus funciones y objetivos, encaminados principalmente a aportar una vía para lograr el orden social que ha sido quebrantado (Aguilar Avilés, 2010).

El ejercicio de este tipo de control es llevado a cabo por las instituciones que integran el sistema penal: el Sistema Policial, el Poder Judicial y el Sistema Penitenciario los que conforman el control social punitivo, y es dirigido a quienes han vulnerado las normas sociales e incurrido en conductas que fueron tipificadas por la ley como delictivas. Los agentes de control social punitivo actúan de modo coercitivo imponiendo sanciones a los individuos. Este control social funciona cuando el control social informal ha fracasado.

2.2.2 Medios informales de control social

Son aquellos que no están institucionalizados, como los medios de comunicación, la familia, la educación, las normas morales, etc., los que no tienen una formalización a través de normas o leyes escritas. Estos son:

La familia: es el primer grupo de referencia de todo ser humano, en el cual el individuo nace, crece y se desarrolla, adquiriendo las primeras nociones de vida que incorpora a través de sus relaciones con adultos.

La escuela: tiene un papel fundamental al igual que la familia. El individuo se integra en esta institución a edades tempranas, cuando ya está preparado para salir del seno familiar y adquirir otros conocimientos a través de la enseñanza y el contacto con personas ajenas que portan otros valores.

La religión: es uno de los medios de control social informal más antiguos de la humanidad, junto con la familia que se ha caracterizado por ser un instrumento de fuerte

dominación. En algunos países, o regiones, aún tiene un fuerte arraigo dentro de la sociedad.

Las organizaciones de masas: insertas dentro de la sociedad como formas organizacionales de los individuos, tienen sus propias reglamentaciones, pudiendo aplicar sanciones morales a quienes desvían el cumplimiento de las normas establecidas.

Los grupos informales y la comunidad: constituyen mecanismos independientes del control social informal y tienen una influencia directa sobre los individuos por ser allí donde éstos se desenvuelven. Su rechazo o aceptación resulta de vital importancia para los individuos en su desarrollo social.

Los medios de comunicación y las redes sociales son formas de control social utilizadas a fin de que se acepten normas éticas, sociales y jurídicas por los individuos. Estas se ejecutan en función de las normas que son impuestas a los ciudadanos cuyo objetivo es el de reprimir conductas que puedan resultar nocivas para el resto de los miembros de una sociedad. Especialmente las redes sociales presentan normas que son particulares y específicas de cada una, y de las que nos ocupamos en el siguiente apartado.

2.2.3 Redes sociales como medios de control social

Las redes sociales se han convertido en nuevos espacios de control social informal, modificando conductas, pero además contribuyendo a generar espacios delictivos. Delitos contra la privacidad, o de suplantación de identidad, son habituales en las redes sociales. En ellas también, podemos encontrar delincuentes que ya no son hackers o informáticos, sino que se trata de cualquier persona que utilice las redes y, en ellas, manifieste un comportamiento delictivo.

Constante, (2013) sostiene que las redes sociales, son

> "una herramienta telemática de comunicación que tienen como base la web, que se organiza alrededor de perfiles personales o profesionales de los usuarios y tienen como objetivo conectarse secuencialmente a los propietarios de dichos perfiles a través de categorías, grupos, etiquetados personales, etc., ligados a su propia persona o perfil profesional" (p.35).

En los perfiles se vuelcan datos personales, opiniones personales, e interacciones con otros usuarios con los que se comparte, o no, ideas, gustos, preferencias, actividades.

Estas redes, funcionando como panópticos, se nutren de individuos que vigilan y se auto vigilan, que tratan de instaurar tendencias, difundir su propia verdad, vender sueños y felicidad, y de esta forma buscan imponer conductas (Pérez, 2020). Como empresa es un macro-panóptico con sus megas estructuras informáticas, que tienen la capacidad de adquirir información de cualquier sujeto o grupo y venderla (Pérez, 2020). De esta manera, las redes sociales construyen identidades, difunden ideas, establecen comportamientos, deseos, creando subjetividades que alienan y controlan.

Funcionan como dispositivos de control con sus propias normas y reglas, que de no ser respetadas por sus usuarios, estos son pasibles de algún tipo de castigo. Las formas de control subjetivas que aplican, se basan en comunicaciones que muestran modos de vida que las personas disfrutan, pero también han ido creciendo en referencia a la comisión de hechos delictivos o de violaciones a las normas de convivencia que son aplicables por las propias redes sociales. A continuación, se desarrollan las redes sociales más utilizadas en Argentina, y sus normas.

2.2.3.1 Facebook

Esta red social es la más antigua, creada en 2004 por Mark Zuckerberg. En la actualidad pertenece a la empresa Meta, que incluye una multiplicidad de servicios informáticos y otras redes sociales. Su funcionamiento se basa en sistemas GNU/Linux, usando el conjunto de tecnologías LAMP, entre otras (Pérez, 2020).

Su funcionamiento es amplio y permite ingresar desde una amplia gama de dispositivos con conexión a internet. Para su ingreso los usuarios pueden crear un perfil contando previamente con un e-mail de referencia, en el que se incluyen datos como nombre, fecha de nacimiento (se requiere ser mayor de 18 años), lugar de residencia, profesión, trabajo, lugares visitados, preferencias musicales, entre otros datos de carácter personal que pueden ser vistos por otros usuarios. La red solicita muchas veces la conexión con un teléfono celular, pero esta no es una condición excluyente para crear usuarios.

Una vez creado el perfil, los usuarios podrán buscar personas para incluirlas en su red, además de recibir sugerencias de amistad, propuestas de inclusión en grupos, o seguimiento de páginas especiales, todo lo cual se encuentra predeterminado por la red en

relación a los gustos del usuario y sus interacciones con otros usuarios. A su vez, esta red cuenta con una mensajería privada que permite a los usuarios, mantener charlas privadas con otros usuarios.

En la actualidad esta red cuenta con 2.420 millones de usuarios registrados alrededor de todo el mundo, los que interactúan independientemente de su ubicación geográfica. La red cuenta con un MarketPlace donde se realizan ventas y compras, las cuales pueden ser, además, compartidas en grupos creados por los usuarios con la finalidad de comprar y vender todo tipo de artículos, nuevos y usados. Por otro lado es utilizada con mucha frecuencia para realizar delitos de *grooming*, mediante la modalidad de escraches generados por perfiles que no son reales; estafas; *ciberbulying*; *sextorsion*; circulación de pornografía infantil, como los más frecuentes (Pérez, 2020). Además, el ciberodio puede reflejarse en los denominados *haters*, quienes realizan comentarios y comportamientos negativos y críticos para dañar a otras personas, haciéndolas sentir mal. Este tipo de mensajes pueden también, hacerse en forma personal, sin embargo las redes sociales son el espacio preferido para realizar este tipo de manifestaciones.

Frente a reiteradas denuncias recibidas en la red, ampliaron el sistema de normas comunitarias, que tiene por finalidad la de controlar los contenidos. Las mismas comprenden la violencia e incitación a la violencia; organización de actividades nocivas y publicidad de la delincuencia; regulación de bienes de compra/venta (como drogas, armas de fuego, sus piezas, entre otros); fraudes y estafas. En este punto buscan evitar las estafas financieras, estafas relacionadas con una identidad no auténtica, estadas con productos o premios, documentos falsos, robos de información como fraude con tarjetas de crédito/débito, comercialización de exámenes educativos, entre otros. Contenidos que inciten al suicidio y lesiones; explotación sexual, abuso y desnudos de menores; explotación sexual de adultos; *bullying* y acoso; explotación de personas; vulneraciones de la privacidad y derechos de privacidad de imágenes; discursos de odio o incitación al odio; contenido gráfico violento; entre otras normas (Facebook, 2022).

Califican la integridad de las cuentas mediante sistemas de seguridad de identificación, ya sea por el correo electrónico aportado como también por el teléfono asociado a la cuenta. Respeto por la propiedad intelectual; contenido multimedia

manipulado; noticias falsas y los contenidos que pueden ser denunciados por los usuarios. En este punto es importante tener en cuenta que muchas veces estos contenidos denunciados por los usuarios no reciben sanciones (Facebook, 2022).

2.2.3.2 Twitter

Creada por Jack Dorsey en el año 2006, posee aproximadamente 300 millones de usuarios que generan 65 tuits diariamente. Esta red es más dinámica que Facebook, es considerada como el servicio más importante de redes sociales de internet. Cuenta con una plataforma que permite escribir hasta 280 caracteres por cada interacción, que se muestran en la página principal (Pérez, 2020). Para su utilización, al igual que Facebook se requiere de un correo electrónico con el que se procede a la creación de un perfil personal, en el que se pueden volcar los mismos datos que en Facebook. Esta red ha creado un sistema propio de lenguaje que permite a los internautas identificar rápidamente acciones como la implementación del *Hashtag* # permite conectar los *Follow Friday* (temas del momento, del día), permite conectar sobre temas específicos facilitando la búsqueda en Twitter ; la **@** que además de ser parte de un correo electrónico, es la denominación que antecede al nombre de usuario y el que permite su identificación en la red; avatar, el cual es la imagen de cada usuario; *block*, el término designado para la práctica de bloqueo de usuarios; *Direct Messages* (DM), mensajería directa, la cual puede ser individual o grupal; *Follow* por su nombre en inglés significa seguir a otro usuario, convertirse en *follower*; *timeline* es la línea de tiempo en la biografía personal; *Reply*, que significa enviar un tuit directamente a un usuario utilizando la fórmula: @NombreUsuario + tweet a enviar; *Retweet*, consiste en republicar los tuits que interesa replicar; *Treding Topic* (TT), temas populares que diariamente alcanzan mayor representación en la red y *Unfollow*, que significa dejar de seguir (HelpTwitter, s.f.). Esta red presenta, al igual que todas las redes, la opción de bloqueo de usuarios.

Siendo la red preferida por los políticos, es también una red que es utilizada para ciberdelitos, como la estafa, la difusión de pornografía, difusión de desnudos, *ciberbullying*, *phishing*, entre otros. Sus normas comunitarias son más laxas que las presentadas en la red Facebook. No cuenta con un espacio de compra venta y la interacción de los usuarios es mucho más dinámica pero con menos contenido multimedia. No permiten la violencia, sin

embargo los tuits suelen estar presentes un tiempo, y muchas veces permanecen más de 24 h si no han sido denunciados; no permiten realizar actos de terrorismo; no se permite la explotación sexual infantil; el acoso/abuso es también parte de las normas comunitarias de la red; contenidos que inciten al suicidio o autolesiones; no permite usar el servicio para actividades ilegales (Twitter, s.f.), entre otras normas.

Las normas de seguridad de esta red son menos rígidas que otras redes, ya que no siempre detectan contenidos prohibidos, lo que la convierte en la red preferida por los *haters*.

2.2.3.3 Instagram

Esta red social es propiedad de la empresa Meta, y fue creada en el año 2010, ganando rápidamente popularidad con más de 100 millones de usuarios activos en 2 años. En la actualidad posee más de 300 millones de usuarios (Pérez, 2020).

Al igual que las otras dos plataformas, Instagram permite crear usuarios que pueden contener datos personales que cada persona desee incorporar. Más semejante a Facebook que a Twitter, esta red social permite la realización de intercambios comerciales gracias a las propagandas y la gran participación de grandes marcas que promocionan sus productos. Con un soporte técnico que permite el intercambio de archivos multimedia, y bajo la forma de proporcionar más información mediante imágenes y videos, se diferencia de las otras redes en tanto muchos usuarios comparten momentos permanentes de su vida cotidiana. Cuenta con mensajería privada en la cual los usuarios interactúan en forma privada.

La red es utilizada por famosos y por los denominados "*instagramer*" que son usuarios que realizan ventas y promociones de producto, marcando tendencias de moda y contribuyendo con la distribución del mercado. Desde el año 2017, la red cuenta con el denominado Instagram Shopping, herramienta que permite etiquetar hasta 5 productos en una sola foto, o 20 en lo que se denomina "formato carrousel" que consiste en subir una serie de fotos en las historias, las cuales tienen una duración de 24 h. Las etiquetas pueden ser mostradas por las marcas, y redirigir a los usuarios hacia sus tiendas web para que concreten la compra. Es una importante herramienta del *ecommerce* mundial (Pérez, 2020).

A diferencia de las otras dos redes, en esta los contenidos multimedia son los que caracterizan el uso de Instagram, contando además con un conjunto de filtros que permite modificar imágenes y contenidos. Los usuarios pueden compartir con sus seguidores contenidos en vivo, mediante videos en tiempo real en los cuales interactúan pudiendo vender productos, ofrecer servicios o simplemente compartir tiempo libre.

Las normas comunitarias de esta red son más rígidas que las anteriores, ya que detectan palabras ofensivas, limitando a los *haters* en sus comentarios. Cuenta con algunos hashtags prohibidos que, de usarlos, ponen en riesgo las cuentas. Esta red cuenta con la denominada "activación en dos pasos", la cual consiste en verificar un correo electrónico y, generalmente, un número de teléfono y envío de código a WhatsApp y mensaje de texto; permite eliminar comentarios no deseados en las publicaciones; no permite desnudos o actividad sexual; símbolos o lenguaje que incitan al odio; violencia u organizaciones peligrosas; venta de artículos ilegales o regulados; *bullying* o acoso; infracción de la propiedad intelectual; suicidio, autolesión o trastornos alimenticios; información falsa y otros motivos que permite describir y son evaluados (Instagram, s.f.).

Las redes mencionadas son las más utilizadas en Mendoza y Argentina, si bien existen otras a nivel internacional, a la presente investigación le interesan aquellas que, ejerciendo mecanismos de control social informal, se han convertido en espacios de interacción que permiten realizar hechos delictivos.

2.3 El delito en la era digital

Las conceptualizaciones del delito informático han también evolucionado, al igual que el concepto de internet. Han sido denominados como "delitos electrónicos", "delitos relacionados con la computadora", "crímenes tecnológicos", "delitos telemáticos, "delitos informáticos".

El inexorable paso del tiempo, en combinación con otros aspectos, como el aumento de la dependencia de las personas de las tecnologías de la información, han contribuido a la aparición de incidentes de seguridad de la información que hacen que el ciudadano común vaya tomando conocimiento y dimensión de la existencia de este tipo de delitos. Esta fluidez de información que circula en forma permanente, ha violado otros derechos del hombre, dando inicio a nuevos fenómenos delictivos.

Al respecto la doctrina menciona casos emblemáticos como los datos difundidos por Wilikeaks (2010), o las acciones realizadas por Edward Snowden, quien en 2013 había mencionado que podían *hackear* a cualquier computadora del mundo, o el ciberataque más grande del mundo llevado a cabo por PRISM, que logró dejar sin sistemas a grandes multinacionales, entre ellas Telefónica, afectando a 99 países (Temperini, 2018).

Para realizar un análisis de la seguridad informática, se deberán conocer las características de lo que se pretende proteger, que no es otra cosa más que la información.

El Dr. Cristian Borghello sostiene que la información

> "Es una agregación de datos que tiene un significado específico, más allá de cada uno de estos. Establecer su valor es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación" (p.38).

Entonces, siguiendo la doctrina, podemos sostener que el incidente de seguridad son todos los hechos no deseados donde se compromete, de cualquier forma, la seguridad de la información. Es decir, todos los delitos informáticos son, en el fondo, incidentes de seguridad de la información (Temperini, 2018).

Curi, Delaux y Waker (2005) definen a los delitos informáticos como: "aquellas conductas disvaliosas socialmente reprochables desde el punto de vista penal, que concretadas mediante instrumentos, sistemas informáticos y virtuales, pueden tener como objeto la violación de cualquiera de los bienes jurídicos tuteladas por la ley, en un momento dado". (p.134).

2.4 La cibercriminología

Las definiciones para los crímenes informáticos o cibernéticos, incluyen a los términos: cibercrimen, ciberdelito, cibercriminalidad, ciberdelincuencia, criminalidad informática y delito informático, lo que supone un problema para la ciencia social como la criminología, en la que los conceptos deben ser claros.

Esta evolución del término es importante de rescatar puesto que la misma se vincula con el avance de las tecnologías y su perfeccionamiento en relación con las comunicaciones. Desde la criminología moderna, el estudio de los comportamientos ilícitos

en la red y la preocupación legal que existe en este contexto, ha ido modificando el análisis del riesgo de la información. Así, en un primer momento de la cibercriminalidad, lo característico era que el delito se ejecutaba a través de ordenadores, posteriormente el delito se cometía a través de internet y, por último y más actualmente el delito se comete exclusivamente con el uso de las TIC (Miró Llinares, 2012). De esta forma, el término cibercrimen incorpora la información que pueden contener los sistemas informáticos, la afectación a la intimidad o el patrimonio, pero y fundamentalmente, las interacciones y crímenes que en el ciberespacio, se pudieran producir y que pudieran afectar a otros bienes jurídicos como la indemnidad sexual, la dignidad personal y hasta la seguridad nacional. Desde esta concepción podemos entender que, si bien internet es un espacio de interacción e información, todos los delitos que en ella se cometan, deberán ser considerados delitos informáticos en primera instancia, para luego proceder a identificar que otros bienes protegidos se han violentado (Miró Llinares, 2012).

El ciberdelito, se diferencia del delito convencional en que el primero se desarrolla en un mundo virtual, a través de un medio informático y por lo general, con el uso del internet sin desarrollarse en un ámbito físico, aunque pueda tener vinculaciones con este.

El "Convenio de Ciberdelincuencia del Consejo de Europa" (conocido como el Convenio de Budapest), define a los delitos informáticos como: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos" (Council of Europe, 2001, p. 5). Estos presentan características particulares en sus comportamientos, además de requerir de tecnología para su ejecución, las que se describen en el siguiente apartado.

2.4.1 Características de los ciberdelitos

Este tipo de delitos presenta un comportamiento que incide en el soporte lógico de un sistema informático, implicando el uso de redes computacionales, y que implican las siguientes conductas:

- Aquellas que suponen destrucción o inutilización de datos o programas de sistemas informáticos, que suelen vincularse con el concepto de sabotaje informático;

- Las que implican acceso u obtención indebidos de datos o programas de sistemas informáticos, que suelen ligarse con la idea de espionaje informático;
- Las que suponen alteración o manipulación de datos o programas de sistemas informáticos, que suelen vincularse con el concepto de fraude informático (Lux, 2018).

Los aspectos de los ciberdelitos son similares a otros delitos, ya que existe una acción u omisión por parte de un sujeto que debe ser típica, es decir prevista en nuestro Sistema Jurídico-penal, que sea antijurídica y no se encuentre amparada por alguna causa de justificación. Debe existir culpabilidad en el sujeto, y debe ser pasible de una determinada sanción (Linares, 2020). Así, la doctrina establece que los delitos informáticos deben presentar en su estructura, las mismas características que todo tipo de delitos, comprendiendo entre ellos, los aspectos básicos que hacen que una conducta sea reprochable y castigable por el ordenamiento penal.

El delito informático implica actividades criminales que fueron, en un principio, difíciles de tipificar en figuras preexistentes como el robo, hurto, fraudes o falsificaciones, entre otras. Sin embargo, lo que ha prevalecido en la clasificación de estos delitos, ha sido la utilización de una computadora para su regulación. El medio de comisión delictiva es la informática, en la cual confluyen muchas técnicas y procesos, como también diferentes tipos de máquinas. Aquí, es importante destacar lo que plantea Laura Lux (2018), sosteniendo que la doctrina entiende que algunos de esos comportamientos, pueden tener en común algunos aspectos de otros delitos como una estafa. Sin embargo, será el componente informático el que determine que se trata de un ciberdelito, ya que corresponde con el medio utilizado para la realización de dicha estafa. Es por esto que muchos de los delitos informáticos, pueden ser difíciles de encasillar, aunque la doctrina, al igual que la jurisprudencia, presenta una tendencia a encasillar aquellos que requieren del uso de redes computacionales, como contexto delictivo en el que puedan surgir particulares riesgos para los individuos.

2.4.2 Principales delitos informáticos

La doctrina ha tratado de sistematizar de diversas formas los nuevos comportamientos ilícitos surgidos en el ciberespacio, buscando sistematizar el "*target*" (objetivo), y la "*toll*" (herramienta) del ataque delictivo. Miró Llinares (2012) sostiene que lo que se persigue en la calificación delictiva del ataque es

> "…que el cibercrimen lo es tanto cuando Internet, sus servicios o las terminales informáticas a él conectadas, constituye el objeto sobre el que se realiza el ataque, como cuando es el medio a través del cual se ejecuta la agresión. Se trata, por tanto, de una mera sistematización inclusiva y simbólica, más que de una clasificación que diferencie entre las tipologías de conductas por algún tipo de efecto asociado a cada una de ellas. En otras palabras: no se deriva ninguna consecuencia del hecho de que un cibercrimen lo sea por el medio utilizado o por el objeto contra el que se comete, pues en última instancia se trata de una sistematización tipológica que sirve para incluir conductas y no para separarlas (p.48).

La siguiente clasificación tipológica de la cibercriminalidad agrupa por tres tipos de cibercrímenes, atendiendo al aspecto en que inciden las TIC en el comportamiento criminal y a su propósito en el ámbito del ciberespacio:

Tabla 1 Modalidades de cibercrimen

	CIBERATAQUES PUROS	CIBERATAQUES RÉPLICA	CIBERATAQUES DE CONTENIDO
CIBERCRÍMENES ECONÓMICOS	• *Hacking* • *Malware* intrusivo • *Malware* destructivo • Ataques *insiders* • Ataques DoS • *Spam* • Ciberocupación red • *Antisocial networks*	• Ciberfraudes: *phishing, pharming, scam, auction fraud*, etc.) • *Ciberspyware* (uso de *sniffers* y demás *spyware*, ciberespionaje de empresa) • *Identity theft* • *Spoofing* (DNS *sopoofing*, ARP *spoofing*, IP *spooging*) • Ciberblanqueo de capitales • Ciberextorsión • Ciberocupación	• Distribución de pornografía infantil en internet • Ciberpiratería intelectual
CIBERCRÍMENES SOCIALES		• *Spoofing* • *Cyperstalking* • *Cyberbullying* • *Online barassment* (ciberamenazas, coacciones, injurias, etc.) • *Sexting* (y extorsión con imágenes sexting) • *Online grooming*	
CIBERCRÍMENES POLÍTICOS	• Ataques DoS (*cyberwar*) • Ataques DoS (*Cyberhacktivism*) • Malware intrusivo	• Ciberespionaje terrorista • Ciberguerra	• *Obline bate speech* • Ciberterrorismo (difusión de mensajes radicales con fines terroristas)

Fuente: Miró Llinares (2012)

Los ciberataques puros son aquellos actos que se producen únicamente en el ciberespacio. En estos delitos tenemos la definición de los siguientes delitos:

- *Hacking:* es el delito cometido por un hacker que ingresa ilegítimamente a un sistema informático y borra, destruye, inutiliza o modifica datos, información, imágenes, software, etc., tipificado en el art. 183 del Código Penal.

- *Malware intrusivo:* programa hostil intrusivo denominado como "virus informático" que permite al cibercriminal ingresar en equipos, sistemas o redes y dañarlos asumiendo el control de parte o de todas las operaciones del equipo. Existen los virus, gusanos, troyanos, *ransomware, spyware, adware*

- *Malware destructivo*: son programas que, introducidos en los dispositivos, destruyen datos y archivos en ellos guardados.

- *Ataques insiders:* personas que actúan en contra de la organización a la que pertenecen. Son trabajadores, ex trabajadores o proveedores que aprovechan la capacidad de acceder a la información influyendo negativamente, robando información, perjudicando o atacando intereses de la empresa o institución en la que trabajan o trabajaron.

- *Ataques DoS* (Denegación de Servicio): este tipo de ataque afecta al servicio, ya que tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina bloqueando el servicio. Este tipo de ataques puede afectar a la fuente que ofrece la información, como puede ser una aplicación o el canal de transmisión, como la red informática.

- *Spam*: es el correo comercial no solicitado generalmente enviado a las direcciones electrónicas de los consumidores sin la autorización y consentimiento del consumidor, comúnmente es enviado por empresas de mercadeo o telemercadeo. Pero además, es utilizado por compañías ilegítimas o por ciberdelincuentes con la finalidad de obtener información del usuario.

- *Ciberocupación red:* es el registro de un nombre o dominio, sabiendo que un tercero tiene interés legítimo en el mismo, con una doble finalidad: una especulativa que implica solicitar una cantidad económica para que ese tercero

lo compre, o bien, una finalidad publicitaria para atraer a visitantes y tráfico a la web sirviéndose de la reputación de ese tercero.

- *Antisocial networks:* se refiere a las conductas antisociales que se realizan en las redes sociales, las cuales muchas veces se constituyen en delitos de calumnias, injurias, ciberodio, entre otras.

Los ciberataques réplica son aquellos que se cometen en el espacio offline y tienen su espejo en el ciberespacio.

- *Ciberfraudes*: se refiere a un conjunto de delitos económicos, de fraude y estafa como el *phishing, vishing, smishing, pharming,* que realizan los estafadores a través de correos electrónicos engañosos, llamadas telefónicas, SMS o WhatsApp falsos, buscando la captura de datos personales de sus víctimas y cometer el fraude.

- *Ciberspyware*: se trata de software malicioso que infecta los ordenadores y dispositivos recopilando información personal, de navegación, y todos los datos útiles, ejecutándose en segundo plano y sirve para el ciberespionaje de personas, empresas e instituciones.

- *Identity theft*: robo de identidad (ID) ocurre cuando alguien roba su información personal para cometer fraude. El ladrón de identidad puede utilizar la información para solicitar crédito, retirar dinero o cualquier acción que afecte a la víctima.

- *Spoofing (DNS sopoofing, ARP spoofing, IP spooging*): es la suplantación de identidad en redes con la finalidad de falsificar datos en una comunicación. Incluye la suplantación de identidad por falsificación de tabla ARP se trata de la construcción de tramas de solicitud y respuesta ARP modificadas con el objetivo de falsear la tabla ARP (relación IP-MAC) de una víctima y forzarla a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. Suplantación de DNS se corresponde con la suplantación del dominio

web, falseando una relación entre nombre de dominio y una IP ante una consulta de resolución de nombre.

- *Ciberblanqueo de capitales*: el blanqueo de capitales o lavado de dinero es el conjunto de operaciones destinadas a transformar bienes, dinero o activos de origen ilegítimo o ilegal, en productos de carácter lícito y transparente, o al menos logrando que aparenten esas características. Se constituye en ciberdelito cuando se utiliza el ciberespacio para su ejecución.

- *Ciberextorsión*: se incluye en los artículos 168 a 171 del Código Penal. Reprime con 5 a 10 años, cuando se produzca intimidación o simulando autoridad pública o falsa orden de la misma, se obligue a otra persona a entregar, enviar, depositar o poner a su disposición o la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos. Incluye la utilización de violencia o las amenazas contra el honor o de violación de secretos.

- *Cyperstalking*: forma de persecución que consiste en el uso de internet u otro instrumento computarizado con la intención de asediar o perseguir a alguien, a través de acciones metódicas, persistentes e indeseables generadoras de incomodidad en la vida de las víctimas.

- *Cyberbullying*: Este delito se produce mediante la utilización de mensajería instantánea, *satlking* en WhatsApp, Telegram, Messenger y en las redes sociales con la intención de perseguir, acechar a otra persona, difamarla, atentar contra su honor e integridad moral. Ello a través del descubrimiento y revelación de secretos, de la publicación de comentarios o videos ofensivos o discriminatorios, la creación de memes o el etiquetado de publicaciones (UNICEF, s.f.).

- *Online barassment*: es un tipo de acoso que se da por medio del uso de internet, caracterizado por el seguimiento e investigación constante de información sobre una persona o empresa.

- *Sexting*: Es una forma de explotación sexual en la cual una persona es inducida o chantajeada, mediante el uso de aplicaciones de mensajería por internet, con una imagen o video de sí misma, desnuda realizando actos sexuales. Por lo general los extorsionadores se comunican por medio de las víctimas con perfiles falsos en redes sociales bajo engaños de buenas intenciones. La víctima es coaccionada para tener relaciones sexuales con alguien, entregar más imágenes eróticas o pornográficas, dinero o alguna otra contrapartida, bajo la amenaza de difundir las imágenes originales si no accede a las exigencias del extorsionador o de la extorsionadora (Álvarez, 2017).

- *Ciberespionaje terrorista*: consiste en obtener datos secretos sin el permiso del poseedor de la información de individuos, competidores, rivales, grupos, gobiernos y enemigos para ventaja personal, económica, política o militar usando métodos en internet, redes sociales o computadoras individuales.

- *Ciberguerra*: es un área dentro de las agencias militares de los países que tiene como objetivo encontrar las vulnerabilidades técnicas de los sistemas o redes informáticas del enemigo para penetrarlas y atacarlas, tanto así como para extraer datos e información sensible. En este caso el ciberespacio es el campo de batalla y las armas son programas o aplicaciones informáticas.

- *Online grooming:* Tipificado como delito en el año 2013, a través de la Ley 26.904/2013 es la acción deliberada, por parte de un adulto de acosar sexualmente a un niño, niña o adolescente, a través de internet. Implica que se puede dar por cualquier canal relacionado al uso de la red, como redes sociales, páginas web o aplicaciones de mensajería instantánea. El comportamiento de los acosadores se puede dar de diferentes maneras, pero siempre es a través de internet. Por lo general el acosador presenta una identidad falsa con la que logra engañar a la víctima, con la que han logrado establecer una amistad ganando la confianza de la víctima. Para que exista *grooming*, siempre tiene que haber un componente sexual. Siempre el objetivo del acercamiento es de carácter sexual, aunque se dé por redes sociales y aunque ese componente esté ausente en las primeras etapas -cuando los vínculos son más prolongados (CPDP, 2022).

Ciberataques de contenido son aquellos que vierten el contenido ilícito dentro del ciberespacio desde donde se transmite.

- *Distribución de pornografía infantil en internet*: El artículo 128 de la ley 26.388/08, ha sido modificado por la ley 27.436/2018, estableciendo que :

  > "Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales y de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior. A su vez, será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder el material con fines inequívocos de distribución o comercialización. Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años".

  De esta forma el nuevo artículo castiga la tenencia simple de material pornográfico sin importar si se lo posee con intenciones de compartirlo o comercializarlo, con una pena de 4 meses a 1 año de prisión. Así mismo, el nuevo tipo penal mantiene la sanción a la posesión con fines de distribución o comercialización con una pena de 6 meses a 2 años, por entender que quien posee el material con fines de distribución realiza una conducta más lesiva que quien posee el material de forma simple sin esa intención. El nuevo tipo penal tampoco contempla aquellos que acceden o consumen el material sin poseerlo, como quienes lo hacen vía *streaming*. Por último, la modificación que se introduce es que las escalas penales se elevarán cuando la víctima sea menor de trece años.

- *Ciberpiratería intelectual*: consiste en la apropiación, copia y distribución ilegal de obras y productos protegidos por derechos de autor, como películas, libros, música, videojuegos, software o cualquier material protegido a través de los diferentes medios disponibles para llegar al público.

- *Online bate speech:* es el tipo de discurso de odio en línea que se lleva a cabo a través de redes sociales o internet, con el propósito de atacar a una persona o un

grupo sobre la base de atributos como raza, religión, origen étnico, orientación sexual, discapacidad o género.

- *Ciberterrorismo*: difusión de mensajes radicales con fines terroristas.

Este tipo de hechos delictivos, requiere de nuevas prácticas y nuevas formas de intervenir desde la Seguridad Pública, la cual ha recurrido también a obtener, desde las TIC, nuevas formas de intervenir en hechos delictivos, cualquiera sea su naturaleza.

2.5 Uso de las TIC en Seguridad Pública

La incorporación de las TIC ha permitido obtener mayor eficiencia y eficacia, tanto para la prevención, la investigación, el esclarecimiento del delito como también para la producción de análisis de inteligencia sobre delitos.

El mapeo del delito, los sistemas de video vigilancia, y el análisis que se deriva de los mismos, se han convertido en herramientas claves para la prevención, disuasión, control e investigación, contribuyendo a disminuir la sensación de seguridad en la población. Para esto es necesario contar con equipos altamente capacitados, pero además, es necesario contar con herramientas que permitan el almacenaje y resguardo de imágenes y fatos.

2.5.1 Incorporación de TIC en la Policía de Mendoza

Los dispositivos generados por la industria de la seguridad electrónica fueron los sistemas de intrusión, de videovigilancia, de controles de accesos, de reconocimientos biométricos, de geolocalización, de comunicación y de gestión de central de alarmas.

La innovación tecnológica a nivel de la Seguridad Pública, se evidencia en el campo de la seguridad informática la que se encuentra en desarrollo en la provincia de Mendoza, aunque su incorporación no se ha producido ni con la misma rapidez, ni el mismo impacto que la aparición de TIC en otros ámbitos. Cancino, (2017) y Dammert (2016) coinciden en afirmar que en el mundo se observan muchos cuerpos policiales que siguen utilizando los mismos medios e instrumentos convencionales para prevenir el delito y combatir el crimen. “Un ejemplo de esto, lo constituyen la utilización de la georeferencia, el análisis y el estudio de los datas para predecir los eventos delictivos, son un privilegio de muy pocas policías” (Dammert, 2016, p. 7).

La importancia de contar con acceso a TIC para los cuerpos policiales adquiere una mayor relevancia toda vez que en la actualidad los cuerpos policiales se enfrentan a nuevas modalidades de crimen. Esto lleva a que su principal reto sea el de utilizar la tecnología como herramientas que permitan al policía identificar dónde, cuándo, cómo y quién va a cometer un delito, a fin de prevenirlo. Pero también, les permiten contar con las capacidades necesarias para realizar prospectiva de posibles perfiles criminales, lo que se constituye en las mejores formas de luchar contra el crimen.

En la provincia de Mendoza, la incorporación de tecnología fue paulatina, comenzando con la adquisición de radios, telefonía celular y computadoras. En la actualidad se cuenta con tecnología de última generación en la Policía de Mendoza destinados a la Seguridad Pública, la que se describe a continuación.

2.5.1.1 Sistema TETRA

El sistema TETRA (*Trans European Trunked Radio*), es un estándar definido por el Instituto Europeo de Normas de Telecomunicaciones, cuya finalidad es unificar diversas alternativas de interfaces de radio digitales para la comunicación entre los profesionales de los servicios de emergencias y servicio público.

En Mendoza funciona en todo el territorio siendo una plataforma de comunicaciones inalámbrica disponible de manera continua, las 24 horas d los 7 días de la semana, con cobertura, en zonas rurales y urbanas. Integra todas las fuerzas de seguridad y emergencia, como Policía, Bomberos, SEC, Gendarmería, Defensa Civil, municipalidades, Vialidad y Metrotranvía, permitiendo la coordinación y gestión de los recursos operativos y tácticos en forma eficiente, confiable y segura. La provincia cuenta con 54 sitios TETRA, cuya capacidad de radiocomunicación, permite continuar con la conectividad por medio de anillos y enlaces ante eventuales catástrofes naturales, como aludes en Alta Montaña o tormentas de viento y lluvia. La plataforma es de vital importancia, ya que al ingresar un llamado de emergencia al 911 y generarse un suceso, las fuerzas de emergencia se comunican internamente mediante el sistema para la resolución. Ofrece suscriptores de distintas agencias, y cada uno de ellos está georreferenciado en la provincia.

Su tecnología permite una comunicación de voz en tiempo real entre los equipos TETRA y hacia y desde los centros de control operados por los despachadores, ubicar geográficamente a los equipos TETRA, transmitir datos y mensajes y grabar todas las comunicaciones (Prensa Gobierno, 2021).

2.5.1.2 Cámaras de seguridad

La provincia de Mendoza posee 1522 cámaras de seguridad con monitoreo de vigilancia Bosch, el que consiste en un sistema de video de seguridad destinado a la prevención del delito. Su análisis inteligente de videos, le permite al operado atender una gran cantidad de cámaras al mismo tiempo, las que poseen una tecnología capaz de detectar el movimiento y que realiza un análisis inteligente para alertar sobre objetos en movimiento o abandonados, mediante cruces de líneas virtuales, merodeos en zonas bancarias, realizando búsquedas de imágenes forenses, a partir de las imágenes almacenadas previamente. Esto permite realizar un trabajo en tiempo real y actuar rápidamente ante situaciones delictivas. Esto se monitorea desde el CEO (Centro Estratégico de Operaciones) que trabaja como el principal centro de la provincia (UNIDIVERSIDAD, 2021).

Para su implementación se cuenta con una red de datos de alta capacidad y confiabilidad vinculada con fibra óptica de hasta un Gigabit a cargo de la empresa Arlink, manteniendo el protocolo IP correspondiente.

2.5.1.3 Aparatos biométricos faciales

En la actualidad, el aporte de las nuevas tecnologías y los sistemas basados en datos biométricos de identificación, permiten una rápida búsqueda y respuesta.

El sistema biométrico de reconocimiento facial es una tecnología capaz de identificar a un sujeto a través de una imagen o video que haya captado su rostro. Esta tecnología recoge un conjunto de datos biométricos únicos de cada persona, asociados a su rostro y expresión facial para identificar, verificar y/o autenticar a una persona.

En la actualidad son múltiples los dispositivos destinados a las capturas de huellas dactilares, muchos de los que presentan estándares de tipo *inkless* (dispositivos que posibilitan la adquisición de huellas sin necesidad de calcar dibujos) (INTERPOL, 2022). Requiere de un dispositivo que disponga de tecnología fotográfica digital, a fin de generar y

obtener las imágenes y datos necesarios para crear y registrar el patrón biométrico facial de la persona a identificar. Este tipo de identificación se diferencia de otros en tanto utiliza patrones matemáticos únicos y dinámicos de la persona, lo que convierte a este dispositivo de identificación, en uno de los más seguros y eficaces.

La gran dificultad reside en lograr que este proceso se realice en tiempo real, algo que no está al alcance de todos los proveedores de software de verificación de identidad.

Este tipo de dispositivos corresponde al grupo de las denominadas tecnologías de Inteligencia Artificial (IA), que pueden funcionar con los más altos estándares de seguridad y fiabilidad, con la gran ventaja de llevar a cabo el proceso en tiempo real.

Al igual que la biométrica dactilar, pueden ser utilizados mediante una aplicación móvil.

2.5.1.4 Biométrica dactilar

Los captores ópticos reflexivos permiten colocar el dedo sobre una superficie de cristal iluminado por un diodo LED. Una vez que se coloca el dedo sobre el cristal, la luz absorbe las crestas dactilares, a través de un sensor de imagen, los que son enviados a una base de datos pudiendo identificar personas.

Esta tecnología de última generación fue adquirida en el año 2017 y adaptada para identificar rápidamente a las personas mediante la utilización de dispositivos biométricos de seguridad. Estos dispositivos permiten identificar personas mediante la huella dactilar, la cual ingresa al compendio histórico de antecedentes, mediante el sistema ALEGIS (*Advanced Electronic Guidance Information System*), el cual es un motor de interpretación de la base de datos almacenados de la población mendocina (INTERPOL, 2022). La policía de Mendoza dispone de más de 300 equipos biométricos, con tecnología 3G y 4G, que pueden trabajar de manera móvil utilizando redes de telefonía, redes de Wifi o cualquier tipo de conexión a la red que les permita obtener los datos en un lapso no mayor a treinta o cuarenta segundos.

2.5.1.5 Sistema CoDIS

El sistema CoDIS (Combined DNA Index System) es un software del FBI destinado a recopilar los datos genéticos que se aplica en Mendoza desde octubre de 2018, convirtiendo a esta provincia en pionera en la adopción de esta tecnología. Consiste en la toma de muestras de ADN de casi la totalidad de los delincuentes arrestados o condenados por algún hecho ilícito, a fin de generar un banco de perfiles genéticos (Gobierno, 2018).

2.5.1.6 Drones

Desde el año 2019 Mendoza ha incorporado 4 drones al Ministerio de Seguridad, destinados a reforzar las tareas de patrullaje y apoyo de los recursos apostados en tierra, pudiendo operar de día y de noche con un bajo nivel de ruido y alzando más de 100 metros de altura. Cuentan con cámaras con capacidad de transmisión de imágenes en tiempo real, y video con zoom que permite la identificación de rostros y patentes. Estos nuevos aparatos tienen base en la Base Cóndor, la cual depende del C.A.P (Cuerpo Aéreo Policial) y son transportados por el CEO Móvil, el cual es un vehículo policial adaptado para tal fin. También son trasladados en los helicópteros del Cuerpo de Aviación Policial (CAP) (PoloTIC, s.f.).

2.6 Uso de las TIC en la investigación Criminal

La innovación tecnológica ha acompañado los cambios en las formas de realizar la investigación criminal en los últimos años, sobre todo en las diferentes técnicas que se aplican para la recopilación de datos. Desde el registro dactilar, hasta la identificación biométrica, la tecnología ha servido de herramienta para la investigación criminal.

La tecnología se puede aplicar a todo tipo de delitos, por muy tradicionales que sean, incluso en casos de homicidio, agresión sexual o rapto, las autoridades pueden valerse de recursos tecnológicos para rastrear la huella digital, intervenir las comunicaciones o seguir los movimientos a través de cámaras de seguridad.

La importancia de utilizar la tecnología en la investigación criminal radica en que no sólo aportan pruebas, sino que además permiten agilizar las investigaciones. La principal ventaja radica en su operatividad, para la obtención de evidencias de cualquier clase de delito, dado que resulta una eficaz herramienta, sobre todo en la que los dispositivos electrónicos pueden constituirse en una prueba.

La incorporación de la ciencia de datos al trabajo policial, contribuye además, al trabajo preventivo y la focalización de la intervención de las fuerzas policiales. El procesamiento de los datos históricos es una herramienta de gran utilidad, principalmente en el desarrollo de algoritmos basado en el análisis computacional de macrodatos[2] forenses. Ceballos Espinoza (2021), sostiene que:

> "…en este contexto, surge del concepto de Inteligencia e Investigación Digital, para referirse al campo de conocimiento que se ocupa de los usos policiales de la tecnología para detectar e interrumpir la delincuencia, así como para obtener una mayor conciencia del panorama delictivo para el desarrollo de análisis e inteligencia criminal" (Ceballos Espinoza, 2021, p.68).

La vigilancia digital se ha centrado en dos campos particulares: la predicción y la prevención delictiva, enfocada principalmente en actividades como la vigilancia en línea y la vigilancia policial predictiva (Ceballos Espinoza, 2021).

La criminología moderna apoyada por el análisis computacional y el desarrollo de algoritmos para el procesamiento y la gestión de la información proveniente de macrodatos forenses, ha demostrado su utilidad en distintos contextos propios del sistema de persecución penal y de la investigación criminal. Con respecto a esto último, Ceballos-Espinoza (2021) rescata la relevancia de los elementos criminógenos levantados en cada investigación criminal, los que considera imprescindibles para comprender la fenomenología tras cada delito investigado. En particular, aquellos casos en que se desconoce la identidad del autor del ilícito, agregando que la investigación crimina, (llevada a cabo por la policía) debe recurrir a estrategias innovadoras que permitan asegurar el esclarecimiento de la criminodinámica de los hechos y, dentro de ella, el rol desempeñado tanto por el victimario como por la víctima (Ceballos Espinoza, 2021).

2.6.1 La prueba digital

Con el advenimiento de las redes sociales y el servicio de mensajería, como formas de interacción social, cada vez más usadas, las pruebas digitales han adquirido nuevas formas de comprensión.

[2] Big data o macrodatos es un término que hace referencia a una cantidad de datos tal que supera la capacidad del software convencional para ser capturados, administrados y procesados en un tiempo razonable. El volumen de los datos masivos crece constantemente.

La prueba digital es “toda información digital empelada por las partes para afirmar la realidad de un hecho durante el proceso judicial” (Rivolta, 2012). Para que esta prueba sea validad, la información debe haber sido producida, almacenada o transmitida por medios digitales (por ejemplo por un correo electrónico, conversaciones de WhatsApp, entre otras). Deber ser, además, capaz de acreditar los hechos.

La información que se genera y transmite en el ámbito digital puede ser de dos formas. Una es aquella que no es inteligible para las personas, es decir la forma como se crea, viaja, transmite y se almacena la información, y por otro lado, la representación visual que si puede ser interpretada por las personas.

Huertas Gutiérrez (2021) consultor de UNODC[3], sostiene que la evidencia digital es “Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático” (p.17). Esto demuestra que es un término utilizado de manera amplia para describir “cualquier registro generado por, o almacenado en un sistema computacional que puede ser utilizado como evidencia en un proceso legal” (Huertas Gutiérrez, 2021, p.17).

Las pruebas digitales se caracterizan por ser:

- *Intangibles*, puesto que no puede apreciarse a través de los sentidos, ya que se requiere de procesos informáticos y dispositivos electrónicos para poder verla.
- *Duplicable*, ya que el formato digital permite que una prueba pueda ser copiada o duplicada tantas veces como se desee. Sin embargo plantea el problema de la distinción de la originalidad.
- *Volátil*, en tanto que su intangibilidad y los medios que se emplean para su creación, envío, almacenamiento y reproducción permiten que se pueda manipular, modificar o alterar.
- *Deleble* ya que puede ser destruida con facilidad, sin necesidad de destruir los soportes que la contienen.
- *Parcial*, ya que es habitual que una prueba digital esté formada por diferentes ficheros informáticos, repartidos en varios soportes digitales y localizaciones.

[3] Oficina de las Naciones Unidas contra la Droga y el Delito

La información que se obtiene de la prueba digital, se produce y almacena en instrumentos o dispositivos electrónicos o digitales, como sistemas informáticos y sus aparatos tecnológicos, que incluyen la telefonía móvil, los ordenadores, las tablets, pendrives, discos duros, DVD entre otros.

La doctrina ha considerado a la prueba digital o electrónica, como prueba documental por las semejanzas que guarda con otro tipo de documentos y por la idoneidad de su introducción en el proceso como tal. Sin embargo ha debido enfrentar una gran dificultad en su obtención ya que, como sostiene Roberto Pérez Cascella (2017)

> "existe un gran conflicto de la veracidad de la información, el riesgo de la intromisión en la vida privada a través de las redes sociales, la implicancia en la persecución del delito y el tenue velo de la obtención de prueba válida para el proceso civil" (p.6).

La protección de la esfera privada por parte de los Pactos Internacionales, a los cuales nuestra Constitución Nacional se encuentra adherida, no permiten la intromisión en los datos personales, por lo cual estas pruebas digitales deben contar con un resguardo especial y cuidando de no dañar la privacidad, especialmente de las víctimas, en función del artículo 5, artículo 10 y artículo 17 de la Convención de los Derechos Humanos.

Michell Taruffo sostiene que cuando los archivos multimedia son admitidos como medios de prueba, tiene que determinarse su valor probatorio. En general puede decirse que es estimado discrecionalmente por el fiscal o el juez, y que, en todo caso, un archivo informático nunca tiene la fuerza vinculante de algunos documentos especiales regulados por el ordenamiento codificador (Taruffo, 2008).

Muchas veces el archivo informático es considerado como el comienzo de una prueba escrita, por lo tanto es admitido como tal. Puede ser considerado también, como prueba cuando en ella se encuentra información que aporta al esclarecimiento de un delito.

Los medios de prueba establecidos en la legislación procesal argentina se unifican en la confesional, documental, el testimonio de personas que pudieron haber percibido los hechos, la inspección judicial y la prueba de peritos o dictamen calificado de expertos. Sin embargo, en la actualidad nos enfrentamos a una escasa directriz valorativa respecto a los elementos informáticos (Granero, 2019).

Los documentos electrónicos son aquellos cuyo soporte material, es algún dispositivo electrónico o magnético, y donde el contenido está codificado. Para su lectura, para su reproducción o para su interpretación, necesitaremos también el auxilio de la tecnología disponible. Fundada en el art. 319 del Código Civil y Comercial de la Nación, se establece que

> "El valor probatorio de los instrumentos particulares debe ser apreciado por el juez ponderando, entre otras pautas, la congruencia entre lo sucedido y narrado, la precisión y claridad técnica del texto, los usos y prácticas del tráfico, las relaciones precedentes y la confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen".

Esta norma entiende que la prueba electrónica no basta para tener por acreditados los hechos, sino que su utilidad radica en que puede constituir indicios suficientes para dar nacimiento a presunciones judiciales. En el ámbito forense, a mayor confiabilidad de los soportes utilizados y de los procedimientos técnicos que se apliquen a su creación, mayor será la fuerza probatoria de la misma en el juicio.

En el marco de un proceso judicial, la prueba electrónica tiene por objeto cualquier registro que pueda ser generado dentro de un sistema informático, entendiendo por éste a todo dispositivo físico (computadoras, smartphones, tablets, CDs, DVD, pen drives, etc.) o lógico, empleado para crear, generar, enviar, recibir, procesar, remitir o guardar a dichos registros, que, producto de la intervención humana u otra semejante, han sido extraídos de un medio informático (por ejemplo: registros en planillas de cálculo, correos electrónicos, registros de navegación por Internet, bases de datos, documentos electrónicos) (Vaninetti, 2018).

En la actualidad los sistemas de mensajería instantánea se han configurado como método probatorio para acreditar la ocurrencia o no de hechos que hayan sido recogidos por personal idóneo de investigaciones. La correcta identificación de la prueba documental y la prueba pericial, se amparan en el principio de libertad de la prueba, y en este punto la incorporación de datos informáticos o digitales que se presenten en un medio o instrumento independiente con denominación de prueba digital, prueba tecnológica o prueba telemática, o en algunos casos como documento electrónico por sus características diferenciales en cuanto a encriptamiento o forma codificada de la información que pueda tener, adquieren igual validez que un documento escrito en papel.

Estos nuevos elementos probatorios requieren que se realice una nueva adaptación y clasificación para su admisión, respetando las garantías para las partes intervinientes, como también respetando que dichas pruebas no sean aportadas a la publicidad hasta tanto lo decida el juez (Ambrosino, 2021). Para esto se requiere de un conjunto de actividades que garanticen el resguardo de las pruebas.

2.5.1 Guía procedimental de recolección de evidencia digital

Desde el año 2010, el Ministerio de Justicia y Derechos Humanos, junto con el Consejo de Procuradores, Fiscales, Defensores y Asesores de la Argentina, se encuentran trabajando en la creación de laboratorios forenses regionales, para lo cual se ha invertido en equipamiento, contratación y capacitación de técnicos de diversas disciplinas, lo que ha permitido contar con sofisticados laboratorios forenses de alta complejidad.

La recolección de la evidencia es la piedra angular de la pesquisa: configura los anclajes necesarios para determinar qué sucedió y cómo y cuándo se cometió un delito. De allí, la necesidad de su correcto tratamiento y procesamiento. En esto radica la importancia del protocolo de actuación, pues, si en los primeros momentos la investigación falla, entonces la identificación del autor se convierte en una tarea titánica, prácticamente imposible. En consecuencia, el esclarecimiento de un hecho sencillo puede complejizarse enormemente sin las evidencias iniciales, ampliándose la posibilidad de cometer errores que conduzcan a su impunidad o, peor aún, a la condena de un inocente.

Esta recolección de evidencia debe cumplir con requisitos específicos tanto en la labor de campo, momento en el cual los operadores intervienen en los lugares del hecho y/o escena del crimen, y luego de enviarlos al laboratorio, los especialistas realizan las investigaciones correspondientes. En este proceso, el las muestras o evidencias deben cumplir estándares mínimos para su tratamiento.

Las pruebas recolectadas deben adquirir el carácter de confiabilidad y que haya sido obtenida de acuerdo a la normativa vigente. Para esto se debe documentar todo el procedimiento realizado, a fin de que la misma adquiera la relevancia correspondiente para la investigación, y que esta sea suficiente. Para esto, y siguiendo con el Protocolo Unificado para el levantamiento y colección de la evidencia, se deben seguir las siguientes etapas.

El correcto procesamiento de la evidencia implica una adecuada manipulación en la escena del crimen; la estandarización de criterios entre los operadores intervinientes en el campo y los del laboratorio, lo que se denomina proceso de cadena de custodia; y, finalmente, su tratamiento siguiendo los parámetros de objetividad y transparencia de acuerdo a los desarrollos más avanzados de las disciplinas correspondientes. Para ello, es necesario metodicidad científica durante todo del proceso, desde la recolección hasta la producción de la prueba pericial, garantizando el efectivo cumplimiento de los principios de identidad e inalterabilidad de la prueba.

Respecto a la prueba digital esta es definida como elementos tecnológicos que pueden poseer información almacenada en formato digital, como PC, notebook, netbook, tablets, celulares, pendrive, CD, DVD, discos rígidos, servidores, etc. Para aquellas situaciones que involucren procedimientos judiciales en empresas o instituciones de gran envergadura, a priori se procurará obtener información tendiente a conocer las características generales de la infraestructura tecnológica y hardware existente en el lugar del hecho.

Se aconseja evitar el secuestro masivo de evidencia ya que esta requiere mucho tiempo para su análisis. Los principios generales para la recolección y embalaje de las evidencias digitales halladas en la escena del crimen son:

- Registrar lo que es visible en los dispositivos de salida como pantallas e impresoras y no intentar explorar los contenidos ni recuperar información de una computadora u otro dispositivo electrónico (cámara de fotos, celular, etc.) sin contar con los conocimientos técnicos para realizarlo.
- No presionar cualquier tecla ni hacer clic del mouse.
- Verificar si existen discos o CD puestos en unidades.
- Identificar claramente qué dispositivos móviles están en uso y a quién pertenecen, dar cuenta también de los dispositivos que se encontraron apagados, guardados o en aparente desuso.
- No encenderlo si se encuentra apagado
- Dejar encendido hasta agotar batería.
- Para apagar desconectar el enchufe de la red de energía.

- No desarmar el equipo sin batería.
- No abrir la tapa de una computadora portátil si está cerrada.
- Si se realiza un cambio regístralo y justificar.

En el lugar del hecho, durante el proceso de allanamiento se debe separar a las personas que se encuentren trabajando sobre esos equipos, y no permitirles volver a utilizarlos. Se deben obtener las contraseñas cada vez que se pueda. Fotografiar los equipos informáticos antes de moverlos o desconectarlos. Levantar el material informático con guantes descartables para rescatar huellas dactilares, o ADN. Si se encuentran equipos apagados se los debe mantener así, al igual que si estos están encendidos, en este último caso se espera no perder información volátil. Identificar los aparatos conectados a la línea telefónica. Identificar correctamente todo el material tecnológico a secuestrar. Roturar hardware en computadoras (Ministerio de Justicia y Derechos Humanos, 2017).

El proceso de investigación forense informática para la adquisición de pruebas digitales, se compone de 5 fases que deben ser realizadas en forma sistemática, organizada y ordenada:

- *Adquisición*: en este momento se delimita el objeto de la investigación y se obtienen las pruebas digitales se consideren relevantes para el caso investigado.
- *Preservación*: en este momento se preservan las evidencias digitales de la investigación forense que se deberán mantener inalteradas, a fin de que pueda demostrarse que dichos elementos son idénticos a los obtenidos durante la adquisición.
- *Análisis*: en esta fase se aplican técnicas y herramientas del ámbito de la informática forense con el fin de obtener información relevante.
- *Documentación*: se procede a redactar el correspondiente informe pericial informático. Dicho informe reflejará en detalle la operación de adquisición y preservación de cada una de las evidencias digitales, así como los análisis sobre los elementos intervenidos con suficiente detalle como para poder ser replicados por un tercero en las mismas condiciones de laboratorio forense. Finalmente contendrá las conclusiones de la investigación sustentadas por argumentaciones lógicas extraídas de los resultados del análisis forense.

- *Presentación*: se procede a explicar la labor de informática forense realizada ante el tribunal que debe enjuiciar los hechos, de la forma más comprensible posible.

2.5.2 Definición de cadena de custodia en la prueba digital

Es el procedimiento "que permite de manera inequívoca conocer la identidad, integridad y autenticidad de los vestigios o indicios digitales relacionados con un acto delictivo, desde que son encontrados hasta que se aportan al proceso como pruebas" (Ministerio de Justicia y Derechos Humanos, 2017).

La finalidad de la cadena de custodia es la de garantizar la exacta identidad de lo incautado y de lo analizado. Por tanto, la cadena de custodia digital tiene un valor instrumental, ya que sirve para garantizar que lo analizado y presentado ante un tribunal como prueba es lo mismo que los indicios digitales recogidos.

La cadena de custodia digital garantiza la fiabilidad de la prueba digital que se aporta en el juicio y la adecuada defensa mediante la correspondiente pericial informática. Resulta imprescindible, dentro del procedimiento de prueba pericial informática/tecnológica, para garantizar su autenticidad e integralidad, debido a que puede ser fácilmente manipulada. Siguiendo el correcto proceso de cadena de custodia digital se consigue evitar la contaminación de los medios probatorios. Es importante que al localizar el material objeto de investigación se documente y fotografíe la obtención de la prueba digital (discos duros, dispositivos móviles, portátiles, aplicaciones, etc.).

La cadena de custodia garantiza la fiabilidad de la prueba digital que se aporta a un juicio, se debe preservar su manipulación en todo momento, garantizando la autenticidad e integralidad de las pruebas digitales.

2.5.3 Tipos de herramientas forenses y convencionales de análisis informático

El análisis forense digital es una especialidad muy importante en la Seguridad Pública, ya que se debe contar con una capacitación suficiente para adoptar las técnicas adecuadas que permitan extraer la información de los equipos.

En la actualidad existen sistemas operativos que disponen de un gran número de herramientas de informática forense que permiten el análisis de las pruebas, estas se dividen en herramientas pagas, y otras que son gratuitas. José Antonio Lorenzo (2020) publica las más destacadas que se utilizan en informática forense, las que se presentan a continuación, separando en primer lugar aquellas que son pagadas, y posteriormente las que son gratuitas:

CAINE. Se trata de un sistema operativo completo orientado específicamente a la informática forense, basado en Linux el cual incorpora una gran cantidad de herramientas. Dispone de una interfaz gráfica de usuario y su utilización es muy sencilla. Se puede usar en modo LiveCD sin ingresar en el almacenamiento del ordenador donde se desea investigar, lo que permiten mantener la información del disco duro intacta y realizar una copia de la información. Incluye las herramientas The Sleuth Kit, Autopsy, RegRipper, Wireshark, PhotoRec, Fsstat y muchas otras (Lorenzo, 2020). Este sistema dispone de herramientas que se pueden utilizar en Windows.

Kali Linux. Este sistema operativo es de los más utilizados en seguridad informática. Posee gran cantidad de herramientas forenses y dispone de un modo Live específico para análisis forense, sin modificar nada en el disco duro o almacenamiento interno de los dispositivos analizados. Impide que, cuando se introduce un dispositivo de almacenamiento extraíble, se monte automáticamente.

DEFT Linux y DEFT Zero. Estos sistemas operativos están orientados al análisis forense e incorporan la gran mayoría de herramientas de CAINE y Kali Linux. Dispone de gran cantidad de herramientas forenses listas para usar. DEFT Zero, es una versión más ligera y reducida, que requiere menos recursos y es compatible con sistemas de 32 bits y 64 bits y con sistemas UEFI.

Las herramientas gratuitas de análisis forense son:

Autopsy y The Sleuth Kit. La herramienta Autpsy es una de las más utilizadas y recomendadas. Permite localizar programas y plugins de código abierto. Esta interfaz gráfica muestra los resultados de la búsqueda forense, posee la característica de ser extensible, lo que significa que los usuarios pueden agregar nuevos complementos de manera fácil y rápida. Incorpora herramientas como PhotoRec, para recuperar archivos, permite extraer información EXIF de imágenes y videos. Por su parte The Sleuth Kit es una

colección de herramientas de comandos en línea para investigar y analizar el volumen y los sistemas de archivos utilizados en investigaciones forenses digitales.

Magnet Encrypted Disk Detector. Esta herramienta verifica de manera rápida y no intrusiva los volúmenes cifrados de un ordenador. Permite detectar discos físicos cifrados con TrueCrypt, PGP, VeraCrypt, SafeBoot, o Bitlocker de Microsoft.

Magnet RAM Capture y RAM Capture. Estas herramientas están diseñadas para obtener la memoria física del ordenador a fin de recuperar y analizar datos que se almacenan en la memoria RAM y no en un disco duro o SSD. RAM Capture permite volcar los datos de la memoria RAM de un ordenador a un disco duro, pendrive u otro dispositivo de almacenamiento extraíble.

Magnet Process Capture. Es una herramienta que permite capturar la memoria de procesos individuales de un sistema.

Magnet Web Page Saber. Permite capturar la web en un momento determinado, pero requiere conexión a internet.

FAW o Forensics Acquisition of Websites. Permite descargar páginas web completas para su posterior análisis forense, con requisitos muy básicos. Se pueden obtener pruebas de páginas web rápidamente, pudiendo capturar las imágenes o el código de fuente HTML.

SIFT o SANS Investigative Forensic Toolkit. Se trata de un conjunto completo de herramientas forenses. La versión para utilizar en máquina virtual utiliza Ubuntu LTS 16.04 en su versión de 64 bits.

Volatility. Es una aplicación forense de memoria de código abierto que da respuesta a incidentes y análisis de malware. Permite analizar el estado de tiempo en ejecución de un dispositivo mediante la lectura de la memoria RAM.

XRY FORENSIC. Este software permite rescatar los datos de teléfonos móviles de alta calidad en menos tiempo y funciona en el sistema operativo Windows. Es un método de extracción rápida para acceder y recuperar datos en vivo y del sistema de archivos desde el dispositivo directamente en la escena del crimen, comunicándose directamente con el sistema operativo del dispositivo.

AMPED FIVE. Herramienta destinada al procesamiento forense de imágenes y videos digitales, todo en una sola plataforma sin necesidad de plug-in adicionales o de terceros. Amped FIVE es reconocido a nivel mundial, y permite presentar pruebas consistentes y confiables ante tribunales (Hansgross, 2022).

BriefCam. Es una herramienta que permite la búsqueda multicámara identificando a hombres, mujeres, niños y vehículos de interés con velocidad y precisión. Utiliza filtros de reconocimiento facial, similitud de apariencia, vestimenta, color, tamaño, velocidad, ruta, dirección, tiempo de permanencia y cambio de iluminación (BriefCam, 2022).

Universal Forensic Extraction Device (UFED). Se trata de un dispositivo y un *software* fabricado por la empresa Cellebrite para ser utilizado por las policías, el cual es capaz de acceder a datos guardados en un equipo, aun cuando este tenga algún bloqueo como un PIN o contraseña. Requiere la identificación exacta del dispositivo del cual se requiere extraer la información, y posteriormente se siguen las instrucciones que entrega el software. Se pueden obtener datos como llamadas, contactos, fotos, videos, audios, datos del teléfono como el IMEI, y el número de información de geolocalización, entre otros (Cellebrite, s.f.).

I-2 IBM. Esta herramienta, utilizada para la seguridad nacional, la defensa, la prevención de amenazas empresariales ciberénticas, permite integrar datos dispares y encontrar conexiones ocultas que informen decisiones operativas eficientes y efectivas. Permite convertir datos dispares en datos inteligentes, con conocimientos prácticos en tiempo real. Facilita a los analistas e investigadores a descubrir redes, patrones y tendencias en volúmenes crecientes de datos estructurados y sin estructurar (Security M3, 2022).

Capítulo III

La investigación policial en la era de la información

Las formas como, desde el Sistema Penal se abordan los ciberdelitos se encuentra en un proceso de profundos cambios, lo cual no es ajeno a la realidad internacional. La vertiginosidad como se producen los cambios sociales en referencia a las nuevas tecnologías, es igual para la aparición de nuevos delitos, o la modificación de delitos ya existentes, en consecuencia el Derecho requiere realizar nuevos aportes a la justicia, herramientas suficientes para abordarlos. Los primeros pasos se dirigieron hacia la protección de la información y los dispositivos, posteriormente fueron apareciendo normativas jurídicas que buscaron tipificar conductas delictivas que se llevan a cabo tanto en el ciberespacio, como con la utilización del mismo. Luego, poniendo la tecnología al servicio del Derecho, comenzó a surgir la Informática Jurídica Administrativa o de Gestión, que se ocupa de compilar y organizar documentos jurídicos, y la Informática Jurídica Decisional, que busca suplantar decisiones humanas mediante el uso de programas de software.

Importantes avances en materia de incorporación de las TIC, podemos observarlos en el Derecho Informático y el Derecho de Alta Tecnología, en el cual se aplican las normas jurídicas vinculadas con la tecnología. Y es en este último donde existe un área relacionada con el Derecho Penal, que consiste en el estudio de los delitos en los cuales la informática presenta un papel condicionante como medio para la comisión de un delito. Estos son los denominados delitos informáticos o ciberdelitos.

En este capítulo nos ocupa conocer como el Sistema Penal aborda estas problemáticas y cuáles han sido las modificaciones que debieron asumir para lograr los objetivos de impartir justicia, logrando dar un resarcimiento a las víctimas.

3.1 Cibercrimen en el sistema penal argentino

La legislación de vanguardia con la que contamos en la actualidad, brinda herramientas que permiten investigar y juzgar el cibercrimen.

En nuestro país, la doctrina considera que este tipo de delito puede ser realizado internacionalmente afectando ciudadanos argentinos, ya que su comisión es transnacional, y

esto hace que su comisión a distancia desde cualquier parte del mundo; las dificultades probatorias en función de la volatilidad de los rastros del crimen; su atemporalidad, ante la posibilidad de programar su ejecución automática para determinada fecha y hora (para el caso de los virus), el anonimato que permite determinados entornos virtuales y la inadecuación legal de determinadas conductas ilícitas a las normas penales vigentes, entre otros.

Gustavo Sain (2017), sostiene que este tipo de hechos delictivos tienen una alta tasa de hechos denunciados en la justicia, pero "un porcentaje muy ínfimo tiene resolución penal en términos de identificación de los responsables" (Sain, 2017, p.2). Esto puede radicar en que los ciberdelitos se producen velozmente y se desarrollan en la gran complejidad de funcionamiento de las tecnologías modernas, lo que dificulta su descubrimiento, a lo que se suma el desconocimiento por parte de las víctimas de que están sufriendo un hecho delictivo.

Es importante destacar que los esfuerzos de cooperación internacional, dada la naturaleza transnacional del delito, han logrado fortalecer la cooperación entre países, no solo en materia de legislación penal sino también en referencia al derecho procesal, ya que gracias a esta cooperación se han podido identificar hechos delictivos. En este proceso, diferentes organismos internacionales desempeñaron un rol fundamental para la definición de figuras penales y la armonización legislativa en relación a este tipo de conductas. A raíz de esto, en Argentina se creó la Unidad 24/7, a través de la Resolución 1.291/2019, con el objetivo de servir como punto de contacto localizable respecto del Convenio sobre Ciberdelito adoptado en Budapest, para mitigar los problemas de la transnacionalidad y el aporte de información entre los países.

Desde la sanción de la Ley 26.388/2008, se incluyeron las conductas típicas asociadas al cibercrimen, como la falsificación de documentos electrónicos (art. 77 y 292 del C.P.), el ofrecimiento y distribución de pornografía infantil (art. 128 C.P.), las conductas vinculadas a la violación de secreto y privacidad (art. 153, 153 bis, 155, 157 y 157 bis del C.P.), el fraude informático (art. 173, inc. 17 del CP) entre otros.

A partir del nuevo Código Procesal Penal de la Nación de diciembre de 2014, se incorporó una nueva regulación en materia probatoria, la cual se encuentra en el Libro IV "Medios de Prueba", Título Primero "Normas Generales" del Código Procesal de la Nación, sosteniendo que:

> Podrán probarse los hechos y circunstancias de interés para la solución del caso, por cualquier medio de prueba, salvo que se encuentren expresamente prohibidos por la ley. Además de los medios de prueba establecidos en este Código, se podrán utilizar otros, siempre que no vulneren derechos o garantías constitucionales y no obstaculicen el control de la prueba por los demás intervinientes.

Debido a la intromisión de las nuevas tecnologías en la sociedad, la evidencia digital comenzó a tomar un protagonismo importante en diferentes hechos delictivos. Si bien no existe en el país una legislación que puntualice cada una de las posibles pruebas digitales que se puedan aportar, sobre todo en la búsqueda de garantizar el derecho de defensa del imputado, se hace evidente que esta prueba cada vez resulta ser más efectiva, eficaz y eficiente (Ambrosis, 2018). En este punto la doctrina considera que es fundamental contar con procedimientos preestablecidos de actuación para la obtención de estas pruebas digitales, sobre todo desde la entrada en vigencia de la Ley 26.685/2011 de Expedientes, documentos, firmas, comunicaciones, domicilios electrónicos y firmas digitales en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales.

Sostiene Mariángeles Rodríguez Rosario (2020) que el impacto que esta evidencia digital tienen en el derecho procesal penal probatorio, debe cumplir su vínculo con el instituto que la habilita, para así cumplir con el principio de libertad probatoria, incorporado en el nuevo Código Procesal Penal de la Nación, y consiste en que "en el ámbito del derecho procesal penal todo objeto de prueba puede ser probado por cualquier medio" (Rodríguez Rosario, 2020, p.13).

Las limitaciones probatorias que existen se originan "en la Constitución Nacional y los Derechos Humanos radicados en ella, en consecuencia la libertad probatoria no podrá

avalar las pruebas obtenidas en desmedro de garantías constitucionales" (Rodríguez Rosario, 2020, p.13).

Por otro lado se debe tener en cuenta el principio de *nulla coactio sine lege*. Este instituto consiste en que todos los mecanismos de investigación, procedimientos probatorios o medios de prueba que impliquen algún grado de injerencia en los derechos fundamentales reconocidos por las normas constitucionales, deben estar fundados en una ley, la cual, a su vez, no debe alterar, sustituir o modificar el principio constitucional que reglamenta. Es a raíz de este principio que Bruzzone y Bertolino (2005) establecen una diferenciación entre los medios de prueba en general (aquellos que no tienen ningún grado de injerencia en los derechos mencionados), de los medios asociados a las "medidas de coerción probatoria" donde sí se contempla la afectación a los derechos fundamentales.

Otro principio a tener en cuenta es el de derecho a la intimidad. Dado que la cantidad de datos que circulan por medios electrónicos es numeroso e importante, y se encuentra en millones de dispositivos electrónicos, se debe reflexionar sobre la intimidad de las personas, la cual muchas veces se encuentra en múltiples dispositivos.

3.1.1 Tipos de pruebas electrónicas y su validez

Dada su naturaleza completamente diferente a la prueba física, se debe realizar un análisis de las formas de producción, teniendo en cuenta su extrema volatilidad, sensibilidad e intangibilidad. La traducción de esta prueba se realiza mediante una interfaz de lenguajes como el código binario, hasta que aparece representado como texto, imagen o video. Por esto, las pruebas requieren no sólo de una recolección especial, sino también de un tratamiento pericial de preservación, conservación y protección de la cadena de custodia tratada en el capítulo anterior.

La justicia argentina admite como pruebas a:

- El correo electrónico
- La imagen digital
- Evidencia guardada en la nube.
- Celulares y smartphones
- Redes sociales

- Computadoras: PC, Notebook y Netbook.
- Tablets

La ley N° 27.063 del nuevo CPPN incorpora dos artículos, el Art. 143 en donde especifica o habilita la intercepción y secuestro de correspondencia o cualquier medio de comunicación electrónica. En sintonía tenemos el Art. 144 que establece la incautación de datos de un sistema informático o de una parte de éste, o de un medio de almacenamiento de datos informáticos o electrónicos, con el objeto de secuestrar los componentes del sistema, obtener copia o preservar datos o elementos de interés para la investigación (Bruzzone y Bertolino 2015).

En la provincia de Mendoza, a partir de la Ley 6.730/1999 del Código Procesal Penal de Mendoza, se incorporaron herramientas procesales para la obtención de evidencia digital.

3.2 La prueba digital en el proceso penal en Mendoza

Nuestro Código Procesal Penal no ha incorporado aún, herramientas procesales para la evidencia digital. En referencia a este punto, el fiscal Santiago Garay, ha realizado una propuesta de ley destinada a la modificación de dicho Código, en materia de cibercriminalidad y obtención de evidencia digital.

En base a la aprobación de la Convención de Budapest sobre el ciberdelito por nuestro país en el año 2017, entendiendo que se requiere aplicar una política penal común a nivel internacional con el objeto de proteger a la sociedad de la ciberdelincuencia, el autor considera necesario que dicha normativa legal se encuentre en nuestro procesamiento penal mendocino.

Dado que en nuestro país ya la normativa legal ha ido incorporando delitos vinculados a la cibercriminalidad informática, como la Ley 26.388 de Delitos Informáticos, tipificando la ciberpornografía infantil, la violación, el apoderamiento y desvío de comunicaciones electrónicas, la interceptación o captación de las mismas, el acceso indebido a un sistema o dato informático, la publicación indebida de una comunicación electrónica, la revelación de datos que por ley deben ser secretos, el acceso indebido a un banco de datos personales, la inserción de datos falsos en un archivo de datos personales,

las defraudaciones por el uso ilícito de tarjeta de crédito o débito, la defraudación informática, el daño informático. Luego se incorporaría la Ley N° 26.904 de Grooming, y por último la Ley 27.436 que penaliza la tenencia de pornografía infantil.

En referencia a las pruebas, el Código Procesal Penal de Mendoza tiene reglas relativas a medidas de prueba tales como el registro, el allanamiento, el secuestro, la requisa personal y la interceptación de comunicaciones; la aplicación de las mismas a la evidencia digital no es posible, pues el desafío que plantea su tratamiento, requiere de medidas de prueba específicas, o la adaptación legal de las ya existentes.

El principio de libertad probatoria, debe ser interpretado a la luz de la máxima *nulla coactio sin lege*, que tiene recepción en nuestro ordenamiento procesal en el que se existe interpretar restrictivamente las disposiciones legales que coarten la libertad personal, o limiten el ejercicio de un derecho conferido a los sujetos del proceso y prohíbe la interpretación extensiva y la analogía mientras no favorezcan la libertad del imputado ni el ejercicio de una facultad conferida a quienes intervienen en el procedimiento.

Se pone en evidencia que no existen estándares generalizados de judicialidad, motivación, proporcionalidad y legalidad al momento de recabar, tratar y valorar la prueba digital. Hay que tener en cuenta que hoy, ingresar en un dispositivo tecnológico es mucho más invasivo que allanar un domicilio, en consecuencia se deben respetar los derechos de intimidad y privacidad los que pueden ser vulnerados. Por estos motivos es indispensable que la ley expresamente, prevea una medida para su ejecución. Buscando amparar derechos y garantías de las personas ante el poder coercitivo del Estado, se requiere asegurar un procedimiento transparente y válido reformulando artículos que consagran medidas probatorias que suponen una injerencia en la vida privada de las personas.

Garay propone incorporar artículos que refieren al registro de dispositivos tecnológicos que contengan evidencia digital, ya sea este físico o remoto. Por otro lado, propone establecer la posibilidad de confiscar datos informáticos almacenados, incorporar los nombres de usuarios y contraseñas necesarios para entrar a un sistema informático; otras medidas aplicables al tratamiento de la evidencia digital; solicitar la conservación rápida de datos informáticos a proveedores de servicio para que no sean alterados en el

transcurso de la investigación entre otras modificaciones que protegerán no solo los datos, sino también el procesamiento de los mismos. Este proyecto de ley fue presentado en el año 2021 y aún se encuentra a la espera de aprobación (Expte. Nro. 0000072000).

Gastón Bielli (2019), en referencia a la prueba electrónica y la utilización de capturas de pantalla en Derecho de Familia y Derecho Penal, entiende que

> "…debemos partir de la existencia de un novedoso escenario, caracterizado por el exponencial e ininterrumpido crecimiento de las fuentes probatorias de naturaleza digital, producto de la acelerada evolución tecnológica y la utilización masiva de los instrumentos electrónicos o digitales en todos los sectores de la vida social. Nos encontramos con nuevos instrumentos informáticos, multimedia y/o de comunicaciones, así como con novedosos formatos y soportes: teléfonos móviles, smartphones (Iphones, Androids y otros teléfonos inteligentes), tabletas, ordenadores, dispositivos USB, ZIP, CD-Rom, DVD, reproductores de MP3 o MP4, servidores de información, PDAs, navegadores, pantallas táctiles en automóviles...; sin olvidar el relevante ámbito del cloud computing" (p.4) (Bielli, 2019)

Al respecto, la doctrina ha sostenido que esta incorporación de la comunicación electrónica, se ha convertido en una temática de gran interés para las partes que requieren producir pruebas, a fin de fundamentar sus peticiones. Lo distintivo de la prueba electrónica es que está esencialmente vinculada a hechos o actos jurídicos ocurridos en o realizados a través de medios informáticos. Es decir, resulta determinante que los hechos asuman una configuración informática.

Los sistemas de mensajería instantánea como WhatsApp, o Messenger o Instagram Direct (mensajería de Instagram), Telegram, entre otras, han resultado un método probatorio por excelencia para acreditar diversos hechos. Por esta razón, los diálogos, audios, imágenes o videos que se comparten en tales conversaciones se han convertido en una importante fuente de prueba que puede ser incorporada en cualquier juicio.

De esta forma podemos observar cómo, tanto en la justicia federal como en los fueros provinciales, las pruebas digitales se constituyen en valiosas herramientas para la probatoria de hechos delictivos.

Frente al incremento de producción probatoria digital, a nivel nacional y provincial, existen áreas de apoyo técnico judicial que se describen en los siguientes apartados.

3.3 Unidad Fiscal Especializada en Ciberdelincuencia (UFECI) del Poder Judicial

Creada a través de la Resolución PGN N° 3743/15, su objetivo es el de robustecer la capacidad del organismo en materia de detección, persecución y represión de la criminalidad organizada y de los delitos que más menoscaban la seguridad ciudadana (UFECI, s.f.).

Esta unidad se ocupa de los delitos constituidos por ataques a sistemas informáticos, o cuando el medio comisivo principal o accesorio de una conducta delictiva, incluye la utilización de cualquier tipo de sistema informático. Prestan especial atención al crimen organizado y aquellos en los que sea necesario realizar investigaciones en entornos digitales, aun cuando no hayan sido cometidos contra o mediante un sistema informático.

Esta unidad interviene en aquellos casos que resulten competentes por su vinculación con la cibercriminalidad, mediante la recepción de denuncias o la realización de investigaciones preliminares, actúan como nexo entre los diferentes actores e instituciones que pueden tener alguna incidencia en cuestiones vinculadas con la temática.

Esta unidad realiza investigaciones en cibercriminalidad en las que se vuelcan datos estadísticos anuales, además de contar con links de interés para el público en general, que les permite acceder a datos confiables para verificar correos o páginas web.

Realiza acciones de prevención que incluye la difusión de herramientas y consejos para no ser víctima de engaños, maltratos, extorsión, invasión a la privacidad u otros riesgos a los que se exponen diariamente las personas que utilizan tecnologías.

3.4 Unidad Fiscal especializada en delitos informáticos de Mendoza

Desde el año 2019, mediante la resolución de la Procuración General de la Suprema Corte de Justicia del Poder Judicial Mendoza, se amplió la Unidad Fiscal de Delitos Económicos a la materia de Delitos Informáticos, diferenciándola de los Delitos económicos y buscando que cuente con profesionales especializados en la materia.

En esta unidad se pueden realizar denuncias, con un procedimiento igual al de cualquier otro delito, e incluso la denuncia se puede hacer mediante un medio digital, ya

sea a través de la página web del Ministerio Público Fiscal, como también a través de la aplicación para celulares.

El punto central de esta distinción es tomar un criterio a través del cual se defina lo particular de cada hecho, tomando criterios propios y basados en conocimientos suficientes sobre la temática. A tal fin la Procuración General (2021) ha resuelto que los casos que corresponden a esta unidad

> "…cuando esté implicado un delito que se ejecute a través de una computadora, sistemas informáticos u otros dispositivos electrónicos de comunicación que tengan por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos"

La Unidad Fiscal de Delitos Informáticos se encuentra integrada por dos Fiscalías de Instrucción con funcionamiento en turnos matutino y vespertino que comenzó a funcionar desde el día 2 de agosto de 2021.

Desde el Poder Judicial de Mendoza, a través de su Departamento de Aula Virtual (2021), se realizan capacitaciones en Informática. Los objetivos de estas capacitaciones son:

- "Brindar, a la mayor cantidad posible de agentes judiciales de cualquier categoría escalafonaria, acceso a diferentes niveles de conocimientos informáticos.
- Dar a conocer la Informática como recurso e instrumento para el proceso de enseñanza-aprendizaje, integrando la computadora como medio fundamental.
- Valorar la importancia de la alfabetización informática en las actividades cotidianas, tanto personal como laboral
- Identificar las posibilidades de aplicación de las nuevas tecnologías en el ámbito laboral judicial y sus ventajas.
- Conocer los alcances y funciones de los recursos que nos aportan las herramientas de la Web 2.0 para la tarea judicial" (p.1).

Estas capacitaciones son semestrales y están destinadas a personal de diferentes áreas gubernamentales.

Otra de las actividades que desarrolla el Poder Judicial de Mendoza es su búsqueda por la digitalización en sus actividades cotidianas, buscando la despapelización, y experimentando con Inteligencia Artificial (IA) y datos abiertos. Luego de la aparición de

la pandemia de Covid-19, y gracias a los grandes cambios que se produjeron en el año 2020, se está buscando una eliminación casi total del papel, además de la creación de un portal ciudadano de datos más accesible que le aporte una mayor transparencia a las acciones judiciales. Se ha creado el teléfono de Justicia N° 160, para la gestión de turnos y denuncias penales, "se han establecido convenios con Amazon para tener datos abiertos y hasta pruebas con Inteligencia Artificial para automatizar acuerdos en algunos foros" (SIJUM, 2021, p. 1).

En relación a la aplicación de IA se realizan pruebas piloto en procesos judiciales del fuero tributario y laboral, con el sistema argentino Prometea, siendo Mendoza la ciudad que cuenta con el primer equipo en el interior del país.

Desde el año 2019, ENACOM ha autorizado la utilización del número único de Justicia 160, el que ha posibilitado la gestión más fluida de trámites de los ciudadanos con el Poder Judicial, en lo referente a turnos de defensores civiles y familia, la realización de denuncias en el fuero penal, mediante comunicación con el Ministerio Público, la posibilidad de acceder a algunas causas, entre otras medidas.

Esta incorporación de avanzada en referencia a la tecnología representa un ahorro económico significativo aproximadamente del 60% (SIJUM, 2021)

3.5 Unidad 24/7 de Delitos Informáticos y Evidencia Digital

Creada por la Resolución 1.291/2019, a fin de servir como punto de contacto localizable respecto del Convenio sobre el Ciberdelito adoptado en Budapest. La finalidad de esta Unidad es la de asegurar la asistencia inmediata en la investigación de infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recolección de pruebas electrónicas de una infracción penal.

Las acciones de asistencia que realiza la Unidad 24/7 facilitan la aplicación de las siguientes medidas:

- Aportar consejos técnicos:
- Conservar datos según lo dispuesto en los art. 29 y 30 del Convenio;

- Recolectar pruebas, aportando información de carácter jurídico y localización de sospechosos.
- Facilitar la recolección de pruebas informáticas.
- Colaborar en los efectos transfronterizos que se generan por la ocurrencia de delitos relacionados con la tecnología y la volatilidad e intangibilidad de la evidencia digital.
- Prestar asesoramiento y asistencia técnica en las investigaciones penales en las que los Estados Parte del Convenio, requieran colaboración.
- Asistir a funcionarios del sistema penal del país, tanto a nivel federal como provincial.
- Proveer y requerir a las contrapartes extranjeras, asistencia internacional idónea durante el proceso de investigación inicial, buscando preservar la evidencia digital relevante, de modo que esta se encuentre disponible en un momento posterior de tiempo cuando sea requerida, mediante los canales de cooperación internacional vigente.
- Se debe tener en cuenta que esta oficina debe trabajar rápidamente, "a velocidades sin precedentes para preservar los datos electrónicos y localizar a los sospechosos" (Res. 1.291/2019), para lo que podrá solicitar a los proveedores de servicios de internet, ubicados en diferentes jurisdicciones, su colaboración para la preservación de los datos.

Conforma un punto focal, para que sea un interlocutor válido ante los diferentes países adheridos, cuando se detecte una infracción penal por los diferentes medios electrónicos, con la finalidad de actuar en forma inmediata.

Esta Unidad, funciona en la órbita de la Dirección Nacional de Asuntos Internacionales, dependiente de la Unidad de Coordinación General del Ministerio de Justicia y Derechos Humanos, y su actuación es en conjunto con el Ministerio de Relaciones Exteriores y Culto, como órgano central de cooperación internacional.

3.6 Proceso de investigación de cibercrimen

La planificación de la investigación cibercriminal comienza con una denuncia realizada por un particular afectado por la conducta delictiva, o por solicitud del juzgado. Frente a esto, numerosos son los datos que se deben obtener y, a su vez, de numerosas fuentes sobre todo cuando estas han intentado ser borradas. Por otro lado se debe tener en cuenta el carácter internacional que adquieren estos delitos, ya que si los mismos son perpetrados por ejemplo, en redes sociales o en los servicios de mensajería, se debe solicitar la información internacional.

El anonimato que ofrece Internet y la posibilidad de ejecución de conductas dañosas a distancia dificultan la detección de los posibles delitos. Tampoco es fácil delimitar quien es el autor de dichas conductas. Por eso para investigar una comunicación delictiva realizada a través de las TIC lo que hay que determinar los datos de tráfico y los rastros de navegación, ya que son los que aportarán la información fundamental sobre el origen de las comunicaciones y los caminos que estas han recorrido. Para esto, se obtiene de los proveedores de servicio de internet los siguientes datos:

- Dirección de IP asignada al sospechoso por el proveedor y los datos contractuales (nombre, dirección) junto con otros datos como fechas, horas, duración de las comunicaciones, etc.
- Localización geográfica desde la que se conecta el sospechoso.
- Cuentas asociadas al pago de servicios.
- Número de teléfono de origen y destino de las comunicaciones.
- La comunicación completa, o la transacción que se haya realizado.
- La copia de archivos que tuviere el sospechoso en la nube.
- Identificación de los equipos de telefonía celular.
- Recuperación de mensajes.
- Recuperación de registro de GPS, si se requiere.
- Y, en general todos los datos que puedan resultar de utilidad para el esclarecimiento del ilícito.

3.6.1 Fases de la investigación

En general estas fases suelen desarrollarse en tres etapas:

Fase previa: permite identificar que ha sucedido y esto brindará el punto de partida para realizar la investigación.

Fase de investigación propiamente dicha: en este momento se identifica quien pudo ser el posible responsable y si ha perpetrado alguna acción punible. O si la utilización de las herramientas tecnológicas ha posibilitado o contribuido con los hechos delictivos.

Fase incriminatoria: en este momento se obtienen y aseguran las pruebas delictivas (Rayón Ballesteros, 2020).

El análisis pericial se realiza sobre los datos obtenidos y tienen por finalidad:

Localizar e identificar las evidencias electrónicas para constituir la prueba indiciaria.

Localizar e identifica las evidencias que permitan vincular el equipo, el usuario, el abonado y los datos.

Estos análisis se realizan de acuerdo a los recursos de cada institución de seguridad en forma diferenciada, en función además, de los conocimientos tecnológicos y la selección de las herramientas que se consideren más adecuadas.

El análisis que se realiza no siempre es concluyente, ya que los indicios que pueden surgir de manera separada, pueden no significar nada, pero en su conjunto pueden constituir la prueba para el juicio.

Una vez obtenidas y analizadas las pruebas se elabora un informe técnico de naturaleza policial para entregar a la fiscalía según corresponda, en el cual deben figurar todas las operaciones practicadas detalladamente a fin de evitar interpretaciones erróneas.

En el siguiente capítulo, desarrollaremos nuestro trabajo de campo exponiendo cuales son las acciones en concreto, que se llevan a cabo en la Policía de Mendoza para la obtención de pruebas digitales, ya sea que estas resulten de utilidad para esclarecer delitos

digitales, o también para esclarecer delitos de otra índole en los que los medios digitales, sirvan como prueba.

Capítulo IV

Trabajo de campo

“El Sistema de adquisición de comunicación electrónica del departamento de Asistencia Tecnológica y Apoyo Investigativo de la Dirección de Investigaciones de la Policía de Mendoza. Preservación y análisis de datos de mensajería digital, protocolo de identificación, resguardo y presentación de informes analíticos, durante el período del 2019 al 2021”

4.1 Entrada en contexto

La presente investigación parte de analizar la utilización de las TICs para la comisión de hechos delictivos, y la obtención de la prueba para su comprobación. Desde la cibercriminología hemos coincidido en la concepción de cibercrimen, la cual es adecuada para nuestra investigación, ya que en ella se pueden abarcar los ciberataques como puros, réplica o de contenido, sean estos económicos, sociales o políticos, dado que todos ellos requieren de la existencia de un ciberespacio para llevarlos a cabo.

En la sociedad de la información, en la que nos encontramos inmersos, Argentina y Mendoza, no están exentas de la utilización del ciberespacio para la ocurrencia de este tipo de delitos, los cuales ocurren con la particularidad que el contexto de la provincia, puede brindar.

En el ámbito de las redes sociales como Facebook, podemos encontrarnos con delitos contra la privacidad, o económicos como la estafa o los robos, el acoso o las calumnias e injurias. De igual manera funciona Instagram, aunque en menor medida. Por otro lado, los mensajes privados en estas redes, o los mensajes enviados pro WhatsApp o Telegram o SMS, son también importantes de destacarlos pues en ellos observamos amenazas, robo de archivos multimedia, o incluso, robo de identidad.

Otros delitos, como robos, asaltos u homicidios, pueden ser detectados mediante la utilización de los dispositivos de seguridad vigentes en la provincia de Mendoza, como las cámaras de vigilancia, o el análisis de llamadas, mensajería de WhatsApp, Telegram o SMS, o también mensajería privada de redes sociales.

Estas intervenciones, de alta especificidad que requieren recabar información fehaciente para la comprobación de hechos delictivos, se llevan a cabo, en la provincia de Mendoza, por el Departamento de Asistencia Tecnológica y Apoyo Investigativo (DATAI), el cual es el encargado de recabar las pruebas necesarias desde diferentes dispositivos tecnológicos.

4.1.1 Departamento de Asistencia Tecnológica y Apoyo Investigativo DATAI

Este organismo depende del subjefe de Policía en Función Judicial, cuya función es la de coordinar y controlar funcionalmente, las actividades operativas y administrativas

llevadas a cabo por las Divisiones Análisis Criminal, Delitos Tecnológicos y Escuchas Telefónicas y Antisecuestros.

Su tarea requiere de una actuación mancomunada en aquellos delitos que involucren alguna de las Divisiones mencionadas y que, en el marco de las investigaciones sean requeridos.

Por otro lado, tiene a su cargo, todo tipo de coordinación con las autoridades del Poder Judicial y Ministerio Público Fiscal a fin de implementar y/o mejorar los distintos procedimientos que involucren tanto a dependencias judiciales como de la Dirección Investigaciones. Debe mantener informado, en forma permanente, a la Jefatura de Policía en Función Judicial sobre el avance de las intervenciones en que se vean involucradas las Divisiones a su mando. Además, debe gestionar los recursos necesarios, en función de los avances tecnológicos, ante la Dirección correspondiente y las autoridades ministeriales que correspondan y coordinar intercambios con otras instituciones externas que sirvan de apoyo a la investigación criminal, en función de lo establecido por el Convenio de Budapest (Anexo I, página 135).

Del DATAI dependen otras instituciones que se describen a continuación.

4.1.1.1 División Análisis Criminal

La jefatura de esta división es desempeñada por un Oficial Jefe P.P, en servicio efectivo, de las Policías de la Provincia de Mendoza.

La función específica de la Jefatura de la División Análisis Criminal es la de dirigir, coordinar y controlar las actividades de reunión y análisis de información correspondiente al ámbito delictivo. Esta División mantiene una guardia cuya función es la de recabar toda la información registrada al nivel de la Policía en Función Judicial, tanto de hechos delictuales, medidas investigativas desarrolladas e identificación de personas a través de los programas existentes, información que una vez reunida es transmitida a conocimiento de la Superioridad y de demás unidades especializadas.

En esta División se mantiene la actualización constante de todas las bases de datos, con la finalidad de producir la inteligencia adecuada para realizar una persecución del

delito, determinar nuevos *modus operandis* delictuales, contrarrestando la ejecución de acciones delictivas, debiendo efectuar su difusión a los organismos pertinentes.

Bajo su directa dependencia, estarán la sistematización de datos e información territorial, que consiste en la actualización diaria y permanente de los registros y verificación de detenidos que sean identificados por la División Judiciales, manteniendo la permanente actualización de las bases desarrolladas. En tanto que el Centro Integrador de Análisis Tecnológico CIAT tiene como función, la visualización y análisis de cámaras del CEO, el desarrollo de pericias producto de la extracción de información de dispositivos tecnológicos, todo ello en apoyo de las unidades especiales que dirigen la investigación. Se realiza además el monitoreo de redes sociales y sistemas de comunicación con la finalidad de advertir la comisión de hechos delictivos (Anexo II, página 135).

4.1.1.2 División Delitos Tecnológicos

La Jefatura de la División Delitos Tecnológicos es desempeñada por un Oficial Jefe P.P. en servicio efectivo de las Policías de la Provincia de Mendoza.

La función específica de la División Delitos Tecnológicos será la intervención investigativa con realización de pericias en sistemas informáticos o electrónicos y el análisis de pruebas obtenidas en hechos delictivos. Efectuará la elaboración de fotogramas y todo lo relacionado a grabaciones en video.

Asimismo, el mantenimiento de las bases de datos propias de la Jefatura de Policía en función Judicial TESSA y otras.

Se ocupa de la extracción de información de dispositivos informáticos y tecnológicos y el posterior análisis del resultado obtenido. Tareas que se hacen en apoyo de las unidades especiales que dirigen la investigación e investigaciones propias respecto de delitos tecnológicos (*grooming*, pornografía infantil). Por otro lado se realiza la adquisición, y preservación de evidencia digital de dispositivos electrónicos, con relevamientos en las zonas del hecho.

La oficina de observaciones tecnológicas, dependiente de esta División, se ocupa de la adquisición de información de dispositivos electrónicos mediante herramienta UFED. (Anexo II, página 135).

4.1.1.3 División escuchas telefónicas y antisecuestros

La Jefatura de la División Escuchas Telefónicas y Antisecuestros, es desempeñada por un Oficial Jefe P.P. en servicio efectivo de las Policías de la Provincia de Mendoza.

La función específica de esta División Escuchas Telefónicas y Antisecuestros, será la gestión de oficios judiciales, relacionados a intervenciones telefónicas, escuchas telefónicas, transcripción mecanográfica, confección de master (comunicaciones de interés), escuchas directas en tiempo real, análisis de planillas de registro de comunicación a través de software adaptado, análisis de información, trascripciones de audio vinculados a expedientes investigados.

Para el desarrollo de estas actividades podrán:

- Utilizar software que permitan la comparación forense de voces.
- Participar, tanto operativa como administrativamente, en forma directa e inmediata, en aquellos delitos en que se registre la privación ilegítima de la libertad de una persona con fines extorsivos, quedando a disposición del Juzgado Federal interviniente y para lo cual coordinará con la Autoridad Judicial y policial los pasos a seguir en forma inmediata (Anexo II, página 135).

4.2 Desarrollo metodológico

Metodológicamente, esta es una investigación decampo, con un diseño cualitativo y, por lo tanto, flexible ya que combina diferentes técnicas. El alcance es descriptivo, dado que busca dar cuenta de las formas como se obtienen los ciberdatos que permiten esclarecer diferentes hechos delictivos, cuál es su procesamiento y cuidado y, sobre todo, la utilidad que estos presentan para la justicia. Los estudios de alcance descriptivos buscan describir, como lo dice su nombre, este tipo de pruebas.

Los estudios descriptivos permiten identificar propiedades y características de los grupos de personas y/o fenómenos estudiados, que son sometidos al análisis del

investigador, como bien menciona Hernández Sampieri (2014). Siguiendo a Montbrún Ruggiero (2013), las investigaciones de alcance descriptivo tienen como objetivo, dar cuenta de eventos o circunstancias que corresponden a un mismo tipo de fenómenos, mediante procedimientos metódicos que muestren el objeto de análisis proveyendo una enrome cantidad de material que posibilita el acopio de datos.

Para su desarrollo nos hemos valido de estadísticas de intervenciones que se han realizado mediante la utilización de tecnología como cámaras de seguridad, investigación en dispositivos electrónicos y casos relevantes que puedan dar cuenta de los procedimientos. Se incluyen entrevistas realizadas a fiscales de la provincia de Mendoza.

Para la presente investigación partimos de la siguiente hipótesis:

- La falta de un protocolo de recolección de evidencia digital establecido normativamente en la Provincia de Mendoza, provoca dificultades en la elaboración de informes técnicos presentados por el Departamento de Asistencia Tecnológica y Apoyo Investigativo, en causas penales ante el Poder Judicial, en los años 2019 al 2021.
- El aumento de la obtención de datos en dispositivos electrónicos, acrecienta la complejidad y calidad de la presentación de informes técnicos por parte del Departamento de Asistencia Tecnológica y Apoyo Investigativo perteneciente a la Dirección de Investigaciones, por lo tanto, es necesario cumplir con los procedimientos adecuados para la obtención y preservación de las pruebas, a fin de que las mismas, puedan ser utilizadas como

4.2.1 Fuentes de información

Son aquellas de donde se extrae la información para luego someterla a un análisis que nos permita obtener los datos necesarios para su estudio interpretacional. Estos, se componen de los aportes de intervenciones y el conocimiento de profesionales que desarrollan sus actividades en la problemática.

4.2.1.1 Fuentes secundarias

Tomamos como fuentes de información secundaria, los datos estadísticos provenientes de la Asociación Argentina de Lucha Contra el Cibercrimen (AALCC),

correspondientes al año 2021, y dos casos en los que el DATAI ha intervenido para la obtención de pruebas que permitieron su esclarecimiento.

4.2.1.2 Fuentes primarias

Como fuentes de información primaria se realizaron entrevistas a personal del DATAI.

4.2.2 Técnicas de recolección de información y análisis de datos

4.2.2.1 Técnica documental

Esta técnica consiste en la identificación, recolección y análisis de documentos que nos permiten presentar la actuación de un caso particular, a fin de poner de manifiesto la actuación policial en un caso particular.

4.2.2.1.1. Caso femicidio en Mendoza

En el presente caso de feimicidio, se preservó el nombre de la víctima como también el lugar del hecho y demás datos que puedan dar cuenta del mismo, dado que se trata de una menor.

En el mes de diciembre del año 2020, ingresa una llamada al servicio de emergencias 911, del CEO de Mendoza, en la cual una persona informa que escuchaba gritos de auxilio en la casa de sus vecinos, en la cual convivía una pareja de 33 y 27 años. El vecino denuncia que hay un caso de violencia de género en un domicilio ubicado en un pasaje, brindando incluso el número de la calle. Es importante destacar este detalle, puesto que el domicilio no se encontraba en una calle, sino en un pasaje. Cuatro días después, el cadáver de la chica de 14 años, fue encontrado en el mismo departamento, por el personal de la Policía Científica y de la Unidad Fiscal de Homicidios, envuelto en mantas y parcialmente calcinado, marcado por golpes, con un pronunciado corte en el cuello.

En este caso, la investigación realizada por el DATAI, fue fundamental. La siguiente secuencia de acciones llevadas a cabo por la División, dan muestra del rol desempeñado:

- En primer lugar, el personal elaboró un análisis de las llamadas al CEO.

- Posteriormente, personal de la División de Delitos Tecnológicos, realizó el correspondiente relevamiento, preservación, resguardo, análisis y presentación del material fílmico correspondiente a la zona de actuación.
- Este análisis les permitió elaborar los respectivos informes georeferenciales, con la finalidad de precisar la ubicación en la zona, tanto de la víctima, como del imputado.
- Por otro lado, indagaron sobre los datos obtenidos respecto al dominio de los vehículos que hubieran intervenido en el hecho. A la vez, realizaron las georeferenciaciones correspondientes a los datos obtenidos de las cámaras y pórticos.
- El personal que elabora los análisis correspondientes, mediante la utilización de la herramienta I2, procedió a la elaboración de un mapa interactivo, en el que se reflejaron las llamadas ocurridas desde las terminales del imputado y la víctima. Esta tarea fue realizada por el personal de la División de Escuchas Telefónicas
- En referencia al material procedente de la tarjeta RED BUS, el personal procedió a su adquisición y resguardo, lo que les permitió observar los datos de su utilización en las líneas de colectivo que unían la vivienda de la víctima con la del imputado.
- Este último dato, les facilitó al personal de Delitos Tecnológicos, analizar imágenes de cámaras de seguridad, de las paradas de colectivo cercanas a la vivienda del imputado, y así poder obtener datos en los que pudieron observar a ambos caminando por la zona, en dirección a la casa del imputado.
- En última instancia, el personal obtuvo datos procedentes de las redes sociales de la víctima, los cuales luego de cumplir con su correspondiente preservación, fueron analizados. Este análisis permitió que el personal de Delitos Tecnológicos, obtuviera las conversaciones entre la víctima y el victimario, en las cuales descubrieron que este último, acosaba a la menor, como también a otras menores.

La investigación llevada a cabo por los diferentes analistas del DATAI que desarrollan sus tareas en las áreas de dicho departamento, una vez unidas en su conjunto, permitió que descubrieran que además, el imputado, mantenía chats en las aplicaciones de Facebook e Instagram, con otras adolescentes, llegando incluso a acechar a la víctima, varias semanas antes del hecho.

Los análisis realizados, les permitieron inferir a los pesquisas, que el femidica, a través de estos chat, invitó a la víctima a su propiedad, hacia donde se dirigió la menor, quien salió de su casa mintiendo a sus padres, informándoles que se iría a visitar a una amiga. Fue a través, del análisis de imágenes provenientes de cámaras de seguridad, sumado al análisis del recorrido de la tarjeta Red Bus de la menor y las imágenes de la cámara de seguridad del colectivo, que el personal del DATAI, pudo determinar que la menor había descendido del colectivo el sábado al mediodía, e inmediatamente se había encontrado con el femicida, en las inmediaciones de la vivienda de este último. El imputado, fue a buscarla, y juntos se dirigieron a su vivienda, lo que ha quedado registrado en imágenes de cámaras de seguridad, pero además, estos datos fueron informados a la policía, por algunos vecinos que pudieron verlos. Por otro lado, el equipo de analistas, cuando observó las redes sociales de la víctima, identificaron que la misma había publicado un estado de WhatsApp en el que afirmaba estar “con el tío más piola”, durante el transcurso de ese día. En este análisis, los forenses analíticos, pudieron observar también, un chat que la víctima mantuvo con su amiga, 40 minutos antes de que la mataran.

Por otra parte, alrededor de las 18:58h., un vecino escuchó una voz pidiendo auxilio, proveniente de la casa del imputado. En ese momento, realizó la llamada al 911 donde nunca obtuvo respuesta.

El femicida, degolló a la menor quemando su cuerpo en un pozo séptico, quizás pensando en desaparecerlo en el lugar, buscando borrar evidencias. Como no pudo terminar su objetivo, llamó a un amigo pidiéndole que lo llevara en un vehículo a tirar un perro que, supuestamente, había atropellado un auto, arrojando el cuerpo de la menor, en una acequia de una zona semi urbana.

El caso, que generó grandes movilizaciones en la provincia, que incluyeron incidentes en marchas por pedido de justicia, que se realizaron en la zona céntrica, las cuales llegaron incluso a quemar partes de la Casa de Gobierno y la Legislatura provincial, no podría haber sido resuelto, sin la intervención del personal del DATAI, mediante la recuperación de pruebas cibernéticas, como imágenes de cámaras de seguridad; la recuperación de datos de una tarjeta de viajes; la recuperación de datos de redes sociales de la víctima, su resguardo correspondiente, y el análisis profundo realizado por los especialistas en informática.

El día 8 de julio de 2021, se realizó el juicio abreviado solicitado por el imputado quien fue sentenciado a prisión perpetua. En el mismo se ofrecieron las pruebas digitalizadas que permitieron el esclarecimiento del hecho en 6 días. (Anexo II pág. 138)

4.2.2.1.2 Análisis e interpretación de resultados.

Como se ha podido observar, el caso de femicidio citado pudo ser resuelto en 6 días a partir de realizar un análisis informático correspondiente. Los datos obtenidos permitieron determinar los pasos que la menor había realizado el día que salió de su casa, además de imágenes obtenidas de diferentes cámaras en las que se pudo observar el femicida en diferentes lugares cercanos a su casa.

La recolección de datos de los dispositivos telefónicos, así como el acceso a redes sociales, permitió identificar el acoso generado por el femicida, y la forma como atrajo a la menor a su domicilio.

Por otro lado, el análisis de los datos del CEO, permitió identificar la llamada realizada por el vecino y la respuesta desde la institución.

4.2.3 Fuentes primarias

Las fuentes primarias provienen de entrevistas realizadas a referentes del Departamento de Análisis Tecnológico y Apoyo Investigativo

La población de estudio se compone de:

- Profesionales que desarrollan actividades en diferentes áreas de tecnología
- Profesionales que recaban información digital

- Profesionales que analizan información digital

Se realizó una muestra teórica voluntaria, e intencional, que corresponde a 3 efectivos policiales que realizan sus funciones en el DATAI. Se aplicó una guía de entrevista cuyo objeto de estudio consistió en indagar sobre las siguientes categorías de análisis.

4.2.3.1 Categorías de análisis

- *Antigüedad en la dependencia*: en esta categoría buscamos conocer el tiempo que el entrevistado lleva trabajando en la dependencia.
- *Capacitación y conocimientos*: la tarea de idóneo o perito informático requiere de la adquisición de un conjunto de conocimientos específicos. En esta categoría buscamos identificar los mismos.
- *Herramientas más utilizadas*: se busca identificar las herramientas que se utilizan en las diferentes áreas, para la obtención de pruebas.
- *Prueba digital*: es "toda información digital empelada por las partes para afirmar la realidad de un hecho durante el proceso judicial" (Rivolta, 2012). Para que esta prueba sea validad, la información debe haber sido producida, almacenada o transmitida por medios digitales (por ejemplo por un correo electrónico, conversaciones de WhatsApp, entre otras). Deber ser, además, capaz de acreditar los hechos.
- *Obtención de pruebas*: esta categoría busca identificar cuáles son los principales dispositivos de los cuales se pueden obtener pruebas, incluyendo redes sociales o georeferenciación.
- *Relación entre áreas*: la vinculación entre áreas permite la organización del trabajo para la obtención de pruebas, su preservación y posterior utilidad para la justicia.
- *Relación con el Poder Judicial*: en esta categoría buscamos conocer cómo es esta relación, la cual presenta características que le son propias, dado que, como sostiene la Procuración General (2021), se requiere la participación de especialistas "…cuando esté implicado un delito que se ejecute a través de una computadora, sistemas informáticos u otros dispositivos electrónicos de comunicación que tengan por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos". Además, el Poder Judicial, solicita intervenciones del DATAI

cuando, para el esclarecimiento de un hecho delictivo, se puede contar con datos provenientes de dispositivos electrónicos.

- *Cadena de custodia de la prueba digital:* Es el procedimiento "que permite de manera inequívoca conocer la identidad, integridad y autenticidad de los vestigios o indicios digitales relacionados con un acto delictivo, desde que son encontrados hasta que se aportan al proceso como pruebas" (Ministerio de Justicia y Derechos Humanos, 2017).
- *Función del perito informático y del idóneo informático*: esta categoría pretende identificar cuáles son los conocimientos que se requiere poseer para ser perito informático o idóneo, en función de que en el país aún no se cuenta con una carrera de grado especializada en esta disciplina.
- *Necesidad de contar con guías o protocolos por áreas y en general*: se busca identificar la importancia que adquiere tener una guía procedimental o un protocolo para el proceso de obtención y cuidado de pruebas.
- *Crecimiento del DATAI:* en esta categoría buscamos conocer la opinión que tienen los profesionales respecto al futuro de la institución y su crecimiento.
- *Medidas preventivas aconsejadas en ciberseguridad*: con esta categoría buscamos conocer cuáles serían las medidas preventivas más adecuadas para que la población se proteja de ser víctima de delitos informáticos.

Categorías emergentes

- *Desfasaje de DVR*: esta categoría surge de lo expresado en referencia a las pruebas obtenidas de cámaras de seguridad.
- *El cibercrimen y los delitos puros*: en esta categoría presentamos los ciberdelitos puros que se producen en la provincia de Mendoza
- *Preservación de datos del dispositivo original*: la importancia de preservar los dispositivos originales, como también la privacidad de las personas se refleja en el análisis de esta categoría.
- *Experiencias en casos relevantes*: se analizan los casos relevantes que manifiestan los entrevistados, en los que las pruebas digitales cobraron un gran protagonismo.

- *Relevancia de los dispositivos electrónicos en la obtención de la prueba*: la importancia de conocer los dispositivos electrónicos es lo que garantiza la adopción de la mejor herramienta para acceder a los datos.

4.2.3.1.1 Técnicas de conversación

La técnica de conversación seleccionada fue la entrevista semiestructurada, para lo cual se realizó una guía de entrevista aplicada a las unidades de análisis. Estos datos han sido organizados en función de las categorías de análisis propuestas, incluyendo aquellas que emergieron de las respuestas obtenidas.

4.2.3.1.2 Guía de entrevista

La guía de entrevistas se encuentra en el Anexo IV, pág. 145:

- Subjefe de División de Delitos Tecnológicos
- Subayudante de la Policía de Mendoza, integrante de la División de Delitos Tecnológicos y del DATAI.
- Efectivo de la División de Delitos Tecnológicos (Anexo IV, pág. 146 a 164)

4.2.3.1.2.2 Antigüedad en la dependencia

Los entrevistados cuentan con un promedio de 3 a 12 años de trabajo en la dependencia, lo que permite inferir que han ido adquiriendo experiencia en la actividad. Las incorporaciones en el lugar han sido paulatinas, y se ha seleccionado personal que cuenta con experiencia en escuchas telefónicas, o secuestros extorsivos, a partir de realizar una entrevista con los jefes, y posteriormente evaluar respecto a los conocimientos informáticos. Se observa que el personal se ha ido capacitando paulatinamente.

4.2.3.1.2.3 Capacitación y conocimientos

Una de las mayores dificultades de la especificidad profesional, se vincula con la falta de espacios de capacitación con niveles de grado, como tecnicaturas, licenciaturas o posgrados, que permitan a los interesados, adquirir conocimientos.

Sin embargo, los profesionales cuentan con formación que han obtenido de la Policía Federal, cursos de antisecuestros extorsivos; Comisiones en la Ciudad Autónoma de Buenos Aires en el Departamento de Tecnología Aplicada de la Policía Federal; cursos de

Office; Congresos en Rosario con una duración de una semana completa; cursos en el departamento de San Rafael “donde hemos recibido la misma temática respecto a cómo es la investigación o cuál es la función de la policía en una investigación criminal”; Congreso en Córdoba donde se estudiaron conceptos de la Deep Web y la Dark Web.

4.2.3.1.2.4 Herramientas más utilizadas

Las herramientas utilizadas para la obtención de pruebas contenidas en diversos dispositivos, son variadas. Algunas de ellas, como I-2 requieren de un conjunto de aprendizajes que deben llevar a cabo quienes la apliquen. Esta herramienta “es algo innovador y se relaciona con aquellas que, humanamente, no se pueden identificar datos ya que existen múltiples ramificaciones e interrelaciones, hasta incluso causas”. Esta herramienta, utilizada para la defensa nacional, permite convertir datos dispares en datos inteligentes, en tiempo real, facilitando a los investigadores identificar “las redes, patrones y tendencias en volúmenes crecientes de datos estructurados y sin estructurar” (Security M3, 2022).

Otra herramienta importante y valiosa es el relevamiento de cámaras, la cual le permite extraer datos sobre un ilícito. Esta acción parte de identificar las cámaras más cercanas del lugar del hecho, “poder observar, en primera instancia, cómo ocurre el hecho, y también observar hacia dónde van los autores del hecho, para hacer un seguimiento y dar con ellos”. Se identifican las cámaras cercanas, tanto privadas como las cámaras del Estado.

Para este análisis se aplican software de análisis de imágenes, mediante programas se puede “identificar si la dimensión de píxeles se puede regular de determinadas formas para ver o darle forma a una silueta. Son programas no fáciles de trabajar, son complejos, no son como en las películas que se ve en el primer zoom. Lleva mucho tiempo y muchas pruebas a la hora de ver y mejorar la imagen”.

4.2.3.1.2.5 Prueba digital

Esta prueba lleva muchos años utilizándose, dado que ha colaborado en el esclarecimiento de múltiples hechos. Consiste en obtener datos de dispositivos electrónicos, en los cuales se almacenan imágenes, o historial de navegación, o comunicaciones telefónicas, o conversaciones, y que, como pruebas, “adquieren una gran importancia en el

hecho porque resultan determinantes". Tal ha sido el caso de una mujer que envenenó a su marido, y que pudo esclarecerse el hecho, gracias a las pruebas obtenidas de su teléfono celular.

Uno de los expertos, nos menciona que esta prueba debe ser entendida en un contexto determinado, y es allí donde radica su comprensión. Cuando el personal policial se encuentra investigando la prueba digital, "ya estamos con una investigación judicial en curso, o por lo menos que se está iniciando", lo que significa que la misma comienza a ser relevante para aportar claridad al hecho. Esta evidencia puede ser diversa, en tanto provenga de una cámara de seguridad, o de un mensaje contenido en un dispositivo electrónico de una mensajería electrónica, como también puede ser un chat o información contenida en un disco rígido que exista en una computadora para una investigación de estafa. Esto demuestra la diversidad de las pruebas digitales.

La información que se obtiene, es aquella que no es inteligible para las personas, sin embargo, la misma debe ser reinterpretada y hacerla legible para que la misma pueda ser utilizada en la investigación, y posteriormente, en un juicio de ser necesario.

Las características de las pruebas digitales, son observadas por los especialistas, mencionando que las mismas "son volátiles, con lo cual hay tiempos perentorios". Esta volatilidad se debe a que "tanto los medios que se emplean para su creación, envío, almacenamiento y reproducción permiten que se pueda manipular, modificar o alterar" (Huertas Gutiérrez, 2021).

4.2.3.1.2.6 Obtención de pruebas

Las investigaciones que se realizan, permiten obtener pruebas tecnológicas que son transversales, dado que "en todas las investigaciones se encuentra como una gran herramienta la tecnología". Estas herramientas tecnológicas facilitan el avance de la investigación, permitiendo la identificación, por ejemplo de "la ubicación aproximada del autor del hecho".

Las pruebas que han sido obtenidas, en el caso de una cámara de seguridad, resultan de gran aporte: "nos fijamos el horario estimado del hecho a investigar, se visualiza una

hora para atrás, una hora para adelante, y se tiene mucha atención respecto a la información que se tiene de calles y testigos".

Luego, los datos de una cámara de seguridad, son procesados: "se comienza a analizar cada una de las imágenes, se realizan fotogramas q consideramos de interés, y en ellos se realiza la explicación del movimiento de las personas o aquellos datos que consideramos importantes para la causa, por ejemplo una moto, un vehículo, o la acción que está llevando a cabo cada una de las personas. Una vez que terminamos ese informe, se agrega al acta de extracción que se llevó a cabo en el lugar de la extracción fílmica, y es enviada a las oficinas fiscales".

Estas pruebas, surgen de diversos dispositivos, como los mencionados, permitiendo obtener información que contribuya al esclarecimiento de los hechos delictivos. Sin embargo, este proceso requiere de muchos cuidados "no es cuestión de meterse en un teléfono y nadar en los datos porque hay información muy sensible y se puede borrar cualquier elemento que esté, incluso en internet, un simple reinicio de un teléfono lo puede borrar". Los resultados de estos dispositivos suelen ser los más importantes, ya que en ellos la interacción social es más fluida que en un computador, por ejemplo. Se aspira al que se denomina "un escenario ideal" en el cual "lo correcto es secuestrar el aparato electrónico y colocarlo en una jaula Faraday, esto corta cualquier tipo de comunicación externa del dispositivo, con lo cual no hay forma de enviar comandos remotos para blanquearlo o borrarlo".

Es importante tener en cuenta que para la obtención de estas pruebas, el personal debe contar con conocimientos adecuados de tecnología, y especialmente, de los diferentes tipos de dispositivos, puesto que estos pueden almacenar su información en sus propias memorias internas, pero también este almacenamiento puede estar anclado en la nube. "La información ya no se contiene en un ordenador, por eso antes se llamaban delitos informáticos, hoy se llaman ciberdelitos o cibercrimen porque contempla esta idea de ciberespacio, en el cual está contenida toda esa información". Algunos dispositivos, si bien utilizan la nube para el intercambio, e incluso para su almacenamiento, "algunas aplicaciones conservan, en el dispositivo electrónico una copia".

Desde la experiencia en capacitación, uno de los entrevistados menciona que en Córdoba se hablaba de los delitos que se cometen utilizando la Deep Web y la Dark Web, lugares en los que "aquí en Mendoza no se han visto, o por lo menos no se han detectado casos en donde se cometan delitos en esos espacios, pero son espacios terribles que están sin control, prácticamente, y es muy difícil para la policía llegar a esos espacios en búsqueda y detectar ese tipo de delitos, toda vez que se trabaja con encriptaciones, trabajan con IP camufladas". En este punto, el denominado por los entrevistados como "delito puro", es decir un delito de grooming por ejemplo, tendrá personajes que "nunca muestran sus facetas, ya que estas se camuflan. Y es justamente una de las características que tiene el ciberespacio que es el anonimato, es su frutilla en el postre. Por eso es tan difícil detectarlos, y llevarlos a la cárcel".

4.2.3.1.2.7 Relación con el Poder Judicial

La importancia del trabajo mancomunado en referencia a la prueba digital, queda evidenciada en los aportes de los entrevistados. Esto es así, dado que el trabajo en conjunto, y sobre todo ágil y veloz, garantiza un rápido esclarecimiento de los casos. La solicitud de intervención policial, surge desde el CEO, y se desplaza al personal al lugar del ilícito. Dependiendo de la gravedad del hecho, también concurre el fiscal o ayudante de fiscal, quienes avalan la identificación del material informático que colabora con la investigación, "el cual generalmente, es un DVR, hacemos un barrido de cámaras"… "teniendo en cuenta el hecho puntual, observando las cámaras que se encuentran al mismo, con el objeto de visualizar lo que las cámaras aportan". Estas, como se ha mencionado, pueden ser públicas, o privadas. En este último caso, es necesario que el fiscal emita la orden, si el propietario no quiere colaborar.

El proceso requiere que, en primera instancia, se realice una identificación de las cámaras, luego se procede al reconocimiento, para lo cual se debe extraer el DVR que poseen las cámaras. Luego "se realiza el acta, en presencia de testigos y morador, donde se deja constancia del tipo de DVR, la marca, el número de serie, el desfasaje que posee el mismo, y se procede a la extracción".

En la adquisición y en el análisis de las pruebas digitales, las Unidades Fiscales citan a las partes, mientras que el secuestro lo realiza el personal policial. Las fiscalías reciben un turno para que asistan sus peritos, como también los peritos querellantes o el perito de parte, y se les explica cada uno de los pasos que se llevan a cabo para hacer la copia bit a bit o la investigación forense. Cuando se obtienen los datos, "se da un nuevo turno y se procede a un nuevo análisis de la copia. Siempre protegiendo la copia, la materia prima, el disco original".

Este trabajo es posible gracias a la relación fluida que se mantiene con miembros del poder judicial, quienes solicitan la asistencia policial, pero a su vez contribuyen con la obtención de los datos que requiere el personal, para su análisis. Se debe explicar cada uno de los pasos que se ejecutan.

El DATAI y la Unidad Fiscal trabajan en forma estrecha, con una relación permanente dado que la obtención de pruebas, es lo que permitirá alcanzar un resultado esperado. "El mayor beneficio es que, a través de la comunicación telefónica se nos da la orden de realizar una medida, se deja una constancia, y se labra la correspondiente acta de la orden emanada por la autoridad competente, y se realiza la medida ordenada. Ante cualquier duda en un informe, nos llaman a la dependencia, y esto nos permite incorporar nuevo material, o ampliar informes que ya hemos hecho en el momento. Es muy fluido".

Esta vinculación finaliza cuando finaliza el acto jurídico, es decir cuando se alcanza la sentencia del juicio. Esto es así ya que el personal policial es citado a declarar, expresando los pasos que han realizado en el proceso de investigación, con la obtención y el procesamiento de los datos. "Nosotros como policía, en función judicial, prestamos la colaboración al Poder Judicial en materia de investigación. Al tener una muy buena relación, en este caso División Delitos Tecnológicos y el DATAI tiene buena relación con el Poder judicial, creo que es necesario que esa relación sea fluida, puesto que esa intervención que tenemos en el proceso penal, es dinámica, es rápida y expeditiva".

4.2.3.1.2.8 Relación entre áreas

No solo la relación del personal policial con el Poder Judicial es relevante en estos casos. Sino que además, la relación que se mantiene entre las diferentes áreas policiales, es fundamental para alcanzar los objetivos de esclarecimiento de hechos delictivos.

Esta relación es permanente. "Se vincula la información, dado que los trabajos se entrelazan entre las divisiones, y es necesario atacar en conjunto la misma información para que, desde cada sector se aporte su trabajo idóneo. Lo que veo quizás, es como aporte a como estamos hoy. Si bien está la interrelación entre las 3 divisiones, el problema es estamos en el mismo edificio, pero no se encuentran contenidas en el mismo lugar. Considero que es necesario que algunas divisiones estén dentro de Delitos Tecnológicos, a modo de no realizar, en algunas ocasiones, el mismo trabajo. O acatar el trabajo en conjunto de una sola vez, y dar un informe terminado, y no dar un informe de delitos tecnológicos, otro informe de delito criminal, otro informe de análisis de UFE o cámara y otro informe el personal que está haciendo extracciones UFE".

Consideran que esta relación es una gran optimización de los tiempos del personal, pero también de simplificación de las actividades, ya que todos pueden estar buscando, en diferentes lugares y al mismo tiempo.

"La relación se inicia en la investigación de un homicidio, por ejemplo, en el que puede existir una cámara de seguridad que aporte datos para identificar el autor del hecho, en el cual lo primero que se busca son las pruebas, o los indicios para llegar al autor de algún hecho delictivo y eso da una ayuda a la justicia".

4.2.3.1.2.9 Cadena de custodia y resguardo de la prueba digital

La cadena de custodia se respeta en su proceso, como se ha observado en las entrevistas. El personal de la División de Delitos Tecnológicos, protege el material y lo resguarda en forma segura. Cuando finaliza la extracción, "se realiza un Hash, que es un algoritmo que le brinda autenticidad y seguridad a lo que estamos extrayendo y es firmado también por el personal actuante, testigo y morador".

Una vez que ese material llega a las oficinas donde se analizará, es resguardado en un soporte digital tipo DVD, con su correspondiente Hash, y se pone a requerimiento de las unidades fiscales. Puede guardarse en un DVD, “pero también lo guardamos, teniendo en cuenta la gran cantidad de información a resguardar, en discos rígidos portátiles, en discos rígidos, o se guardan en pendrive aportados por las Unidades Fiscales. Eso depende de la consideración que se tenga, teniendo en cuenta la cantidad de información a resguardar”. A las computadoras se les hace una copia bit a bit sin analizar el original. La búsqueda es dirigida, por ejemplo si se trata de un delito de estafa, se busca una imagen de una boleta que se pudiera estar adulterando.

Las garantías y recaudos que se deben tener en las adquisiciones de la información, buscan proteger la privacidad. Sin embargo, cuando la tecnología es utilizada como objeto, es más complejo, ya que la misma se conecta “con lo que denominamos el clouding o la internet o la nube”. Esa información que no está contenida en los dispositivos, se encuentra en servidores externos, como por ejemplo “cuentas de correo electrónico, redes de mensajería como lo son Facebook, Twitter, Instagram, Snaptchat, WhatsApp, etc”, y en consecuencia algunas veces se debe solicitar a estas empresas que se brinde la información. Esto es posible gracias a la adhesión de Argentina al Convenio de Budapest.

4.2.3.1.2.10 Función del perito informático y del idóneo informático

Una de las dificultades, como hemos mencionado, es la capacitación y posterior certificación, de los conocimientos adquiridos por parte del personal. La formación en tecnología, es permanente, y esto es así porque los cambios son tan vertiginosos, que requieren aprender a manejar nuevos software que van surgiendo a medida que también, el delito se va perfeccionando.

El personal policial del DATAI realiza “labores casi de peritos, no siendo peritos”, pero sí son idóneos en lo que realizan. La formación en academias diarias, en charlas que mantienen con otros profesionales y sus jefes, y aprendizajes de conocimientos que adquieren con su propia investigación, como también la experiencia que van adquiriendo, los habilitan para ocupar los espacios de indagación en pruebas digitales.

La función del idóneo es la de esclarecer lo que se le está solicitando, aportando desde su conocimiento, la mayor prueba posible. La función del perito, está dada por la certificación, y en la capacidad de identificar los procedimientos que los idóneos, desarrollan en la búsqueda de datos que aporten a la investigación.

"La División Delitos Tecnológicos no cuenta con un perito informático, pero si cuenta con idóneos en informática forense, dado que se han hecho cursos, capacitando al personal, que a su vez tiene una larga experiencia y experticia en el tema. No nos olvidemos que el Código Procesal Penal menciona que cuando no exista un especialista en la materia, bien puede ser tomado como tal, aquella persona que presente experticia en la materia. Esto avala al idóneo. Es decir, una persona que se especializa por un período de tiempo determinado realizando la tarea, ya tiene la idoneidad para explicar cómo funciona un determinado mecanismo. Por ahí creo que va la diferencia entre el idóneo y el perito en informática forense, entendiendo también que la División de Delitos Tecnológicos no realiza informes periciales, sino que la División realiza informes tecnológicos. Esto quiere decir que es la experiencia, puesta de manifiesto en un informe, por parte del policía".

Otra de las diferencias se da en los informes que ambos emiten: "En el informe tecnológico, nosotros plasmamos, por ejemplo, una secuencia de video en la que tenemos que buscar a algo o alguien, informamos lo que estamos visualizando. En cambio, el informe que realiza un perito, es más detallista, y utiliza otros programas, en los cuales se ingresa mucho más en la parte técnica de algún tipo de dispositivo, por ejemplo, ya sea computadora, móvil, es mucho más técnico el trabajo. El informe tecnológico es más completo y permite describir lo que nosotros estamos llevando a cabo en la investigación".

4.2.3.1.2.11 Necesidad de contar con guías o protocolos por áreas y en general

Una de las mayores dificultades es que no hay una guía por cada área, o un protocolo en general, que pueda unificar las acciones que se llevan a cabo en el DATAI. Esto sería muy bueno "si vamos a trabajar en conjunto, que cada área conozca el protocolo general que conlleva al conjunto de áreas". Y que además tengan un protocolo en común, entendiendo que no todas las áreas realizan el mismo trabajo, es posible que realicen una guía por área y un protocolo general. De esta forma se podrían optimizar los recursos que cada uno tiene y se podría trabajar con mayor fluidez en conjunto.

4.2.3.1.2.12 Crecimiento del DATAI

Los entrevistados consideran que habrá cada vez, "mayor cantidad de intervenciones en cuanto a cada una de las investigaciones". Esto es así por el crecimiento de la tecnología en la sociedad, pero también un crecimiento de los delitos en el ciberespacio, o con la utilización de medios tecnológicos.

"Creo que la Policía de Mendoza se está preparando para el futuro, lo veo así. Siempre vamos detrás del delincuente en pos de cuestiones de recursos, de preparación. Es más, se entiende que el delincuente siempre está innovando, porque a medida que el control social le va poniendo trabas y justamente va regulando esas conductas para que no ocurran, el delincuente se va renovando", lo que claramente es una mutación del delito, como en toda sociedad.

Importante es el control social informal que ejercen las redes sociales, el cual parece ir más avanzado que el control social formal, puesto que en ellas "se producen ciertos movimientos de ir censurando a personas que hacen, por ejemplo, tráfico de imágenes de menores. Me refiero a la pornografía infantil, o a las cuestiones de suplantación de identidad que no están reguladas como delito en la Argentina, aunque Buenos Aires es la única provincia que lo ha aplicado como una contravención". Sin embargo, las redes sociales con sus propias normas de convivencia, ponen límites a algunas acciones que impliquen daño a otras personas.

Categorías emergentes

4.2.3.1.2.13 Desfasaje de DVR

El desfasaje de DVR hace referencia a que algunas cámaras de seguridad, no cuentan con espacios donde almacenar imágenes por largos períodos de tiempo, como también pueden estar "desfasados en sus horarios, días, años, minutos". Esto debe ser observado por el personal policial, ya que, en el análisis, se requiere tener una orientación en tiempo real de cada una de las imágenes.

Uno de los expertos denomina a esta acción como "pisando", es decir, superponiendo una grabación. Si un DVR, un sistema de grabación, tiene una semana de almacenamiento, cuando llega al octavo día, el primer día se va borrando, es decir que se

pierde esa información. Sin embargo en este caso pudimos dar con buenas cámaras de seguridad, tanto privadas como del Estado, en la cual pudimos lograr dar con Fxxx, y pudimos encaminar los pasos que realizó, y los pasos que realizó también el imputado, para poder aportar las pruebas necesarias a la Unidad Fiscal de Homicidios, y poder aportar los pasos que dio el imputado también que fueron el indicio de que él fue la última persona que estuvo con Fxxx.

4.2.3.1.2.14 El cibercrimen y los delitos puros

Los delitos netamente informáticos y aquellos en los que media la tecnología, "los estamos abarcando nosotros" en el DATAI.

Los delitos puros como el grooming, requieren para su investigación, "de un secuestro de computadoras equipos celulares para periciar, se realiza el análisis de extracción de información UFE, se realiza el geoposicionamiento de Gmail o de cualquier tipo de herramienta que tenga configurado el equipo para localizarlo. Eso es lo que mayor cantidad de trabajo nos llega a la división". Esto es importante dado que este tipo de delitos implica víctimas menores, por lo que el trabajo de estos delitos requiere de gran capacitación profesional.

Los ciberdelitos de estafa son abordados, generalmente, por la Justicia Federal puesto que los mismos competen a este fuero.

4.2.3.1.2.15 Preservación de datos del dispositivo original

Los dispositivos originales no se analizan. Esto es así ya que muchas veces se debe trabajar sobre la prueba original, y volviendo al tema de la volatilidad de los datos, es probable que se pierdan. Pero además, en función de "las buenas prácticas forenses, se hace un clonado bit a bit en caso que se pueda hacer, y se trabaja sobre un clon, a efectos de no adulterar el original. En el 90% de los casos sí se puede hacer un clonado del material a periciar, pero en los dispositivos electrónicos como smartphones, el clonado es imposible por su arquitectura. Pero, como se puede realizar una adquisición parcial de la información, es esa la que se mantiene imperturbable. La utilización o no del soporte original, queda a criterio del experto que realice la medida, dependiendo del tipo de material, será la técnica que se utilice. En todos los casos, se lleva adelante una preservación del material adquirido

y ese si puede ser replicado cuantas veces sea necesario, es decir para la defensa, para la querella etc.

Las dificultades se dan con el tipo de dispositivo, pero en líneas generales se extrae la mayor cantidad de información o datos de usuario que son lo importante. Esto significa que no hay una adquisición completa sino parcial, siempre teniendo en cuenta que toda adquisición está autorizada por un juez de garantías. En cada oficio judicial se explicita que tipo de extracción se debe realizar, la cual debe ser completa para su preservación y resguardo, ya que la herramienta no permite tantos modos de extracción limpia.

"En una conversación, no se busca solo un texto determinado, sino que se extrae completa y luego, en el análisis, se buscan las cuestiones relacionadas con el hecho investigado. En ocasiones esto sale explicitado en la orden judicial, pero en el 95% de los casos somos libres de buscar cualquier parte del material. En todas las ocasiones la copia bit a bit lleva una firma de seguridad y autenticidad llamado Hash".

4.2.3.1.2.16 Experiencias en casos relevantes

En relación con los datos secundarios presentados del caso de femicidio, consideran que fue muy resonante, consistió en una "área contra reloj, porque teníamos que hacer un relevamiento de cámaras, y a medida que se hacen los relevamientos de cámara, se tienen que extraer y visualizar, intentar dar con la víctima y ver hacia donde se dirigió. Mientras tanto que estás visualizando una cámara se puede estar pisando otra, entonces es un trabajo contra reloj".

Otro caso relevante fue el del joven venezolano, quien fue ultimado en la entrada de su casa cuando se disponía a guardar su vehículo luego de regresar de trabajar. El seguimiento del vehículo sustraído, a través de las cámaras de seguridad del CEO, y de privados, permitió obtener la información del recorrido. A esto se sumó la indagación policial respecto del modus operandi de la zona lo que permitió identificar gente vinculada, y esto permitió resolver la causa en 48 horas.

4.2.3.1.2.17 Relevancia de los dispositivos electrónicos en la obtención de la prueba

Los tipos de dispositivos en los que se encuentran las pruebas, son transversales a cualquier tipo de delitos. Nos explica el especialista que: "Se pueden tomar bajo dos

miradas: Una es la mirada de la tecnología como objeto del delito, esto quiero decir que el delito no se podría haber cometido si esa tecnología no se hubiese inventado. Por ejemplo el *phishing*, el cual es un delito en el cual, por ejemplo, yo pongo un señuelo para que otro ponga un dato sensible y yo lo pueda obtener, por ejemplo una página falsa, o un sistema de *login* de un banco falso, que es igual al original, pero no es el original y el ciberdelincuente obtiene los datos especiales para ingresar a esa cuenta de banco y así obtener la información que después usa para robar, cometiendo una estafa. Este es un delito puro, el cual es el que obtiene un dato para ingresar a un sistema que no debería ser accesado, que sin embargo, no se podría haber cometido, si no existiera la tecnología de las páginas web, por ejemplo".

"Por otro lado, la mirada en la que entendemos que la tecnología puede ser utilizada como medio. Con esto me refiero, por ejemplo, envío un mensaje: 'juntémonos en tal lado' para que vos me vendas una bicicleta, la persona concurre a ese lugar y yo lo termino asaltando. En este caso la tecnología no importaba tanto, dado que podría haberlo llamado por teléfono o haber tenido otra comunicación y lo mismo lo hubiera asaltado. Pero sí está siendo utilizada la tecnología como medio para cometer un delito".

Entendiendo estas dos ramas, será como se obtendrá la evidencia para ser aportada en un proceso judicial.

La relevancia que implica conocer e identificar el dispositivo radica también en que será lo que el personal policial, deberá pedirle al juez que solicite, o que emita órdenes para su acceso. Por ejemplo, si gran parte de la información del dispositivo se encuentra en la nube, en Gmail, o en Facebook, el juez deberá expresar un pedido a estas empresas para que se acceda a determinada información, si no se puede acceder desde el dispositivo. "Este ciberespacio cuenta con ciertas características especiales en donde una de ellas es el anonimato, puesto que cualquier persona en el ciberespacio puede hacer uso de ella, tanto como se puede mostrar tal cual es, los ciberdelincuentes no van a andar mostrándose tal cual son".

4.2.3.2 Análisis e interpretación de resultados.

Los profesionales que desarrollan actividades en el DATAI, cuentan con una experiencia de 3 a 12 años, aproximadamente, de trabajo. Teniendo en cuenta que, para el desarrollo de esta tarea no hay capacitaciones formales en la provincia, y que, las existentes a nivel nacional son recientes, es importante destacar la formación personal que cada efectivo, ha logrado desarrollar en su trabajo. En este sentido, contar con tres años de experiencia en la actividad, permite inferir que se han obtenido un conjunto de conocimientos, producto del aprendizaje cotidiano, que contribuyen a la construcción de un aprendizaje tecnológico y científico. Esta dificultad de acceder a formación profesional se debe, en gran medida, a la existencia de una institución que ha ido incorporando paulatinamente herramientas tecnológicas puestas al servicio de la Seguridad Pública.

La capacitación, la adquisición de conocimientos tecnológicos y el aprendizaje que surge de investigaciones personales, se pone en evidencia en el uso de herramientas tecnológicas de gran complejidad, como por ejemplo el sistema I-2, cuya innovación en el campo de la prueba forense cibernética, requiere, por parte de los efectivos, un estudio de sus componentes, de sus procedimientos y sobre todo, el destino de tiempo al aprendizaje de las características particulares de esta, y otras herramientas.

De igual manera, la observación de diferentes cámaras de seguridad, dispuestas en diferentes lugares de la ciudad, requiere de un aprendizaje y ejercicio permanente, sobre todo en la atención y observación de datos. Entendiendo que estos datos no son solo aquellos que puedan ser observados a simple vista, sino que pueden existir otros importantes en su contexto, el profesional que realiza la tarea de observación, debe estar atento a todos los detalles que puedan ser significativos para la investigación. Esto requiere no solo de conocimiento, sino también de entrenamiento que construya la experiencia en la tarea. Si bien se cuenta con software específicos para la identificación de imágenes, existen datos que requieren de la interpretación humana para su contextualización.

Este tipo de pruebas digitales, que llevan mucho tiempo siendo utilizadas, contribuyen en gran medida al esclarecimiento de hechos. Los dispositivos electrónicos almacenan un conjunto de datos consistentes en imágenes, historiales de navegación en internet, comunicaciones, mensajes, de gran importancia, dado que “cualquier registro

generado por, o almacenado en un sistema computacional, puede ser utilizado como evidencia en un proceso legal" (Huertas Gutiérrez, 2021, p. 17). Teniendo en cuenta su intangibilidad, su duplicidad, y sobre todo la volatilidad de la misma, la diversidad de espacios desde los cuales se pueden obtener, permiten organizar el rompecabezas de diversos hechos. En la prueba digital es importante destacar que no siempre son comprensibles para las personas, por lo que estas deben ser interpretadas y luego, hacerlas legibles a fin de su utilidad en la investigación. El seguimiento de diferentes cámaras de seguridad, comparados con la utilización de mensajería en WhatsApp, el seguimiento de la utilización de una tarjeta SUBE y la cámara de seguridad de un colectivo determinado, permitieron observar los pasos de una víctima de femicidio. Estos datos aislados, no significan nada si no son analizados, a la luz del conocimiento forense y la experiencia observacional.

Es por este motivo que la obtención de la prueba digital, debe ser cuidadosa, "no es cuestión de meterse en un teléfono y nadar en los datos porque hay investigación muy sensible y se puede borrar cualquier elemento". Sin lugar a dudas, como ha sostenido Huertas Gutiérrez (2021) estas características de volatilidad, deben ser tenidas en cuenta cuando se obtienen estos datos, puesto que "los medios que se emplean para su creación, envió, almacenamiento y reproducción, permiten que se pueda manipular, modificar o alterar" (p.17). Además, estas pruebas son parciales, puesto que está formada por diferentes ficheros informáticos que se encuentran repartidos en varios soportes digitales y localizaciones. Por otro lado, el almacenamiento cobra una vital importancia, ya que algunos dispositivos pueden tenerlo en sus memorias internas, en su memoria RAM, la cual es más volátil, o bien en la nube. Considerada como prueba idónea, se convierte muchas veces, en la única viable para encontrar las respuestas a hechos delictivos, sin embargo, como bien menciona Pérez Cascella (2017), "existe un gran conflicto de la veracidad de la información"… un "tenue velo de la obtención de prueba válida para el proceso civil", sobre todo en la preservación de la privacidad. Expresado en la Constitución Nacional, esta intromisión en los datos personales, requiere contar con un resguardo especial de la prueba, buscando no dañar la privacidad, tal como lo hemos mencionado en nuestro Marco Teórico (pág. 67).

Si bien, como sostienen Granero (2019), Pérez Cascella (2017), e incluso el art. 319 del Código Civil y Comercial de la Nación, el valor probatorio de la prueba, debe ser apreciado por el juez y los fiscales, de forma tal que aporten conocimiento y claridad al hecho narrado, siempre constatando la veracidad de "los soportes utilizados y de los procedimientos técnicos que se apliquen" (Art. 319, CCCN).

La recolección de la evidencia, sostenemos en la Guía procedimental de recolección de evidencia digital, es la piedra angular de la pesquisa, configurando los anclajes necesarios para determinar qué sucedió, y cómo y cuándo se cometió un delito (p. 60 Marco Teórico). Esta recolección, mantiene el cuidado establecido en los protocolos internacionales para la obtención de pruebas informáticas forenses, y luego se realiza su análisis se realiza mediante copias. Si bien, nuestros profesionales mencionan que el "escenario ideal sería secuestrar el aparato electrónico y colocarlo en una jaula Faraday", lo que suspende cualquier tipo de comunicación externa del dispositivo, no se cuenta con estas herramientas, por lo que se coloca el dispositivo en modo avión, por ejemplo un Smartphone, buscando preservar los datos contenidos en su interior.

En referencia a esta obtención de pruebas, es importante destacar que los delitos puros, como el grooming, pueden tener personajes "que nunca muestran sus facetas, ya que estas se camuflan. Y es justamente una de las características que tiene el ciberespacio que es el anonimato, es su frutilla en el postre. Por eso es tan difícil detectarlos, y llevarlos a la cárcel". En referencia a esto, el ciberespacio es un lugar de amplios almacenamientos de datos, que, por estar inmersos en software de alta complejidad, permiten no solo ocultar el verdadero autor, sino que construyen camuflajes que no permiten identificar las direcciones IP de su procedencia. Esto genera que algunos delitos puros, resulten de difícil resolución, e incluso muchas veces no se pude llegar a solucionarlos. En este punto siempre deberemos tener en cuenta la gran velocidad de crecimiento de las herramientas tecnológicas de las TIC.

Ya sea para la obtención de pruebas tecnológicas que contribuyan al esclarecimiento, en tanto transversales al hecho delictivo, como aquellas que se requieren para comprobar delitos puros, la relación establecida con los miembros del Poder Judicial, es fundamental puesto que la interacción con fiscales y ayudantes de fiscales, permite

definir qué buscar y donde buscarlo. También es importante la relación que se establece entre áreas, ya que este trabajo requiere de múltiples conocimientos. Esto permite vincular información que se encuentra entrelazada en las investigaciones, aunque sostienen que la información debería estar en un solo lugar, por esto consideran que "es necesario que algunas divisiones estén dentro de Delitos Tecnológicos, a modo de no realizar, en algunas ocasiones, el mismo trabajo".

Al igual que la obtención de la prueba digital, la cadena de custodia que esta requiere para su preservación, se realiza mediante un proceso de protección permanente del material para su resguardo seguro. El material es extraído de los diferentes dispositivos, y en ese momento se realiza el procedimiento denominado "Has", algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Este algoritmo matemático, le otorga a cada dato, un componente que le es propio y único, lo que garantiza autenticidad y seguridad. El procedimiento de preservación se lleva a cabo mediante copias guardadas en DVD, discos rígidos portátiles o pendrive, dependiendo de la consideración que se tenga y teniendo en cuenta el volumen de la información a resguardar. En computadoras, las copias se realizan bit a bit, sin analizar el original. En todo el proceso de la cadena de custodia, como también de las copias, se busca proteger la privacidad. El análisis de los datos puede ser presenciado por peritos ya sean estos de la querella, como de la fiscalía ejerciendo los derechos de sus representantes.

En relación con la cadena de custodia y la obtención de pruebas, es necesario que se cuente con una guía procedimental por cada área, y un protocolo en general. Si bien hay una guía, la misma no ha sido creada por la institución y en consecuencia, no contemplarían el contexto particular.

La importancia de la institución, en tanto aportes de pruebas digitales, permite inferir que su crecimiento en el futuro, será mayor, por lo que contar con producción de herramientas propias y adecuadas a la particularidad de la provincia, es indispensable para garantizar un trabajo de excelencia, tal como lo han expresado los entrevistados.

De nuestras entrevistas, se han desprendido nuevos conocimientos como el aportado por la conceptualización de "desfasaje de DVR", el cual debe tener en cuenta las

condiciones particulares de las cámaras de las cuales se obtiene información, dado que su análisis requiere de contextualización en el tiempo, siendo este un dato de vital importancia, como se ha demostrado en varias oportunidades.

4.2.4 Análisis e interpretación de los resultados

De acuerdo a los datos obtenidos, podemos inferir que el personal que desarrolla tareas en el DATAI, cuenta con la idoneidad para desarrollar las actividades de investigación que les son encomendadas. La adquisición de la prueba, su resguardo y posterior análisis, se realiza con los pasos establecidos por nuestra normativa legal vigente, respaldados por lo definido en el Convenio de Budapest, como también en la guía procedimental de recolección de evidencia digital. De igual manera, se respeta la cadena de custodia, lo que ha quedado en evidencia en el caso citado, ya que el posterior análisis de los datos obtenidos, ha contribuido a esclarecer los hechos, aportando pruebas sobre la culpabilidad del imputado.

En este caso, se observa como las redes sociales, adquieren un rol protagónico en la obtención de pruebas, así como también el análisis de los teléfonos y la utilización que las personas, hacen de ellos. La utilización de la mensajería de WhatsApp, como también la de Instagram y Facebook, han aportado indicios valiosísimos que, unificados con la lectura de la tarjeta SUBE y el análisis de cámaras de seguridad, permitieron al personal, resolver el caso.

Pudimos observar que el personal del DATAI, refiere el conocimiento necesario en la manipulación de las pruebas digitales, teniendo siempre en cuenta la fragilidad y volatilidad de las mismas, y, sobre todo, respetando la privacidad de los dispositivos personales que son analizados. En referencia a estos dispositivos personales, el resguardo de pruebas y su análisis, permite que se obtengan desde conversaciones, hasta imágenes, pasando por historiales de visitas en internet, lo que ha facilitado la resolución de otros casos.

Es importante destacar que el almacenamiento de los datos, puede encontrarse no sólo en el dispositivo estudiado, sino que el mismo puede estar guardado en la nube, es decir, en internet. En el ciberespacio, los mismos se guardan en Gmail, drive de Hotmail, o

Dropbox, siendo lugares que requieren autorización para su acceso. Gracias a la normativa vigente, y la adhesión de Argentina al Convenio de Budapest, nos resulta simple solicitar a estas empresas la información correspondiente para su posterior análisis.

En relación a la obtención de estos datos, el personal nos ha manifestado en todo momento, el respeto por la privacidad, lo que nos exige la implementación de herramientas tecnológicas que no invadan los dispositivos, evitando dañarlos y seleccionando solo las pruebas necesarias a la investigación en curso. En este punto, es importante lo que solicita la fiscalía, con la cual se mantiene un trabajo mancomunado, y permanente, en una relación fluida y de entendimiento.

Las pruebas obtenidas en múltiples casos, transversales a los hechos delictivos, nos permitieron identificar a los responsables de los mismos, tal como menciona uno de nuestros idóneos, pudimos identificar que una mujer había envenenado a su marido, a partir de analizar su navegación por internet, y esto gracias a que este historial de navegación no había sido eliminado. Esto es un ejemplo de la volatilidad que tienen los datos en los dispositivos, el cual de haber sido simplemente reiniciado, probablemente hubiera desaparecido los datos.

Las investigaciones realizadas por las diferentes áreas, fueron las que permitieron establecer los caminos recorridos por los responsables de los actos delictivos. Y esto reviste una gran importancia, ya que, si bien no se encuentran todos en un mismo espacio trabajando en conjunto, si pueden trabajar las pruebas de manera sincronizada, analizando los datos, y preservando los mismos para su posterior utilización en un juicio, de ser necesario. Estas actividades sincronizadas, facilitan al fiscal, y luego al juez, entender, casi paso a paso, lo que sucedió con un hecho determinado.

De los datos primarios, entendemos la importancia de contar con una guía de procedimientos que nos sea propia, en la que podamos volcar nuestros conocimientos, nuestra experiencia adaptándola al contexto de la provincia de Mendoza.

En referencia a la preservación de los datos del dispositivo original, se debe tener en cuenta siempre que este no es el que se somete a análisis, sino que, en base a las buenas prácticas forenses, se realiza un clonado bit a bit, trabajando sobre el clon, a fin de no

adulterar el original. Esto también se encuentra respaldado en la volatilidad de los datos, y el tipo de dispositivo del que se trate. Para esto, los profesionales deben contar con los conocimientos necesarios que permitan acceder, respetando la privacidad, protegiendo el dispositivo original y obteniendo los datos de manera adecuada, sin dañar smartphones o computadoras, sobre todo teniendo en cuenta que estos dispositivos suelen ser determinantes en muchos casos.

Conclusiones y aportes

Conclusiones

En este trabajo de investigación hemos buscado dar a conocer el trabajo que se realiza en materia de recolección de pruebas tecnológicas. Para esto, nos propusimos como objetivos generales, analizar el Sistema de Comunicación Electrónica que posee el DATAI, en relación a la obtención de datos de redes de mensajería digital, protocolo de identificación, resguardo, análisis y presentación de informes analíticos, buscando visibilizar la importancia que tiene la implementación de un protocolo de recuperación y recolección de datos digitales almacenados en un dispositivo electrónico. La finalidad de esta obtención, preservación y análisis de estas pruebas, es la de esclarecer hechos delictivos en los que, el medio electrónico cobre un significado especial en relación a los datos en el contenidos.

Para alcanzar estos objetivos, en primer lugar contextualizamos la problemática en una sociedad atravesada por el uso de las TIC, en la que Argentina se encuentra inmersa, mostrando que sus habitantes mantienen una importante conectividad, la cual se incrementó durante los dos años de pandemia de Covid-19, momento en el cual el uso de internet, y de sus dispositivos electrónicos, fueron los protagonistas que permitieron a la sociedad, mantener relaciones entre sí. Pero, por otro lado, se constituyeron en herramientas que facilitaron y posibilitaron la generación de hechos delictivos, muchos de los cuales existían previamente, como también su crecimiento. A pesar de que nuestro país presenta una gran brecha digital, tanto interna como en relación con otros países, hemos podido observar que en Mendoza, los datos obtenidos del INDEC (2020) han arrojado que el 85,6% de la población posee internet y el 81% posee teléfono celular, lo cual se ha visto incrementado como producto de las necesidades, sobre todo educativas y laborales, que surgieron en el período 2020-21. El incremento del uso de las TIC, sobre todo durante el presente siglo, ha obligado a los Estados a incrementar las acciones de seguridad en pos de proteger a sus ciudadanos, en este caso de ataques de ciberdelincuentes, pero también de la utilización de estas TIC, como medio para realizar un hecho delictivo. El uso de redes sociales, es un espacio de excelencia para contactar personas, pero también para realizar hechos delictivos o, cuando menos, utilizarlas como señuelos para atraer posibles víctimas. En Argentina, el 79,3% de la población, usa redes sociales activamente, como Facebook, Instagram, Tik

Tok, YouTube, (INDEC, 2021), conteniendo una infinita cantidad de datos, entre ellos los gustos particulares de las personas, sus selecciones de compras y por supuesto, sus relaciones.

En este contexto, las TIC, descriptas en sus conceptualizaciones y funcionamiento en el capítulo II, son protagonistas de la vida cotidiana de millones de ciudadanos, no solo en nuestro país, sino en el mundo. El control social punitivo, como hemos mencionado, ha debido forjar nuevas normativas legales que permitan aplicar sanciones a delitos específicos, como por ejemplo el *grooming* o la sextorsión. Este control social, en su búsqueda de esclarecimiento de hechos delictivos, se vale de los aportes que las TIC le brindan, en tanto huellas que las personas van dejando en diversos dispositivos electrónicos a través de sus interacciones en redes sociales, o su navegación por internet, o sus imágenes. Las redes sociales, son espacios de interrelación en los cuales los datos, contribuyen en gran medida al esclarecimiento de un hecho delictivo, como también a identificar su proceso de construcción. A pesar de que ellas aplican sus propias normas de control social informal, a partir de reglas de convivencia que se encuentran en permanente renovación, muchas veces estos espacios sirven para la ejecución de hechos delictivos.

Es indiscutible en nuestros días, que el delito en la era digital, tiene un gran protagonismo. Y, en este punto no nos referimos solamente a los delitos puros como el hacking, o quizás un malware que busque destruir bases de datos, sino que los ataques réplica o los ciberataques de contenido como el *grooming*, o el *sexting* o el *cyberbullying*, generan grandes daños individuales y sociales. Frente a este exponencial crecimiento del ciberdelito, la Seguridad Pública ha desarrollado sus propias herramientas para enfrentarlos. En nuestro caso particular, la incorporación de las TIC en la policía de Mendoza, nos ha permitido esclarecer múltiples hechos, como hemos demostrado, e incluso identificar hechos delictivos que, sin la existencia de esta tecnología, hubiera sido difícil reconocer. La incorporación del sistema TETRA, permite la comunicación en todo el territorio provincial. Mientras que las cámaras de seguridad, con monitoreo de vigilancia Boshc, han aportado gran cantidad de datos para el esclarecimiento de hechos delictivos. La incorporación de tecnología biométrica, permite la rápida identificación de personas que pueden estar con pedido de captura, y la más reciente adquisición del sistema CoDIS con el

cual se ha logrado generar un banco de perfiles genéticos, siendo Mendoza una ciudad pionera al crear nuestro Registro Provincial de Huellas Genéticas Digitalizadas en el año 2018. Otra incorporación de gran importancia para la Seguridad Pública, son los drones, destinados a la vigilancia. El acompañamiento de la tecnología en la investigación criminal, se ha ido adaptando paulatinamente a los cambios sociales que fueron requiriendo de incorporación de herramientas que permitan incorporar pruebas digitales. Estas pruebas, deben ser protegidas y resguardadas en todo momento, a fin de evitar posibles pérdidas de información, por lo cual la cadena de custodia, en tanto procedimiento "que permite de manera inequívoca conocer la identidad, integridad y autenticidad de los vestigios o indicios digitales relacionados con un acto delictivo, desde que son encontrados hasta que se aportan al proceso como pruebas" (Ministerio de Justicia y Derechos Humanos, 2017), adquiere también un rol protagónico en materia de pruebas forenses. Para esto, nuestra policía cuenta con un conjunto de herramientas tecnológicas de vanguardia, que permiten la obtención de pruebas digitales, y su preservación evitando que las mismas puedan ser dañadas.

Esta conservación, al igual que la obtención, se desarrolla durante un proceso de investigación que presentamos en el capítulo III. El Sistema Penal también se encuentra en un proceso de grandes cambios, ya que la incorporación de pruebas digitales que contribuyen al esclarecimiento de hechos delictivos, ha debido ser adaptada a los procedimientos legales existentes. Durante el año 2020, los cambios producidos en el Poder Judicial estuvieron fuertemente vinculados con la digitalización de la justicia, la incorporación de la prueba digital para la resolución de casos, sean de ciberdelitos o no, ha debido irse modificando paulatinamente, y logrando una colaboración mancomunada entre la policía, fiscales, ayudantes de fiscales y jueces. Los tipos de pruebas electrónicas que se han incorporado son el correo electrónico, la imagen digital, la evidencia que se encuentra guardada en la nube, los datos que se encuentran en celulares y smartphones, datos de redes sociales, y datos de otros dispositivos como PC, Notebook, Netbook y Tablets.

En Mendoza, la prueba digital no ha sido incorporada en el Código Procesal Penal. El fiscal Santiago Garay, ha presentado un proyecto de modificación de dicho Código, en materia de cibercriminalidad y obtención de evidencia digital, que aún se ha aprobado. Esta

propuesta incluye la Convención de Budapest sobre ciberdelito, a la cual Argentina se encuentra adherida desde el año 2017, con la Ley N° 26.388, entendiendo que es necesario que esta normativa se encuentre en nuestro marco legal provincial. Siendo la incorporación de las pruebas electrónicas, un tema de gran interés para todas las partes que requieran la producción de pruebas para sus causas, sería de gran valor que dicho proyecto pudiera ser concretado. Sin embargo, y a pesar de esta falta de normativa legal provincial, los miembros del Poder Judicial, utilizan la producción de pruebas digitales que emergen de la investigación policial, y las valoran para el esclarecimiento de hechos delictivos y su posterior juzgamiento.

En el caso de análisis que hemos presentado, podemos observar cómo, a partir del seguimiento de las cámaras de seguridad, hemos podido reconstruir los pasos de la menor, lo que conjugado con datos provenientes de la utilización de su tarjeta SUBE, y la cámara de seguridad del colectivo que la menor utilizó para su traslado, se pudo identificar al autor del hecho. Posteriormente, y continuando con los datos aportados por cámaras de seguridad, pudo observarse el vehículo utilizado para desprenderse del cadáver. Por otro lado, desde el teléfono de la víctima, se obtuvo más información que permitió identificar chats entre ambos, mediante la utilización de Instagram, en los que el femicida había logrado convencerla de ir a su vivienda para encontrarse. De igual manera, como bien lo han mencionado los entrevistados, las cámaras de seguridad han aportado datos indiscutibles para casos en los que se han producido muertes, facilitando la identificación de los delincuentes, y a su vez, pudiendo encontrar los datos que permiten identificar el *modus operandi* de estos hechos delictivos.

De esta forma podemos inferir que la prueba digital representa una herramienta de gran importancia, puesto que permite reconstruir en un paso a paso, muchos comportamientos de quienes han realizado un delito. El observar las cámaras ubicadas en diferentes arterias, permite reconstruir el recorrido del delincuente y lograr dar con su ubicación, o al menos, comenzar a buscar a partir de la última imagen que se pudo obtener de su proceder. Esto, contribuye con otras áreas policiales, en la búsqueda y posterior esclarecimiento del hecho, para entregar pruebas contundentes a la fiscalía, que permitan juzgar y condenar al autor o autores del mismo. Podemos sostener que la prueba digital,

como han mencionado autores como Granero (2019), Pérez Cascella (2017), entre otros doctrinarios, y el artículo 319 del CCCN, cuenta con su valor probatorio, en tanto aporta al conocimiento y claridad al hecho narrado, siempre constatando la veracidad de "los soportes utilizados y de los procedimientos técnicos que se apliquen" (Art. 319, CCCN). Y, en este sentido, como ha quedado demostrado por el proceder de los profesionales del DATAI, la preservación, manipulación y análisis de la prueba digital, mediante la aplicación de herramientas tecnológicas adecuadas, resulta invalorable para esclarecer delitos.

Para realizar esta investigación, nos planteamos las siguientes hipótesis:

- La falta de un protocolo de recolección de evidencia digital establecido normativamente en la Provincia de Mendoza, provoca dificultades en la elaboración de informes técnicos presentados por el Departamento de Asistencia Tecnológica y Apoyo Investigativo, en causas penales ante el Poder Judicial, en los años 2019 al 2021.
- El aumento de la obtención de datos en dispositivos electrónicos, acrecienta la complejidad y calidad de la presentación de informes técnicos por parte del Departamento de Asistencia Tecnológica y Apoyo Investigativo perteneciente a la Dirección de Investigaciones, por lo tanto es necesario cumplir con los procedimientos adecuados para la obtención y preservación de las pruebas, a fin de que las mismas, puedan ser utilizadas como evidencia digital fehaciente, tal como ha quedado comprobado en los casos citados y en el reconocimiento de los entrevistados.

Como se ha podido observar a lo largo del presente trabajo, la primera hipótesis no ha podido ser comprobada, ya que los informes realizados por el DATAI, han contribuido exitosamente a la resolución de casos complejos, en los que las pruebas físicas resultaban insuficientes para dar con los autores de los hechos delictivos. Esto significa, que a pesar de no existir un protocolo de recolección de evidencia digital propio de la institución o de la provincia, el personal policial, a partir de sus conocimientos, experiencia y compromiso con el trabajo cotidiano, alcanza resultados positivos útiles para el desarrollo pleno de la justicia.

La segunda hipótesis, refleja que la complejidad de la prueba, su obtención, su custodia y, consecuentemente su análisis forense, requiere de informes técnicos altamente complejos, los cuales pueden ser realizados por el personal del DATAI, ya que estos cuentan con la experiencia, y la idoneidad en la materia, tanto como para la recolección, el resguardo y protección y el posterior análisis de la prueba digital, lo que les permite elaborar informes útiles para la justicia de Mendoza.

Aportes a la Seguridad Pública

Consideramos, al igual que nuestros entrevistados, que la creación de un manual de procedimientos común a todos, y posteriormente, un protocolo de actuación en relación a la preservación de la prueba, se convertiría en una gran herramienta procedimental en la cual todos podríamos apoyarnos, sobre todo optimizando recursos y trabajando en forma mancomunada. Este punto es importante ya que contar con una herramienta común a todos, facilitará que el personal se perfeccione en la adquisición de conocimientos.

En referencia a los conocimientos, entendemos que es necesario que la Policía de Mendoza cuente con acceso a la formación tecnológica, especialmente en pruebas digitales. El personal policial ha aprendido con la experiencia, con el trabajo cotidiano y con la búsqueda personal de herramientas que pueden ser adquiridas por instituciones gubernamentales. Si bien algunas de ellas son gratuitas y podemos acceder con facilidad, debemos aprender su funcionamiento, conocer sus componentes e internarnos en búsquedas investigativas cada vez más profundas. Muchos de estos conocimientos los hemos adquirido de la experiencia de la Policía Federal, la cual brinda capacitaciones a policías del interior del país. Además, la asistencia a congresos y charlas, ha permitido adquirir nuevos conocimiento, o perfeccionar otros, a partir de compartir experiencias con idóneos e incluso ingenieros o peritos informáticos. En este punto, creemos que sería de gran ayuda la creación de un espacio de aprendizaje y perfeccionamiento, dentro del IUSP, como por ejemplo una Diplomatura y posteriormente una Maestría, las cuales además, otorgarán un mayor crecimiento a nuestra importante institución universitaria.

Por último, y no menos importante, creemos que en nuestros espacios laborales, construir equipos interdisciplinarios en los cuales confluyan diferentes disciplinas, podrá

contribuir a optimizar una institución que es encuentra en pleno crecimiento. Aportes provenientes de la ingeniería informática y la ingeniería en sistemas, permitirán no solo aprender a manejar nuevas y más complejas herramientas, sino también a crear softwares propios que puedan ser puestos al servicio del DATAI. La incorporación de profesionales de la psicología, puede contribuir a elaborar perfiles delictivos, que nos faciliten la búsqueda, pero sobre todo, y en esto consideramos de una gran importancia su aporte, podrían acompañar a profesionales que deban procesar datos de imágenes en los cuales se investiguen delitos de pornografía infantil o abuso de menores. En este último punto, es importante destacar que el profesional que debe enfrentarse a este hecho, debe mantener su trabajo técnico alejado lo más alejado posible de sus emociones, las que naturalmente fluirán frente a hechos aberrantes de esta naturaleza.

Por último, queremos destacar que nuestra función en esta institución, nos llena de orgullo en tanto somos partícipes la construcción del DATAI desde su génesis, y poder ver el enorme crecimiento que ha tenido, como también saber que hemos sido parte del mismo, resulta de un gran valor como profesionales de la Seguridad Pública.

ANEXOS

ANEXO I

DEPARTAMENTO DE ASISTENCIA TECNOLOGICA Y APOYO INVESTIGATIGO DATAI (9248)

El Departamento de Asistencia Tecnológica y Apoyo Investigativo, dependiente del sub jefe de Policía en Función Judicial.

El cargo de Jefe del DATAI, será ejercido por un Oficial Jefe P.P. en servicio efectivo de las Policías de la Provincia de Mendoza.

La función específica del Jefe del DATAI, será la de coordinar y controlar funcionalmente las actividades operativas y administrativas llevadas a cabo por las Divisiones Análisis Criminal, Delitos Tecnológicos y Escuchas Telefónicas y Antisecuestros. Deberá procurar una actuación mancomunada en aquellos delitos que involucren alguna de las Divisiones mencionadas y que en el marco de las investigaciones sean requeridos.

Asimismo tendrá a su cargo todo tipo de coordinación con las autoridades del Poder Judicial y Ministerio Público Fiscal a fin de implementar y/o mejorar los distintos procedimientos que involucren tanto a dependencias judiciales como de la Dirección Investigaciones.

Deberá mantener informado en forma permanente a la Jefatura de Policía en Función Judicial sobre el avance de las intervenciones en que se vean involucradas las Divisiones a su mando.

Gestionar recursos de acuerdo a los avances tecnológicos, ante la Dirección y autoridades ministeriales que correspondan.

Coordinar intercambios con instituciones externas que sirvan de apoyo a la investigación criminal.

DIVISION ANALISIS CRIMINAL (620)

La División Análisis Criminal, dependerá del DATAI.

La Jefatura de la División Análisis Criminal, será desempeñada por un Oficial Jefe P.P. en servicio efectivo de las Policías de la Provincia de Mendoza.

La función específica de la Jefatura de la División Análisis Criminal será, dirigir, coordinar y controlar las actividades de reunión y análisis de información correspondiente al ámbito delictivo. Deberá mantener una guardia cuya función será recabar toda la información registrada al nivel de la Policía en Función Judicial, tanto de hechos delictuales, medidas investigativas desarrolladas e identificación de personas a través de los programas existentes, información que una vez reunía será transmitida a conocimiento de la Superioridad y de demás unidades especializadas.

Mantendrá la actualización constante de todas las bases de datos con la finalidad de producir la inteligencia adecuada a fin de realizar una persecución del delito, determinar nuevos modus operandis delictuales contrarrestando la ejecución de acciones delictivas, debiendo efectuar su difusión a los organismos pertinentes.

Bajo su directa dependencia, estarán la sistematización de datos e información territorial, que consiste en la actualización diaria y permanente de los registros y verificación de detenidos que sean identificados por la División judiciales, manteniendo la permanente actualización de las bases desarrolladas. El Análisis – Gestión de Sistemas, consistente en confección de partes de novedades agregar igual e identificación de personas. En tanto que el Centro Integrador de Análisis Tecnológico CIAT tiene como función la visualización y análisis de cámaras del CEO el desarrollo de pericias producto de la extracción de información de dispositivos tecnológicos, todo ello en apoyo de las unidades especiales que dirigen la investigación. Monitoreo de redes sociales y sistemas de comunicación con la finalidad de advertir la comisión de hechos delictivos.

DIVISION DELITOS TECNOLOGICOS (6561)

La División Análisis Criminal, dependerá del DATAI.

La Jefatura de la División Delitos Tecnológicos será desempeñada por un Oficial Jefe P.P. en servicio efectivo de las Policías de la Provincia de Mendoza.

La función específica de la División Delitos Tecnológicos será la intervención investigativa con realización de pericias en sistemas informáticos o electrónicos y el análisis de pruebas obtenidas en hechos delictivos. Efectuará la elaboración de fotogramas y todo lo relacionado a grabaciones en video.

Asimismo el mantenimiento de las bases de datos propias de la Jefatura de Policía en función Judicial TESSA y otras.

Extracción de información de dispositivos informáticos y tecnológicos y su posterior análisis del resultado obtenido. Tareas que se hacen en apoyo de las unidades especiales que dirigen la investigación e investigaciones propias respecto de delitos tecnológicos (grooming, pornografía infantil).

DIVISION ESCUCHAS TELEFONICAS Y ANTISECUESTROS (8069)

La División Análisis Criminal, dependerá del DATAI.

La Jefatura de la División Escuchas Telefónicas y Antisecuestros, será desempeñada por un Oficial Jefe P.P. en servicio efectivo de las Policías de la Provincia de Mendoza.

La función específica de esta División Escuchas Telefónicas y Antisecuestros, será la gestión de oficios judiciales, relacionados a intervenciones telefónicas, escuchas telefónicas, transcripción mecanográfica, confección de master (comunicaciones de interés), escuchas directas en tiempo real, análisis de planillas de registro de comunicación a través de software adaptado, análisis de información, trascripciones de audio vinculados a expedientes investigados.

a) utilización de software que permitan la comparación forense de voces.

b) Tendrá la participación tanto operativa como administrativa directa e inmediata en aquellos delitos en que se registre la privación ilegítima de la libertad de una persona con

fines extorsivos, quedando a disposición del Juzgado Federal interviniente y para lo cual coordinará con la Autoridad Judicial y policial los pasos a seguir en forma inmediata.

ANEXO II

CASO FEMICIDIO

Fxxx: termina el caso que sacudió a toda una provincia

Este jueves por la tarde el caso Rxxxx (14) tendrá un final provisorio, cuando la Justicia confirme el proceso abreviado contra Pablo Arancibia. El sujeto está acusado de engañar y asesinar a la chica, a la que luego arrojó en una zona aislada alegando que "era un perro atropellado".

FACUNDO GARCÍA

fgarcia@mdzol.com

JUEVES, 8 DE JULIO DE 2021 · 09:05

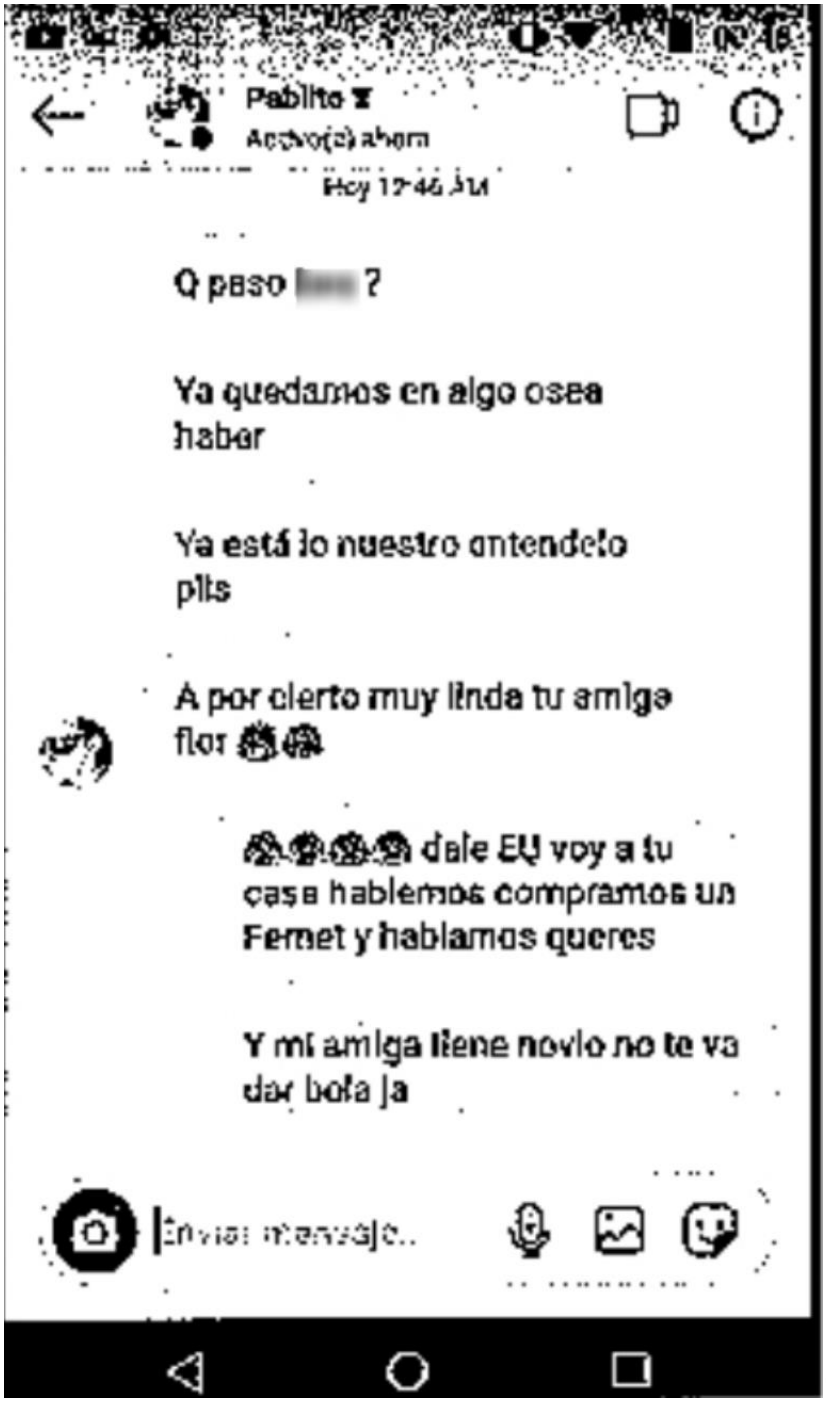
El femicidio de R**xxxx (14)** fue uno de los tristes hitos del 2020, al punto de generar las **movilizaciones** más importantes que registró la provincia el año pasado. Este jueves el caso tendrá un cierre, aunque sea desde el punto de vista jurídico: cerca de las 15, **Pablo Arancibia (33)** firmará un acuerdo de **juicio abreviado** para no exponerse al debate oral y a un jurado. Y será condenado a **prisión perpetua**.

Los padres de la víctima han pedido estar en Tribunales porque **quieren decir algunas palabras** si finalmente se confirma el acuerdo, que debe ser ratificado por el juez tras obtener la venia de la defensa y la fiscalía. Los acompañarán los abogados de la familia, **Cristian Vaira Leyton y Agustín Magdalena**, quienes vienen siguiendo de cerca el proceso desde un principio.

Es imposible analizar el caso sin tomar en consideración la **reacción popular** que generó la muerte de la adolescente. En Mendoza hubo marchas, incidentes y un gran cuestionamiento sobre **el rol del Estado ante la violencia machista**, puesto que se comprobó que alguien pidió ayuda al 911 al escuchar que Rxxxx pedía auxilio, pero **no se envió un móvil** a pesar de que había una comisaría a pocas cuadras del lugar.

Al acecho

El crimen se produjo el **12 de diciembre**, en el pasaje xxx. La investigación posterior demostraría que Arancibia no solamente chateaba con adolescentes aprovechando su máscara de **"adulto compinche"** sino que acechaba a Rxxx desde antes. En efecto, los **chats entre Arancibia y una amiga de Rxxx** así lo demuestran:



"MUY LINDA TU AMIGA Rxxxxxx", ESCRIBIÓ ARANCIBIA ANTES DEL CRIMEN.

El femicida invitó a Rxxxx **a su casa**. La nena se tomó un colectivo diciéndole a su familia que iba a lo de una amiga y el momento en el que se bajó en Gxxxx, su último destino, **quedó grabado** en la cámara de un ómnibus del Grupo xx alrededor del mediodía:

Fxxx BAJANDO DEL COLECTIVO, EN HORAS DEL MEDIODÍA.

Arancibia fue a buscarla y se encontraron. A lo largo de aquella última tarde **serían varios los vecinos** que los vieron. Alguno pensó que se trataba de una sobrina o algo así, ya que Fxxx era muy menuda: **pesaba apenas 35**

kilos.

ARANCIBIA YENDO A ENCONTRARSE CON Fxxx.

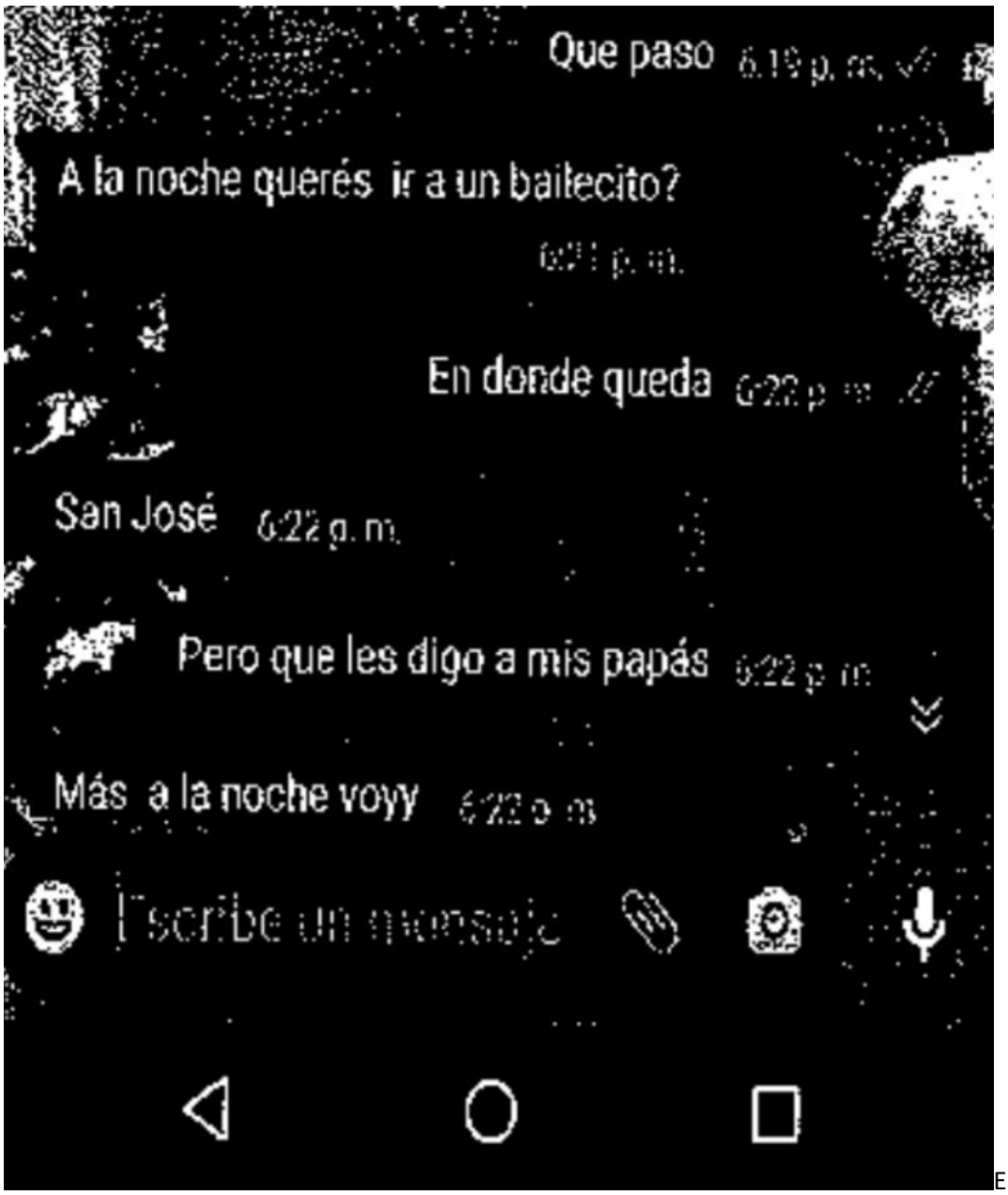
EL CALLEJÓN, DONDE TUVO LUGAR EL FEMICIDIO.

Tarde fatal

Sólo Arancibia sabe de qué conversaron durante tantas horas con Fxxx en su casa. Aparentemente, la menor estaba confiada, porque publicó un estado de WhatsApp donde afirmaba estar **"con el tío más piola"**.

PABLO ARANCIBIA, EL IMPUTADO.

Es más, la muchacha chateó con una amiga **a sólo 40 minutos de que Arancibia la matara a golpes**. Lejos de parecer preocupada, la invitó a **"un bailecito"** que en teoría iba a haber esa noche. Eran las 18:20. A las 18:58, un vecino escuchó a **"una voz suave" que pedía auxilio**.



EL CHAT DE Fxxx CON UNA AMIGA, A MINUTOS DE SER ASESINADA.

Eran las últimas palabras de **Fxxx**, que recibió una andanada de **puñetazos** que le propinó Arancibia, quien además la estranguló aprovechándose de la contextura de la pequeña. El vecino que escuchó los gritos llamó al 911 pero **nunca hubo respuesta**.

Como un perro

Uno de los rasgos característicos de los crímenes de odio es que incluyen la **cosificación de la víctima**. Se la deshumaniza. Es exactamente lo que hizo Arancibia. **Degolló a la joven y quemó su cuerpo** en una cañería séptica, probablemente para borrar evidencias. Luego llamó a un amigo

diciéndole que precisaba ayuda para que lo llevara en un vehículo. Relató que quería **"tirar por ahí a un perro que había atropellado un auto"**.

Hasta se quejó de la **falta de empatía** de la gente, que mata animales en la vía pública y los deja agonizando. El amigo llegó con su coche y vio cómo, en las inmediaciones de **un matadero** ubicado en calle Alsina (Maipú), Arancibia descargaba **un bulto envuelto en cortinas** y lo arrojaba a un costado. Recapitular las horas siguientes causa estupor e indignación. Arancibia **asistió a un asado, jugó algunas horas a la "play", y más tarde pidió que volvieran a trasladarlo al sitio donde había descartado el cuerpo** de la niña. Sus allegados, desde luego, nada sabían del horror que había cometido. Los testigos que estaban con él cuentan que se bajó del vehículo **"como desesperado"**, se asomó al canal donde estaba el cadáver y dijo "vamos, vamos, ya se lo están comiendo los perros".

En su oportunidad, la **fiscal Claudia Ríos** detectó uno por uno estos detalles, así como otros que demuestran la total **falta de respeto por la humanidad** de Flor que tuvo Arancibia. La instrucción y los aportes de la querella fueron tan contundentes que al imputado le quedan pocas chances más que **admitir el femicidio y enfrentar la máxima pena** que prevé el Código Penal.

LA FISCAL CLAUDIA RÍOS EL DÍA EN QUE Fxxx FUE ENCONTRADA.

Miles de mujeres movilizadas

Y está la **historia colectiva**. Porque hubo algo en el caso Fxxx que funcionó como detonante. Incluso antes de que se hallara el cadáver, **miles de mujeres de la provincia se movilizaron** en varios departamentos. La indignación fue tal, que hasta **fueron incendiadas la Legislatura y la Casa de Gobierno**. Los videos de lo ocurrido recorrieron el país.

ASÍ QUEDÓ LA LEGISLATURA MENDOCINA.

Es verdad: Fxxxx fue asesinada y eso no tiene vuelta. Pero ahora mismo hay **millones de nenas en las redes** conversando con extraños. Sería esperable que no se repita la cadena de fallos individuales e **institucionales** que condujeron a su muerte.

ANEXO III

Guía de entrevistas

1. **Edad**
2. **Cargo que ocupa**
3. **¿Desde cuándo trabaja en esta División?**
4. **¿Qué tipo de capacitación ha recibido para trabajar en esta División?**
5. **¿Cuál es la relación que tienen con el Poder Judicial?**
6. **¿Cómo es la Cadena de Custodia?**
7. **¿De qué dispositivos obtienen la información?**
8. **¿Cómo se realiza el resguardo de la misma?**
9. **¿Puede referir alguna intervención significativa?**
10. **¿Cómo es la relación entre las áreas de Escuchas Telefónicas, División de Análisis Criminal, y el Centro de Análisis de Imágenes en Vivo?**
11. **¿Cuál es la función del perito informático y la del idóneo informático?**
12. **¿Considera que es necesario generar guías procedimentales o protocolos para la actuación de las áreas en general o de cada área en particular?**
13. **¿Cómo ve el futuro del DATAI en la Policía de Mendoza?**
14. **¿Qué puede aconsejar como medidas preventivas en función de la ciberseguridad?**

ANEXO IV

ENTREVISTAS

Entrevista N° 1

Oficial principal Federico Ponce. Subjefe de División Delitos Tecnológicos

Edad: 40 años

¿Cuánto hace que está en la dependencia?

En el área de tecnología estoy hace 12 años. Estuve en la División Escuchas Telefónicas, en la División Antisecuestros Extorsivos y posteriormente aquí.

¿Cuenta entonces con más de 10 años de experiencia?

Si hace más de 10 años, en los temas relacionados a tecnología , dispositivos electrónicos, comunicaciones. Tengo una idea respecto a todo lo que serían ese tipo de elementos de comunicación. Ahora nos estamos adentrando a lo que es la parte de tecnología

¿Cuál es su capacitación para estos cargos?

He hecho 2 cursos de antisecuestros extorsivos. He estado en Comisiones en reiteradas oportunidades en la Ciudad Autónoma de Buenos Aires, visitando el Departamento de Tecnología Aplicada de la Policía Federal. Siempre estamos en contacto y transmitiéndonos los conocimientos y experiencias. Tengo un curso de Office, aunque es viejo, pero desde que nací estuve, en un principio, en contacto con la tecnología y con internet. Tengo una idea aproximada de todo esto.

¿Qué herramientas manejas?

Gracias a estos intercambios de conocimientos que hacemos con el Departamento de Tecnología Aplicada de la Policía Federal, el subcomisario Marcelo Wanes tuvo la oportunidad de enseñarme en una Comisión que estuve casi un mes, la herramienta I-2 y fui uno de los primeros en conocer la herramienta y el encargado de tratar de enseñar y explicarle a personal de escuchas telefónicas, de análisis criminal, de delitos económicos, tratar de transmitir un poco este conocimiento, Es algo innovador y se relaciona con aquellas que humanamente, no se puede establecer ya que existen múltiples ramificaciones e interrelaciones, hasta incluso causas.

¿El software hace interrelaciones con una gran cantidad de información? ¿Lo que se podría decir la big data?

Si algo similar.

¿Cómo ve Delitos Tecnológicos, esta idea del cibercrimen, del ciberdelito? ¿Cómo se interrelaciona con otros delitos que no son tan puros, digamos como es un hacking o un phishing, respecto a un homicidio? ¿Cómo ve la policía todo ese proceso como delitos tecnológicos?

Mira lo que entiendo de la División Cibercrimen, es una División que está a conformarse, es una División que va a tratar estos delitos netamente informáticos, hasta el momento lo estamos abarcando nosotros.

¿Hay una intervención?

La intervención proviene de la tecnología, la cual en cualquier investigación es como decimos, transversal, porque en todas las investigaciones se encuentra como una gran herramienta la tecnología. Y mucho más hoy, que las herramientas tecnológicas que podemos obtener y de los avances investigativos que orientan la investigación, en cuanto a colaboración, en cuanto a la identificación, en cuanto a lograr la ubicación aproximada del autor del hecho.

¿Cómo es esa intervención policial en el proceso judicial? ¿Cómo llegan ustedes a colaborar o a trabajar mancomunadamente con el fiscal?

La novedad generalmente surge vía frecuencia policial, vía el CEO, nosotros cobramos conocimientos, somos desplazados al lugar ante un ilícito. En el lugar depende del hecho, de la gravedad del hecho, concurre el fiscal o el ayudante fiscal, nosotros entrevistamos al fiscal o al ayudante fiscal, y empezamos con nuestra labor de identificación del material informático que colabora con la investigación, el cual generalmente es un DVR, es una computadora, y hacemos un barrido de cámaras, teniendo en cuenta el hecho puntual, observando las cámaras más cercanas que se encuentran al mismo, con el objeto de visualizar lo que las cámaras aportan y poder colaborar con la investigación.

Es importante recalcar que la primera intervención que nosotros hacemos es autorizada por el fiscal o ayudante fiscal, en cuanto a la identificación de las cámaras que intervienen en el perímetro o en el lugar del hecho, pedimos oficio, porque nosotros siempre actuamos bajo requerimiento judicial. Lo primero que hacemos es la identificación que abarca la parte de reconocimiento, la parte de extracción de información cuando nos apersonamos al lugar, mantenemos un diálogo con el morador, se le presenta el oficio judicial que nos avala. En algunos casos nos hacemos presentes con el fiscal o ayudante fiscal que nos permite el ingreso, identificamos el DVR que poseen las cámaras y procedemos a la extracción de los datos que se requieren para la investigación.

Una vez que hacemos esta extracción, se labra la correspondiente acta en presencia de testigos y morador, donde se deja constancia del tipo de DVR, la marca, el número de

serie, el desfasaje que posee el mismo, y se procede a la extracción. Con el desfasaje me refiero a que en algunas oportunidades los DVR se encuentran desfasados en sus horarios, días, años, minutos, entonces constatamos ese tipo de desfasaje para que después, cuando se analice, nosotros tengamos una orientación en tiempo real de cada una de las imágenes. Una vez que se procede a la extracción de ese material, es remitido a la División, a nuestra base, a donde se procede el análisis dela información. En el mismo nos fijamos el horario estimado del hecho a investigar, se visualiza una hora para atrás, una hora para adelante, y se tiene mucha atención respecto a la información que se tiene de calles y testigos.

Cuando el material ya está en base, cuando hacemos el análisis del material, se tiene en cuenta lo mencionado, para ver el contexto del hecho, y se comienza a analizar cada una de las imágenes, se realizan fotogramas q consideramos de interés, y en ellos se realiza la explicación del movimiento de las personas o aquellos datos que consideramos importantes para la causa, por ejemplo una moto, un vehículo, o la acción que está llevando a cabo cada una de las personas. Una vez que terminamos ese informe, se agrega al acta de extracción que se llevó a cabo en el lugar de la extracción fílmica, y es enviada a las oficinas fiscales.

Esa acta que ustedes labran en el lugar, que se firma por testigos, moradores y demás, ¿funcionaría como una especie de cadena de custodia?

Exacto, exacto. La finalidad que procura el personal de la División de Delitos Tecnológicos, es la de proteger el material, y resguardarlo de alguna manera. Me estoy acordando que me salté una parte: cuando hacemos la extracción, cuando terminamos se realiza un HASH que es un algoritmo que le brinda autenticidad y seguridad a lo que estamos extrayendo y es firmado también por el personal actuante, testigo y morador.

Una vez que el material llega y hacen esa cadena de custodia, y ¿el posterior análisis se plasma en un informe el cual es enviado nuevamente a la fiscalía?

Exacto, exacto. El material una vez que llega acá, es resguardado en soporte digital tipo DVD, con su correspondiente HASH, y es resguardado en esta base. Y se encuentra a requerimiento de las unidades fiscales.

¿Por qué en DVD y no en otro tipo de soporte?

Generalmente se realiza en DVD, pero también lo guardamos en otras ocasiones, teniendo en cuenta la gran cantidad de información a resguardar, se resguarda en discos rígidos portátiles, en discos rígidos, se guardan en pendrive aportados por las Unidades Fiscales. Eso depende de la consideración que se tenga, teniendo en cuenta la cantidad de información a resguardar.

Esto que me comentas es cuando es un delito, en el cual la tecnología es utilizada como medio para obtener la prueba en un proceso judicial. ¿Son los únicos dispositivos donde se obtiene una prueba para un proceso judicial? ¿Sólo cámaras de seguridad?

O también intervienen con teléfonos celulares? Por ejemplos en una investigación sobre una estafa, o el delito de grooming que es muy conocido. En esos tipos de delitos, más puros, ¿tienen intervención?

Si, como te decía recién, respecto al delito de groming, procedemos a los secuestros de computadoras, equipos celulares para periciar, se realiza el análisis de extracción de información UFE, se realiza el geposicionamiento de Gmail o de cualquier tipo de herramienta que tenga configurado el equipo para localizarlo. Eso es lo que mayor cantidad de trabajo nos llega a la división.

¿El resguardo termina siendo igual? ¿Se hace un HASH para que esa prueba sea guardada la prueba digital?

Claro, por ejemplo en cuanto a una computadora, tenemos los peritos de partes que son citados a requerimiento de la Unidad Fiscal, desde la cual se labora un oficio aportándonos el secuestro, y autorizándonos a la apertura. Esto sería discos o PC, a los que se les hace una copia bit a bit o una copia de la obtención de información forense, le llamamos nosotros, a los discos, teniendo en cuenta que bajo ningún término se analiza el original, y tomamos la copia, la cual analizamos en búsqueda teniendo en cuenta siempre, los avances investigativos que se tienen respecto a la investigación particular. Que es lo que se busca en cada investigación. Por ejemplo hay un hecho en el cual se busca una estafa, y generalmente se busca una imagen o boleta que se esté adulterando, en ese tipo de investigaciones lo que buscamos son imágenes.

Me decías que se llamaba a los peritos de parte, ¿se entiende que hay que solicitar nuevamente al fiscal o a autoridad competente, una nueva autorización para introducirse de nuevo en los dispositivos a buscar información?

Tanto en la adquisición, como en el análisis, las Unidades Fiscales, citan a las partes. Por este motivo nosotros procedemos al secuestro, el cual queda en la base, se le da un turno a la Unidad Fiscal, al cual asiste el perito de parte y el querellante, y se explica cada uno de los pasos que se van a llevar a cabo para hacer esa copia bit a bit o esa investigación forense. Una vez que se tienen esos datos, se les da un nuevo turno y se procede a un nuevo análisis de la copia. Siempre protegiendo la copia, la materia prima, el disco original.

En referencia a que no se analiza el original, ¿me podrías explicar por qué?

No es que no se revisa, la prueba original en ciertas ocasiones sí se trabaja sobre ella. Ocurre que por regla general, y de buenas prácticas forenses, se hace un clonado bit a bit en caso que se pueda hacer, y se trabaja sobre un clon, a efectos de no adulterar el original. En el 90% de los casos sí se puede hacer un clonado del material a periciar, pero en los dispositivos electrónicos como smartphones, el clonado es imposible por su

arquitectura. Pero, como se puede realizar una adquisición parcial de la información, es esa la que se mantiene imperturbable. La utilización o no del soporte original, queda a criterio del experto que realice la medida, ya que dependiendo del tipo de material, será la técnica que se utilice.

En todos los casos, se lleva adelante una preservación del material adquirido y ese si puede ser replicado cuantas veces sea necesario, es decir para la defensa, para la querella etc.

Las dificultades se dan con el tipo de dispositivo, pero en líneas generales se extrae la mayor cantidad de información o datos de usuario que son lo importante

Esto significa que no hay una adquisición completa sino parcial, siempre teniendo en cuenta que toda adquisición está autorizada por un juez de garantías. En cada oficio judicial se explicita que tipo de extracción se debe realizar, la cual debe ser completa para su preservación y resguardo, ya que la herramienta no permite tantos modos de extracción limpia.

En una conversación, por ejemplo, no se busca solo un texto determinado, sino que se extrae completa y luego, en el análisis, se buscan las cuestiones relacionadas con el hecho investigado. En ocasiones esto sale explicitado en la orden judicial, pero en el 95% de los casos somos libres de buscar cualquier parte del material.

En todas las ocasiones la copia bit a bit lleva una firma de seguridad y autenticidad llamado HASH.

¿Han tenido alguna situación en la que haya tenido que venir directamente un fiscal a presenciar una medida? Ya sea por la gravedad del caso o por lo sensible de la información

Si si, nos ha tocado en la parte de análisis y en la parte de obtención de la información. Se me vienen varias causas, por ejemplo una de homicidio, o de Juzgado Federal. Un caso fue el del Dr. Dante Vera cuando se hizo presente, porque intervenimos en el análisis de la información que se había logrado obtener del teléfono del Dr. Vento, ahí se hizo la correspondiente acta, y se encontraba presente el perito defensor también, y se llevó a cabo el análisis en el que se explicaron cada uno de los pasos que se estaban ejecutando. Y esto se fue incorporando al informe.

¿Podríamos decir que las áreas, como el DATAI y la oficina Fiscal, trabajan en forma muy estrecha?

Exactamente, la relación que se tiene con las oficinas fiscales es casi permanente, ya que a través de nosotros, se logran obtener datos significantes que orientan o reorientan una investigación.

¿Esto genera que las directivas sean mucho más claras y que se pueda trabajar un poco mejor?

Exacto, así es. El mayor beneficio es que, a través de la comunicación telefónica se nos da la orden de realizar una medida, se deja una constancia, y se labra la correspondiente acta de la orden emanada por la autoridad competente, y se realiza la medida ordenada. Ante cualquier duda en un informe, nos llaman a la dependencia, y esto nos permite incorporar nuevo material, o ampliar informes que ya hemos hecho en el momento. Es muy fluido.

¿Cuál es la última participación de la División de Delitos Tecnológicos o de la policía en el proceso penal?

La última participación, para mí, del personal de la División de Delitos Tecnológicos es cuando se logra la sentencia del autor del hecho investigado. Somos citados a declarar y ahí, en ese momento explicamos las medidas que se han aplicado, lo que se ha logrado encontrar. Eso ya es en el juicio. De igual manera pasa con los juicios por jurado. Nosotros vamos y le explicamos en el juicio, al jurado, se le explica paso a paso, con palabras lo más sencillas que se puedan utilizar, para una mejor comprensión del jurado, cada uno de los procedimientos que se llevan a cabo y cuál es la interpretación o la hipótesis que se alcanza, teniendo en cuenta la información que se tiene.

¿Cómo ve hacia futuro, la División de Delitos Tecnológicos, contenida en este departamento DATAI? ¿Qué aportes o qué innovaciones pueden surgir?

Yo veo un futuro de cada vez mayor cantidad de intervenciones, en cuanto a cada una de las investigaciones. Veo un futuro en el cual Delitos Tecnológicos brinde cada vez más herramientas, y de más orientaciones respecto de los hechos investigados. Veo un delito tecnológico también con una carga importante respecto a lo que concierne al ciberdelito, al delito de grooming, de phishing. Veo un futuro muy prometedor en cuanto a cantidad de trabajo y beneficios que se le pueda brindar a cada hecho delictivo en particular.

¿Cómo es la relación entre las tres áreas tecnológicas más importantes en Dirección de investigaciones: Escuchas Telefónicas, División Análisis Criminal, y ahora la nueva central del Centro de Análisis de Imágenes en Vivo?

La relación es permanente. Se vincula la información, ya que los trabajos se entrelazan entre las divisiones, y es necesario atacar en conjunto la misma información para que, desde cada sector se aporte su trabajo idóneo. Lo que veo quizás, es como aporte a como estamos hoy. Si bien está la interrelación entre las 3 divisiones, el problema es estamos en el mismo edificio, pero no se encuentran contenidas en el mismo lugar. Considero que es necesario que algunas divisiones estén dentro de Delitos Tecnológicos, a

modo de no realizar, en algunas ocasiones, el mismo trabajo. O acatar el trabajo en conjunto de una sola vez, y dar un informe terminado, y no dar un informe de delitos tecnológicos, otro informe de delito criminal, otro informe de análisis de UFE o cámara y otro informe el personal que está haciendo extracciones UFE.

¿Qué puede aconsejar para la ciberseguridad en tanto medidas preventivas?

El mensaje es que protejamos nuestras contraseñas, que no utilicemos datos referidos a nuestra identificación como DNI, fecha de nacimiento, nombre de padre, de madre. Que utilicemos datos personales para las contraseñas. Poner doble corroboración de contraseña. Utilizar la asociación de líneas telefónicas a las aplicaciones, como por ejemplo al abrir Google, o a WhatsApp la huella digital. Ese tipo de herramientas.

Muchas gracias

Entrevista N° 2

Cristian Leal. Subayudante de la Policía de Mendoza, integrante de la División de Delitos Tecnológicos y del Departamento de Análisis Tecnológico y Apoyo Investigativo.

Edad 32 años

¿Cuál es tu función policial?

Hace 3 años que entré en la fuerza de seguridad de la Policía de Mendoza, después de vivir dos años en España mi intención era la de ingresar a la Policía de Mendoza, y lo logre.

¿Cuánto hace que estas en Delitos Tecnológicos?

Estoy desde el año 2019,

¿Cómo te incorporaste a la División?

Llegue a la guardia del Ministerio, hasta que salieron los traslados, me tocó estar en la guardia de Investigaciones y ahí, en su momento era el principal Carmona Mauricio, me entrevistó, y me dijo que quería tener una entrevista conmigo. Fui a su despacho, me hizo un cuestionario y a las 2 semanas me salió el traslado.

Al ser un efectivo nuevo, ¿no tenías ninguna preparación en el área tecnológica?

Al principio no tenía en claro cómo se trabajaba en la División, pero en los cursos que uno va haciendo por cuenta propia, incluso, te vas formando. Además, el trabajar con los compañeros, más que todo unirse a los que tienen más experiencia que vos, te va formando día a día para adquirir conocimientos en esta división.

¿Qué tareas desarrollas?

Hacemos labores casi de peritos, no siendo peritos somos idóneos en lo que realizamos, nos formamos en academias diarias, en las charlas que tenemos con los jefes, y eso son aprendizajes que uno los lleva a cabo.

¿Entiendo que se van preparando en la disciplina del cómputo forense?

En las academias solemos hablar de los pilares fundamentales que tenemos que tener a la hora de, por ejemplo, secuestrar algo sencillo como es un DVR que tiene que tener su precaución, su cadena de custodia, sus testigos, sus actas correspondientes, su oficio para poder llevar a cabo la medida.

Me nombraste pasos que están contenidos en esta disciplina en lo que es la preservación, la conservación, el análisis que posteriormente será lo que conforme el informe. ¿Qué tipo de informes son los que se crean?

Son informes tecnológicos

¿Cuál es la diferencia que ves entre un informe de un perito y un informe tecnológico?

En el informe tecnológico, nosotros plasmamos, por ejemplo, una secuencia de video en la que tenemos que buscar a algo o alguien, informamos lo que estamos visualizando. En cambio el informe que realiza un perito, es más detallista, y utiliza otros programas, en los cuales se ingresa mucho más en la parte técnica de algún tipo de dispositivo, por ejemplo, ya sea computadora, móvil, es mucho más técnico el trabajo. El informe tecnológico es más completo y permite describir lo que nosotros estamos llevando a cabo en la investigación.

¿Cómo ves la intervención de la División Delitos Tecnológicos en el proceso judicial? ¿Cómo arranca esa intervención?

Esa intervención, incluso puede arrancar en algo tan sencillo como lo que llevamos día a día que puede ser algún tipo de homicidio, en el que puede existir una cámara de seguridad que aporte datos para identificar al autor del hecho, en el cual lo primero que se buscan son las pruebas, o los indicios para llegar al autor de algún hecho delictivo y eso da una ayuda a la justicia, tal como nosotros somos auxiliares de la justicia, para poder brindarle las pruebas suficientes, y encontrar a los autores del hecho. Esto es lo que se viene haciendo en los homicidios, ya que gran parte la División Homicidios y la División de Delitos Tecnológicos están muy compenetradas, porque se pueden esclarecer muchos hechos, con tan solo hacer un relevamiento de cámaras en el tiempo justo, y lograr la extracción. En esto tenemos que tener en cuenta que se trata de un trabajo contra reloj el que nosotros hacemos.

¿Esas intervenciones son por *motus* propio o requieren de autorizaciones?

No. Si vamos a la parte estricta, se requiere un oficio. Pero para un relevamiento de cámaras no necesitamos un oficio. Es simplemente por el hecho de ir y aportar la mayor claridad a la oficina fiscal para que nos pueda aportar las herramientas necesarias, en este caso un oficio, para que nosotros poder ir y hacer la extracción de las cámaras.

¿El relevamiento de cámaras sigue una guía procedimental, hay un protocolo, o es una práctica común que ustedes realizan?

Un relevamiento de cámaras es una herramienta que permite extraer datos sobre un robo o sobre un homicidio, que parte de buscar las cámaras más cercanas, del lugar del

hecho, para poder observar, en primera instancia, cómo ocurre el hecho, y también observar hacia donde se van los autores del hecho, para hacer un seguimiento y dar con ellos.

¿Eso está plasmado en un manual que ustedes siguen? ¿O es a libre albedrío que lo hacen?

No, no no, hay un manual que tenemos que seguir, unos pasos, unos procedimientos el cual nos ayuda en el tipo de trabajo que nosotros hacemos.

Es una guía procedimental que han elaborado con el transcurso del tiempo en base a experiencias, no está homologada.

Es una práctica que, cuando yo llegué a esta división se hacía, y se sigue haciendo.

Es interesante por el modo o por el momento que ocupa dentro del cómputo forense, o de la disciplina de la informática forense, porque va un paso previo a la identificación esto. Imagino que se lleva una especie de orden al momento de hacerlo, o una especie de pasos.

Claro, en un hecho determinado se van a buscar los datos correspondientes a las cámaras cercanas al hecho, tanto sean las privadas como las que puede aportar el Ministerio de Seguridad que son las del CEO.

¿En eso tienen un margen de actuación?

Cuando nosotros hacemos un relevamiento y tenemos una cámara en particular, se lo damos a conocer a nuestros jefes para que ellos den aviso a la oficina fiscal, y así se puede generar un oficio de actuación, ya que las cámaras muchas veces son del sector privado, pero también hay que tener en cuenta, y esto se lo explicamos a los moradoras, que todas las cámaras que enfocan a la vía pública, hay una ley nacional, que regula la disponibilidad permanente para cuando sean solicitadas por una autoridad, sobre todo cuando hay un phishing.

¿Cuál sería la función del perito informático o del idóneo en informática forense?

La función del idóneo o técnico es la de esclarecer lo que se le está solicitando, aportando la mayor prueba posible, para llegar a la resolución del problema.

¿Qué es la prueba digital y cuáles son sus características?

La prueba digital es algo que se está usando desde hace tiempo atrás que aporta grandes evidencias al momento de esclarecer el hecho. Por ejemplo en el caso de la mujer que mató a su marido envenenado, tuvimos la prueba digital tan sencilla como buscar el historial de navegación en su teléfono, de la autora. Esta prueba digital adquiere una gran importancia en el hecho porque fue determinante.

En ese caso, ¿cómo fue la parte técnica, cómo se obtuvo la prueba?

Se solicitó secuestrar el teléfono celular de la imputada mediante un oficio autorizado por el fiscal y por el juez de garantías. En este proceso se debe tener un especial cuidado, no es cuestión de meterse en un teléfono y nadar en los datos porque hay información muy sensible y se puede borrar cualquier elemento que esté incluso en internet, un simple reinicio de un teléfono, lo puede borrar. Eso se debe tener en cuenta cuando se secuestra un teléfono y se manipula, saben que los resultados que pueden obtener son importantes. Lo que hacemos es colocar el dispositivo en modo avión, garantizando que no haya interferencias o itinerancia de datos móviles para que no se pueda borrar ningún elemento que pueda ser probatorio. Te explico el escenario ideal, lo correcto es secuestrar el aparato electrónico, y colocarlo en una jaula de faraday, esto corta cualquier tipo de comunicación externa del dispositivo, con lo cual no hay forma de enviar comandos remotos para blanquearlo o borrarlo.

En análisis de imágenes, ¿ustedes utilizan algún software?

Y Software, para utilizar el tratamiento de imagen, tenemos programas que permiten identificar si la dimensión de píxeles se puede regular de determinadas formas para ver o darle forma a una silueta. Son programas no fáciles de trabajar, son complejos, no son como en las películas que se ve en el primer zoom. Lleva mucho tiempo y muchas pruebas a la hora de ver y mejorar la imagen.

Ustedes han participados en hechos resonantes, la consulta es, en la medida que se pueda informar, porque ya sabemos que es información sensible, y que el fiscal puede aún estar trabajando en estos casos, ¿qué nos puede decir del caso Fxxx por ejemplo?

El caso Fxxxx fue muy resonante, fue una tarea contra reloj, porque teníamos que hacer un relevamiento de cámaras, y a medida que se hacen los relevamientos de cámara, se tienen que extraer y visualizar, intentar dar con la víctima y ver hacia donde se dirigió. Mientras tanto que estás visualizando una cámara se puede estar pisando otra, entonces es un trabajo contra reloj.

El caso del joven Jean Carlos Sosa Delgado, a quien mataron en la 4° sección con motivo de sustraerle su Ford Focus, se resolvió en 48 h. En este caso se trabajó con cámaras del CEO y de privados. Se buscó modus operandi en la zona. Se buscó la gente que estaba vinculada y esto nos permitió resolver rápidamente la causa.

El término “pisando” ¿a qué haces referencia?

Pisando hago referencia a que se van regrabando, digamos si un DVR, un sistema de grabación, tiene una semana de almacenamiento, cuando llega al octavo día, el primer día se va borrando, es decir que se pierde esa información. Sin embargo en este caso pudimos dar con buenas cámaras de seguridad, tanto privadas como del Estado, en la cual

pudimos lograr dar con Fxxxx, y pudimos encaminar los pasos que realizó, y ls pasos que realizó también el imputado, para poder aportar las pruebas necesarias a la Unidad Fiscal de Homicidios, y poder aportar los pasos que dio el imputado también que fueron el indicio de que él fue la última persona que estuvo con Fxxxx.

En los últimos días se ha propuesto una relación propiciada por tu jefe de Delitos Tecnológicos, por el jefe de División de Análisis Criminal y por el Jefe de la División de escuchas telefónicas, en tanto a la interrelación de las tres áreas, y una cuarta área relacionada a la visualización de imágenes en vivo. ¿Cómo ves esa relación en materia de avances en la tecnología?

Esa relación la veo como una gran optimización de los tiempos de los efectivos que están trabajando bajo sus órdenes, porque al haber una unificación, todo se simplifica y se puede hablar el mismo idioma y sabemos lo que estamos buscando todos al mismo tiempo. Lo veo muy bien, ya que tendríamos la posibilidad de visualizar cámaras en vivo del CEO, que si tenemos que extraer algo se extrae. Esto antes era más complejo ya que teníamos que solicitar el oficio para que sea remitido al CEO, por ejemplo si es una cámara de Maipú, y ahí que Maipú remita las cámaras para poder visualizarlo. Ahí se pierde mucho tiempo ya que, a lo mejor, encontramos algo en una cámara del CEO, y cuando vamos a buscar la cámara particular es posible que no tenga el dato ya que puede estar pisada, como expliqué antes.

¿Crees que es necesario ir generando guías procedimentales, o algunos protocolos respecto a la actuación de las áreas en general o solo de tu área?

Estaría muy bien, ya que si vamos a trabajar en conjunto sería muy bueno que cada área conozca el protocolo general que conlleva al conjunto de las áreas. Sí, estaría bien que hubiera un protocolo de actuación en la que las 3 áreas sepan cómo se actúa. También sé que no todas las áreas hacen el mismo trabajo y también es posible que puedan decir que cada una tenga su propio protocolo, pero estaría bueno que se conozcan entre sí los protocolos que tienen para poder optimizar los recursos que tienen.

Algo que quieras aportar desde tu experiencia

Yo llevo poco tiempo y me queda mucho por aprender, pero sí es necesario tener mayores recursos materiales a la hora de realizar labores.

Muchas gracias

Entrevista N°3

Carlos Pérez efectivo de la División de Delitos Tecnológicos

¿Cómo llego a esta división?

Yo soy Auxiliar Primero de la Policía de Mendoza, hace 12 años que he egresado, me he instruido dentro del Instituto Universitario de Seguridad Pública, donde me recibí como auxiliar. Mis primeros destinos fueron en la prevención en Seguridad Pública, trabajé en el parque, motorizada, unidades que existen y otras que no. Después de 4 años fui seleccionado por el Jefe Oficial Principal, Carmona, Mauricio de la División de Delitos Tecnológicos, quien me propuso ir a conformar el equipo de trabajo que él estaba armando, cuando esto recién iniciaba la división.

¿Cómo ve la policía en relación a ciberseguridad o al cibercrimen?

Muy interesante la pregunta porque considero que…, yo lo voy a denominar de ahora en más como cibercrimen. Si bien hay acepciones que pueden ser distintas, dentro de División Delitos Tecnológicos, creo que todos tenemos una misma mirada y hablamos de cibercrimen o cibercriminalidad. Esto es a efectos de que abarque todos los tipos de delitos cometidos, tanto como medio como objeto.

¿Cómo veo la policía respecto a esto?, indudablemente con estos dos años de pandemia se incrementaron considerablemente los ciberdelitos, e incrementaron tanto en materia de delitos puros como son el hacking, phishing, la sextorsión, a veces hemos tenido la pornovenganza, delitos de grooming, también la tecnología como medio para cometer otros delitos como son por ejemplo el robo, la estafa, los homicidios en época de pandemia, se incrementaron, no quiero mentir pero en un 50, 60%.

¿Cómo interviene la policía en el proceso judicial?

La intervención siempre es a raíz del requerimiento, pero entendiendo que el delito primero es denunciado o alertado por el fiscal, con el Poder Judicial, y comienza la investigación. Nosotros como policía, en función judicial, prestamos la colaboración al Poder Judicial en materia de investigación. Al tener una muy buena relación, en este caso División Delitos Tecnológicos y el DATAI tiene buena relación con el Poder judicial, creo que es necesario que esa relación sea fluida, ya que esa intervención que tenemos en el proceso penal, es dinámico, es rápido y expeditivo. Y esto, ¿por qué es importante? , desde mi experiencia puedo decir que es importante porque la prueba digital, o los dispositivos electrónicos que contienen la prueba digital, son volátiles, con lo cual hay tiempos perentorios, que no los marca ni siquiera el proceso judicial, sino que los marcan las propias características del dispositivo electrónico que contenga esa evidencia digital. Por eso creo que esa intervención, que tiene División de Delitos Tecnológicos en el proceso

judicial, tiene que ir de la mano con la relación que tenga con el Poder Judicial. Mientras más expeditiva sea la acción, será más concreto el resultado.

¿Qué formación posee para realizar esta actividad?

Desde que ingresé se han realizado diversas capacitaciones, en lo referido al cibercrimen. En Rosario fuimos a un Congreso de una semana completa, donde se recibió información sobre lo que es cibercrimen, cómo utilizar la evidencia digital en el proceso penal, como se tiene que trabajar con la evidencia digital, lo que es cadena de custodia. También hicimos cursos en San Rafael, donde hemos recibido la misma temática respecto a cómo es la investigación o cuál es la función de la policía en una investigación criminal. Fuimos a un Congreso en Córdoba en el cual estudiamos conceptos como la Deep Web y la Dark Web, los que son lugares que hasta el momento, gracias a Dios aquí en Mendoza no se han visto, o por lo menos no se han detectado casos en donde se cometan delitos en esos espacios, pero son espacios que son terribles porque están sin control, prácticamente, y es muy difícil para la policía llegar a esos espacios de búsqueda, y detectar ese tipo de delitos, toda vez que se trabaja con encriptaciones, trabajan con IP camufladas. Este ciberespacio cuenta con ciertas características especiales en donde una de ellas es el anonimato, ya que cualquier persona en el ciberespacio puede hacer uso de ella, tanto como se puede mostrar tal cual es, los ciberdelincuentes no van a andar mostrándose tal cual son. Un grumer por ejemplo nunca muestra sus facetas ya que estas se camuflan. Y es justamente una de las características que tiene el ciberespacio que es que el anonimato es su frutilla en el postre. Por eso es tan difícil detectarlos, y llevarlos a la cárcel.

¿Cuál es la función de un perito o idóneo en informática forense?

La función de un perito, considero yo que, a diferencia de la función que cumple hoy un idóneo, en informática forense, primero está dado por la certificación. Hasta hace poco no existían carreras en Mendoza, ya que sólo existe en Buenos Aires la que se ha inaugurado a partir del año2021, y tampoco antes no existía certificación respecto de un perito en cómputos forenses. Pero en líneas generales, por ejemplo UTN certifica un ingeniero en sistemas o un desarrollador de sistemas. No había una carrera universitaria como tal que diga vos vas a ser perito informático, hasta el año pasado que en Buenos Aires se han creado carreras tendientes a esta demanda, porque claramente la tecnología avanza y cuando esta avanza trae aparejado la creación de nuevos delitos y, a raíz de eso tiene que existir una rama que investigue esas acciones. Por esto en Buenos Aires se ha creado una carrera o especie de Diplomatura en la que certifican en las líneas generales del cómputo forense, para ser un perito informático.

La División Delitos Tecnológicos no cuenta con un perito informático, pero si cuenta con idóneos en informática forense, dado que se han hecho cursos, capacitando al personal, que a su vez tiene una larga experiencia y experticia en el tema. No nos

olvidemos que el Código Procesal Penal menciona que cuando no exista un especialista en la materia, bien puede ser tomado como tal, aquella persona que presente experticia en la materia. Esto avala al idóneo. Es decir, una persona que se especializa por un período de tiempo determinado realizando la tarea, ya tiene la idoneidad para explicar cómo funciona un determinado mecanismo. Por ahí creo que va la diferencia entre el idóneo y el perito en informática forense, entendiendo también que la División de Delitos Tecnológicos no realiza informes periciales, sino que la División realiza informes tecnológicos. Esto quiere decir que es la experiencia, puesta de manifiesto en un informe, por parte del policía. Termina siendo un informe policial, si se quiere. Ese informe va munido de actas, va munido de firmas de otras partes que intervienen. Todo eso enmarcado en las garantías que hay que dar, que están establecidas en el código procesal penal.

¿De dónde y cómo se obtiene la evidencia digital? Y si tiene algún caso que puede ejemplificar, entendiendo la privacidad, por supuesto.

Para entender la evidencia digital yo debería explicarle un poco el contexto en el que se maneja para ubicar a cualquier persona en las tareas que realizamos

En primera instancia, para hablar de prueba digital debemos hablar de proceso penal, para lo cual ya estamos con una investigación judicial en curso, o por lo menos que se está iniciando, porque se pueden realizar tareas, por ser policías, en las cuales uno detecta un delito y lo tiene que poner, a disposición del fiscal, para que este evalúe o no.

En la parte donde la autoridad judicial ya nos requiere a nosotros para realizar determinada tarea. Esto quiere decir que debe obrar en primera instancia, para comenzar las acciones, una orden de una autoridad judicial competente. Ya sea verbal o por escrito. Entendiendo esas dos órdenes que nos avalan para hacer determinada tarea, se comienza.

La rama en la que se obtiene la evidencia digital puede ser diversa, porque cuando hay un dispositivo electrónico puede contener información para llevar claridad a un hecho que se investiga. Eso puede ser una cámara de seguridad, puede ser un mensaje contenido en un dispositivo electrónico de una mensajería electrónica, puede ser un chat o puede ser información contenida en un disco rígido que exista en una computadora para una investigación de estafa.

Los dispositivos electrónicos son transversales a cualquier tipo de delito. Y se pueden tomar bajo dos miradas: Una es la mirada de la tecnología como objeto del delito, esto quiero decir que el delito no se podría haber cometido si esa tecnología no se hubiese inventado. Por ejemplo el phishing, el cual es un delito en el cual, por ejemplo, yo pongo un señuelo para que otro ponga un dato sensible y yo lo pueda obtener, por ejemplo una página falsa, o un sistema de login de un banco falso, que es igual al original, pero no es el original y el ciberdelincuente obtiene los datos especiales para ingresar a esa cuenta de banco y así obtener la información que después usa para robar, cometiendo una estafa. Este

es un delito puro, el cual es el que obtiene un dato para ingresar a un sistema el cual no debería ser accesado, el cual no se podría haber cometido, si no existiera la tecnología de las páginas web, por ejemplo. Esto es indistinto de la estafa, que esta termina siendo una estafa común. Por otro lado, la mirada en la que entendemos que la tecnología puede ser utilizada como medio. Con esto me refiero, por ejemplo, envío un mensaje: "juntémonos en tal lado" para que vos me vendas una bicicleta, la persona concurre a ese lugar y yo lo termino asaltando. En este caso la tecnología no importaba tanto, ya que podría haberlo llamado por teléfono o haber tenido otra comunicación y lo mismo lo hubiera asaltado. Pero sí está siendo utilizada la tecnología como medio para cometer un delito.

Entendiendo estas dos ramas, será como se obtendrá la evidencia para ser aportada en un proceso judicial.

Aquí es importante mencionar cuales son las garantías y recaudos que se deben tener en cada una de las adquisiciones de esa información. Esto quiere decir que por ejemplo cuando la tecnología es utilizada como objeto, es un poco más compleja porque ahí estamos hablando que la tecnología se conecta con lo que hoy denominamos el clouding o la internet o la nube. Es información que no está contenida en los dispositivos en sí, sino que está contenida en servidores externos. Esto es servidores de cuentas de correo electrónico, redes de mensajería como lo son Facebook, como lo son Twitter, Instagram, Snaptchat, WhatsApp, etc. Hoy creo que la tendencia marca que esto está también un poco como por la era industrial, porque cuando la tecnología avanza, siempre avanza en pos de la economía. Entendiendo esto, hoy por hoy, la sociedad de la información, en referencia a todo ese conjunto de herramientas y tecnología, de recursos, que está puesta y a disposición de la sociedad, en tiempo y forma, tiene que estar clarificada, tiene que dar un contenido, y para la parte económica tiene que dar una venta.

Antes la información era contenida en ordenadores convencionales, que uno tenía en la casa sin conexión a internet. Hoy la información está contenida en servidores y nucleada en determinados lugares, para hacer explotación de esa información porque la información trae conocimiento, y el conocimiento trae poder y el poder trae muchas cosas.

Para que la Inteligencia Artificial (IA), y ya nos metemos en otro campo, pueda ser explotada como tal, requiere de tres grandes partes: el poder de cómputo, los algoritmos necesarios y por sobre todas las cosas y como lo más importante, gran cantidad de información. Esto no es novedoso que toda la información sea contenida o nucleada por Gmail, por Facebook, por TikTok o las distintas redes, que empiezan a recopilar información a lo loco. No es al azar, sino que todo pertenece a esta idea de ir generando sistemas que se retroalimenten. La IA tiene dos grandes ramas: el machine learning y la inteligencia en sí. Es decir, sistemas que se alimentan de sí mismos. Pero para eso necesitan de gran cantidad de información. La información ya no se contiene en un ordenador, por

eso antes se llamaban delitos informáticos, hoy se llaman ciberdelitos o cibercrimen porque contempla esta idea de ciberespacio, en el cual está contenida toda esa información.

Me fui para este contexto, porque cuando yo, como idóneo, le digo al fiscal o al juez "mire doctor yo voy a hacer uso de la información contenida en este dispositivo electrónico" debo comprender muy bien de qué tipo de dispositivo electrónico estoy hablando. Esto es porque ahí puedo saber si la información está contenida realmente en el dispositivo o si este se enlaza a una nube central que está en otro país, en otro lugar, con otra legislación, lo que se llama la transnacionalidad, la cual es una de las características del ciberespacio, ¿A quién le pido yo, como juez de garantía, la autorización para acceder a esa información? Es decir en el cómputo forense, en el apartado de la adquisición, una vez que yo la haya identificado en qué lugar está (en el ciberespacio), ahora tengo que adquirirla, y es el juez de garantía el que pedirá la autorización, para permitirme a mí obtener la información, si no sabemos dónde está contenida. Está en el ciber espacio, pero en el ciberespacio está Gmail, que tiene servidores en Estados Unidos, en Malasia, en Corea del Sur, en distintos lugares por ejemplo, entonces no sabemos con exactitud dónde puede estar la información almacenada. Por lo tanto es importante que el perito o idóneo, deba tener bien en claro donde se encuentra la información y como debe explicarle al juez o al fiscal que está investigando, de donde va a obtener esa evidencia digital, como comenzaste la pregunta.

Lo otro es cuando la tecnología es como medio. Como medio es más sencillo porque podemos ver cámaras de seguridad, mensajes contenidos en un dispositivo, que esos mensajes quedan en forma local. Si bien utiliza la nube para hacer el intercambio, finalmente algunas aplicaciones conservan, en el dispositivo electrónico una copia. Con lo cual ahí no se está invadiendo ningún tipo de privacidad más que la del dispositivo. Y si esto está autorizado por un juez de garantía, el perito tranquilamente, con esa autorización y las partes intervinientes, en este punto hago referencia a peritos de parte, abogados defensores, querellantes, y simples testigos. Pueden estar o no, esas partes, siempre tiene que haber un fundamento por que no están. Pero puede pasar que no estén. Ahí queda más claro donde se va a trabajar Por eso es importante también, en la obtención de la prueba digital, tener bien en claro lo que es cadena de custodia, desde el punto cero en que se identifica un instrumento, hasta que se comienza con la adquisición de la información, como se hace la preservación de la información para luego venir con un análisis y presentación que termine siendo clara para quien lo vaya a leer: jueces, fiscales, querellantes, defensores, testigos y ahora con los juicios por jurados, una de las partes más importantes del perito informático o del idóneo informático forense, es que traslade todo ese conocimiento, a palabras claras que las entienda un ciudadano simple, que son las que conforman los jurados. Puede haber un caso fortuito que haya un técnico, pero la mayoría de las veces son personas comunes que pueden no entender este lenguaje, como funciona la nube, como funciona la adquisición de información, porqué la información es volátil, por

qué hay que tener cuidado, por qué no hay que apagar una computadora, que es la información en una memoria RAM, que es volátil, que si se apaga el ordenador se pierde, como se adquiere eso, como se traduce el binario a un lenguaje común.

¿Algo más que quisiera agregar?

Creo que la Policía de Mendoza se está preparando para el futuro, lo veo así. Siempre vamos detrás del delincuente en pos de cuestiones de recursos, de preparación. Es más, se entiende que el delincuente siempre está innovando, porque a medida que el control social le va poniendo trabas y justamente va regulando esas conductas para que no ocurran, el delincuente se va renovando.

Eso sería la mutación del delito

No hay sociedad que no tenga delito. De alguna u otra forma, existe. Ahora el control social formal, siempre va a regular. Pero el control social informal también ejerce una regulación. Pero el control social formal, esto es el Sistema Policial, el Sistema Judicial y el Sistema Penitenciario, siempre han ido por detrás de los delitos. Siempre ocurrió así a lo largo del tiempo. En este caso el control social informal parecería ir más avanzado, ya que en las redes sociales se producen ciertos movimientos de ir censurando a personas que hacen por ejemplo, tráfico de imágenes de menores. Me refiero a la pornografía infantil, a las cuestiones de suplantación de identidad, que no están reguladas como delito hoy en la Argentina, Buenos Aires es la única que ha presentado algo y esto es a nivel contravencional. Me refiero a la suplantación de la identidad como yo usurpándote Facebook con los mismos datos y las mismas fotos. Como delito no está regulado, entonces es como que vamos detrás del delito. Pero la policía de Mendoza ha avanzado muchísimo y creo que es una de las pioneras, la provincia de Mendoza en tener el Polo TIC, por ejemplo, en el departamento de Godoy Cruz en el cual una serie de empresas se han nucleado para trabajar en torno a las nuevas tecnologías, y producir profesionales y tecnologías nuevas. Generar aplicaciones y demás. Mendoza es pionera en esto.

La policía de Mendoza puede también, gozar de estos espacios y estar un poco más a la vanguardia en tecnología. Cuando yo ingresé en Delitos Tecnológicos hace 10 años esto era impensado, porque se hacían otro tipo de tareas, se ha ido, de alguna manera actualizando a pasos agigantados. Y la División Delitos Tecnológicos, creo desde mi experiencia, siempre ha estado a la altura de las circunstancias, y esto lo dicen los miembros de esta unidad, lo dice la sociedad, lo dicen los jefes, lo dicen los fiscales y lo dicen las dependencias que trabajan con ellos. En mi opinión personal, como parte de la institución, me llena de orgullo.

Más allá de eso, a nivel de jefatura se han hecho avances enormes como es la creación del DATAI. Esta institución, vino a responder a esta necesidad la interrelación de la

información. La policía no se puede pensar ya como un organismo único para investigar un delito. Ahora tiene que estar relacionado con una enorme cantidad de áreas.

Hay que mencionar que el DATAI es el Departamento de Asistencia Tecnológica y Apoyo Investigativo

Exacto, y su función es justamente nuclear y generar el conocimiento de diversas áreas. Porque ya no se pueden pensar por separado. Por eso hoy Dirección de Investigaciones se compone de Policía Científica, de Policía de Dirección de Investigaciones y de Narcotráfico. Ahora están nucleadas las 3 áreas bajo una sola dirección. Y, consecuentemente el DATAI está nucleando División Delitos Tecnológicos, División Análisis Criminal, División de Escuchas Telefónicas y Antisecuestros Extorsivos, y el CAI, que es una nueva área donde se puede visualizar en tiempo real lo que está sucediendo en la provincia de Mendoza, y hacer adquisiciones en tiempo real, lo que significa un avance gigante. Están dando sus primeros pasos y como relacionan la información y como trabajan en materia de cómputos forenses, si se quiere, porque las 3 áreas trabajan con la tecnología. Y esto va a aporta resultados gigantes. Y esto responde a estar atentos con los avances de la tecnología, estar atentos al movimiento de los cibercriminales, estar atentos a los nuevos ciberdelitos, y a los cambios sociales que hoy están atravesados por las tecnologías. Creo que la Policía de Mendoza hoy cuenta con grandes profesionales, que poseen una experticia enorme desde las 3 áreas, y eso hay que explotarlo.

YO me siento orgulloso de pertenecer a este equipo. No es casual que los fiscales siempre estén agradecidos y nos estén nombrando como que somos un pilar en la investigación que ellos desarrollan como fiscales en la Provincia de Mendoza. También se han hecho aportes con otras provincias. El DATAI ha hecho cooperaciones enormes y se han esclarecido delitos en tiempo récord. El caso Fxxxx uno de los más resonantes, el caso de las señoras israelíes que fueron asesinadas por Gil Pereg, en donde circuló cantidad de información producida por las 3 áreas, trabajando en forma mancomunada, logrando resultado óptimos.

Muchas gracias por su amplia colaboración.

Glosario

Adware: es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador.

Brodcast: en las redes informáticas, el *broadcast* es un mensaje que se transmite a todos los miembros de una red y que no necesita ninguna acción de retroalimentación. Un equipo conectado a la red envía un paquete de datos al resto de participantes de la red al mismo tiempo. En este proceso, el emisor no especifica ninguna dirección de destino, lo que distingue el *broadcast* del llamado *unicast*, en que el paquete solo se envía a un único destino conocido. La principal ventaja del *broadcast* es que la información puede distribuirse de forma masiva sin tener que enviarla en más de una ocasión.

Bullying: el acoso escolar o *bullying* es un hecho cada vez más frecuente en los centros de enseñanza y se produce cuando un niño o adolescente es agredido física y psíquicamente de manera reiterada y continuada por un alumno o un grupo de alumnos.

Cyberbulying: es el ciberacoso esto incluye enviar, publicar o compartir contenido negativo, dañino, falso o cruel sobre otra persona. Puede incluir compartir información personal o privada sobre otra persona que cause vergüenza o humillación. Algunos casos de acoso cibernético cruzan la línea y se convierten en conductas ilegales o delictivas.

Direct Messages: en términos de *influencers* es un Mensaje Directo (DM) es una comunicación privada entre una marca o negocio y sus clientes. También se les llama mensajes privados (PM).

Cyperstalking: el *cyberstalking* es una forma de persecución que consiste en el uso de internet u otro instrumento computarizado con la intención de asediar o perseguir a alguien, a través de acciones metódicas, persistentes e indeseables generadoras de incomodidad en la vida de las víctimas.

Dark web: la *dark web*, o internet oscura es el contenido de la World Wide Web que existe en *darknets*, redes que se superponen a la internet pública y requieren de software específico y configuraciones o autorización para acceder.

Deep web: Internet profunda, internet invisible o internet oculta es el contenido de internet que no está indexado por los motores de búsqueda convencionales, debido a diversos factores. El término se atribuye al informático Mike Bergman.

Follow: seguido.

Follower: seguidores.

Follow Friday: *Follow Friday* significa viernes de seguir. Y se ha institucionalizado como costumbre en twitter, el que los días viernes recomendamos a algunas arrobas que nos parecen interesantes o divertidas de seguir. Funciona desde Enero de 2009 y ha tenido tanta acogida que se ha convertido en el Hashtag más popular de Twitter.

GNU/Linux: es un sistema operativo, de código abierto y desarrollado por una comunidad, para computadoras, servidores, dispositivos móviles y embebidos.

Grooming: es la acción deliberada de un adulto, varón o mujer, de acosar sexualmente a una niña, niño o adolescente a través de un medio digital que permita la interacción entre dos o más personas, como por ejemplo redes sociales, correo electrónico, mensajes de texto, sitios de chat o juegos en línea.

Hackear: el *hackeo* hace referencia a las actividades que buscan comprometer los dispositivos digitales, como ordenadores, teléfonos inteligentes, tabletas e incluso redes enteras. Y aunque el *hackeo* puede no tener siempre fines maliciosos, actualmente la mayoría de las referencias tanto al *hackeo* como a los hackers, se caracterizan como actividad ilegal por parte de los ciberdelincuentes, motivados por la obtención de beneficio económico, por protesta, recopilación de información (espionaje), e incluso sólo por la "diversión" del desafío. Ingresar a sistemas informáticos ajenos y manipularlos

Hacking: un hacker es alguien que descubre las vulnerabilidades de una computadora o un sistema de comunicación e información, aunque el término puede aplicarse también a alguien con un conocimiento avanzado de computadoras y de redes informáticas.

Hardware: conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Hash: una función criptográfica hash- usualmente conocida como "hash"- es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud), que permite establecer la autenticidad de un archivo.

Hashtag: hashtag es un término asociado a asuntos o discusiones que desean ser indexadas en redes sociales, insertando el símbolo de numeral (#) antes de la palabra, frase o expresión. Cuando la combinación es publicada, se transforma en un hyperlink que lleva a una página con otras publicaciones relacionadas al mismo tema.

Haters: traducido significa odiador, es alguien que muestra su rechazo a determinados colectivos a través de comentarios y publicaciones. Su blanco de acción pueden ser las personas extranjeras, o las mujeres, o las LGTBI.

Identity Theft: es el robo o suplantación de identidad digital.

IMEI: (International Mobile Station Equipment Identity, en inglés) es un código de 15 dígitos pregrabado por el fabricante para identificar cada equipo móvil a nivel mundial. Está compuesto por un código de identificación de marca y modelo otorgado a los fabricantes por la GSMA (Global System Mobile Association).

Influencer: un *influencer* es una persona que cuenta con cierta credibilidad sobre un tema concreto, y por su presencia e influencia en redes sociales puede llegar a convertirse en un prescriptor interesante para una marca.

Insiders: son personas o empleados que en forma intencional o negligente provocan una brecha de seguridad en un sistema informático o de comunicación electrónica, la particularidad es que es desde el interior de la organización.

Instagrammer: usuario de la red social *instagram*, el *instagrammer* comparte imágenes y vídeos que crea al mismo tiempo que sigue las cuentas de otros usuarios para ver sus fotos y vídeos. Estas publicaciones pueden ser privadas, pero muchas personas tienen cuentas públicas, lo que significa que cualquier persona puede encontrar y seguir a cualquiera que lo desee.

Jaula Faraday: la jaula de Faraday es una caja metálica protectora de los campos eléctricos estáticos, en su interior el campo eléctrico es nulo y se utiliza en la protección de descargas eléctricas, se emplea en laboratorios biomédicos, cámaras de reverberación, en telecomunicaciones, entre otros.

Laptopt: el sustantivo “lap”, que puede traducirse como “regazo” y que tiene una raíz germánica. La palabra “top”, que es sinónimo de “lo más alto” o la “cima” y también posee raíz germánica. Una laptop es una computadora portátil (es decir, un ordenador o computador portátil).

Machine learning: el aprendizaje automático o aprendizaje automatizado o aprendizaje de máquinas es el sub campo de las ciencias de la computación y una rama de la inteligencia artificial, cuyo objetivo es desarrollar técnicas que permitan que las computadoras aprendan.

Malware: Malware es un término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.

Marcadores STRs: en genética molecular, los microsatélites son secuencias de ADN en las que un fragmento se repite de manera consecutiva. La variación en el número de repeticiones, y no la secuencia repetida, crea diferentes alelos. Generalmente se encuentran en zonas no codificantes del ADN

Marketplace: de refiere a un concepto más amplio de ventas online. En esta plataforma, diferentes tiendas pueden anunciar sus productos, ofreciéndole de esa forma, un abanico de opciones al cliente.

Memoria RAM: la memoria RAM es la memoria principal de un dispositivo, esa donde se almacenan de forma temporal los datos de los programas que estás utilizando en este momento. Sus siglas significan *Random Access Memory*, lo que traducido al español sería *Memoria de Acceso Aleatorio*, y es un tipo de memoria que te puedes encontrar en cualquier dispositivo, desde ordenadores de sobremesa hasta teléfonos móviles.

Modo live CD: hace referencia, a la carga de un sistema operativo en memoria RAM, lo cual significa que no requiere una instalación permanente, es reducido, en cuanto a aplicaciones, de esta forma no se pierden datos del disco rígido.

Networks: es la integración de dos sistemas de redes completas. Una red consiste en dos o más computadoras unidas que comparten recursos como archivos, *CD-Roms* o impresoras, y que son capaces de realizar comunicaciones electrónicas.

Nube: del inglés *cloud computing*, es un paradigma que permite ofrecer servicios de computación a través de Internet. En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet, siendo un paradigma en el que la información se almacena de manera permanente en servidores de Internet.

Online barassment: ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas.

PhotoRec: es un software diseñado para recuperar archivos perdidos incluyendo videos, documentos y archivos de los discos duros y CDRoms así como imágenes perdidas (por eso el nombre PhotoRecovery) de las memorias de las cámaras fotográficas, MP3 *players*, *PenDrives*, etc. *PhotoRec* ignora el sistema de archivos y hace una búsqueda profunda de los datos, funcionando incluso si su sistema de archivos está muy dañado o ha sido re-formateado.

Plugins: un *plugin* es un complemento de software que ayuda a que un programa haga algo que normalmente no haría por sí solo.

Ransomware: el malware de rescate, o *ransomware*, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

Reg Ripper: es una herramienta *Open Source*, escrita en Perl, con el propósito de analizar la información de las llaves, valores, y datos del registro de Windows para presentar los mismos con el fin de analizarlos.

Retweet: es el reenvío de un tweet.

Roaming: es un concepto que se refiere a usar una red distinta de la principal. En términos más sencillos, se da cuando salimos de nuestro país y conectamos con la red móvil de un operador que no es el nuestro.

Router: un enrutador (del inglés router) o encaminador es un dispositivo que permite interconectar redes con distinto prefijo en su dirección IP. Su función es la de establecer la mejor ruta que destinará a cada paquete de datos para llegar a la red y al dispositivo de destino.

Self Media: materiales que el usuario puede seleccionar y utilizar cuando desee (por ejemplo: un libro).

Sexting: se refiere al envío de imágenes o videos de contenido sexual a través de softwares de mensajería electrónica, y que se da en forma voluntaria.

Spoofing: es el uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

Streaming: transmisión en vivo o en directo de contenido multimedia a través de redes de comunicación electrónica.

Software: es un conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Spyware: software malicioso que infecta el ordenador o dispositivo móvil y recopila información sobre el usuario, su navegación y su uso habitual de Internet, así como otros datos.

Tablet: es un tipo de computadora portatil, regularmente de mayor tamaño que un smartphone, que cuenta con una pantalla táctil con la que se interactúa sin necesidad de teclado ni mouse.

Target: el target en marketing representa a los clientes potenciales o público que tienen como objetivo las empresas a la hora de hacerles llegar sus productos o servicios. Es un concepto que tiene suma importancia dentro del área del marketing y la comunicación.

Tecnología LAMP: acrónimo para describir una infraestructura de internet, de los términos Linux (Sistema Operativo), Apache (Servidor Web), Mysql (Gestor de Base de Datos), Php(Lenguaje de Programacion).

The Sleuth Kit & Autopsy: *Sleuth Kit* es una colección de herramientas de línea de comandos y una biblioteca C que le permite analizar imágenes de disco y recuperar archivos de ellas. Se utiliza entre bastidores en *Autopsy* y muchas otras herramientas forenses comerciales y de código abierto. *Autopsy* es un programa basado en GUI fácil de usar que le permite analizar eficientemente discos duros y teléfonos inteligentes. Tiene una arquitectura de complemento que le permite encontrar módulos complementarios o desarrollar módulos personalizados en Java o Python.

Treding Topic: Un *trending topic* (tendencia, tema de tendencia o tema del momento en español, y TT en forma abreviada) es una de las palabras o frases más repetidas en un momento concreto en una red social.

Trol: Describe a una persona con identidad desconocida que publica mensajes provocadores, irrelevantes o fuera de tema en una comunidad en línea, como pueden ser un foro de discusión, sala de chat, comentarios de blog, o similar, con la principal intención de molestar o provocar una respuesta emocional negativa en los usuarios y lectores, con fines diversos (incluso por diversión) o, de otra manera, alterar la conversación normal en un tema de discusión, logrando que los mismos usuarios se enfaden y se enfrenten entre sí.

Unfollow: dejar de seguir.

Wireshark: es el analizador de protocolos de red más importante y ampliamente utilizado del mundo. Le permite ver lo que sucede en su red a un nivel microscópico y es el estándar de facto en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas.

Youtuber: es un productor y gestor de contenido audiovisual que usa YouTube como su plataforma de comunicación. Algunos youtubers tienen patrocinadores corporativos que pagan por la colocación de productos en sus videos o producción de anuncios en línea.

Bibliografía

Aguilar Avilés, D. (2010). Control social y prevención delictiva: una introducción al tema de análisis de los medios de comunicación social. *Contribuciones a las Ciencias Sociales, 20*(1), 127-145.

Alfonso Sánchez, I. (2016). La Sociedad de la Información, Sociedad del Conocimiento y Sociedad del Aprendizaje. Referenes en torno a su formación. *Bibliotecas anales de investigación, 12*(2), 235-243.

Alva de la Selva, R. (2015). Los nuevos rostros de la desigualdad en el Siglo XXI: la brecha digital. *Revista Mexicana de Ciencias Políticas y Sociales, 60*(223), 265-285.

Álvarez Ventura, J. (2018). *Manejo de TIC. Definición del concepto de TIC.* Obtenido de http://www.aprenderenlinea.edea.edu.co

Álvarez, J. (2017). Consideraciones acerca del "sextorsión" y el "revenge porn". *Diario Doctrina Penal*(104).

Ambrosino, N. y. (2021). La evidencia digital y su tratamiento en el proceso penal de Córdona. *Terragni Jurista*(26), 2-10.

Ambrosis, R. (2018). Las redes del delito. La sociedad de la información y sus crímenes. *Vlex*(18), 32-39.

Belloch Orti, C. (2020). *Las tecnologáis de la información y comunicación (T.I.C.).* Obtenido de Repositorio Universidad de Valencia. España: https://www.uv.es/~bellochc/pdf/pwtic1.pdf

Bielli, G. (2019). Prueba elecrtónica: incorporación, admisión y valoración de capturas de pantalla en el Proceso Penal. *La Ley, 14*(10), 15-31.

Bisquert, S. (2006). *La figura del "phishing" como modalidad delictiva. Problemática en cuanto a su encuadre jurídico.* Obtenido de SAIJ: http://www.saij.gob.ar/doctrina/dacf060096-bisquert-figura_phishing_como_modalidad.htm

Blanco, A. (2012). *Una sociedad hiperconectada.* Madrid: Fundación Encuentro.

Borghello, C. (2001). *Seguridad informática. Su implicancia e interpretación.* Mendoza: UTN.

BriefCam. (2022). *Transform Video. Reduce Time-To-Target while increasing safety and optimizing operations*. Obtenido de BriefCam: https://www.briefcam.com/

Bruzzone, G. y. (2015). *Estudios en homenaje al Dr. Francisco J. D'Albora* (3° ed.). Buenos Aires: Abeledo Perrot.

Cabero, J. (2001). *Tecnología educativa.* Barcelona: Paidós.

Cacheiro, M. (2014). *Educación y Tecnología: Estrategias didácticas para la integración de las TICs.* Madrid: UNED.

Cacheiro, M. (2017). *Educación y Tecnología: Estrategias didácticas para la integración de las TICs* (2° ed.). Madrid: UNED.

Cancino, H. (2017). *La Tecnología que potenciará la Seguridad Ciudadana.* Obtenido de https://tecno.americaeconomia.com/articulos/la-tecnologia-que-potenciara-la-seguridad- ciudadana- del-futuro

Castano, C. (2008). *La segunda brecha digital.* Madrid: Cátedra.

Castells, M. (1989). *La era de la información.* México: Siglo XXI.

Castells, M. (1997). La era de la información. Economía Sociedad y cultura. En *La sociedad ed* (Vol. 1). México: Alianza.

Castells, M. (2001). *La Galaxia Internet.* Barcelona: Areté.

Ceballos Espinoza, F. (2021). De la criminologia clásica a la criminología moderna: la investigación criminal multifactorial en la era digital. *Formación y Desarrollo Policial, 3*(1), 59-85.

Clarín. (2010). La Casa Blanca implora a WikilLeaks que no filtre más documentos sobre la guerra. *Diario Clarín*.

Constante, A. (2013). *Las redes sociales, una manera de pensar el mundo.* México: UNAM.

Council of Europe. (2001). Convenio sobre la ciberdelincuencia. *Serie de Tratados Europeos*(185), 1-26.

CPDP. (2022). *Grooming: que es, cómo detectarlo y qué hacer.* Obtenido de Centro de Protección de Datos Personales: https://cpdp.defensoria.org.ar/2020/11/13/grooming-que-es-como-detectarlo-y-que-hacer/

Curi, A. D. (2005). El delito informático. *Pensamiento penal*(16), 130-147.

Dammert, L. (2017). *Innovación tecnológica para la Seguridad en América Latina.* Santiago, Chile: University of Santiago de Chile.

De Pablos, J. (2016). Universidad y sociedad del conocimiento. Las competencias informacionales y digitales. *Revista Universidad y Sociedad del Conocimiento, 7*(2).

Facebook. (2022). *Normas Comunitarias*. Obtenido de Facebook: https://www.facebook.com/communitystandards/cybersecurity

Facebook. (s.f.). *Página de inicio*. Obtenido de Facebook: https://es-la.facebook.com

Fernández, E. (2019). Alfabetización digital: ¿Qué es?, ¿Cuál es su importancia? *Revista UNIR, 26*(12), 32-46.

Flores, L. M. (2018). Propuesta de procedimiento para el análisis delictivo basado en la explotación de la información. *XX Workshopp de Investigaciones en Ciencias de la Computación*(10), 20-30.

Galperín, H. (2017). *Sociedad digital: brechas y retos para la inclusión digital en América Latina y el Caribe.* Montevideo: UNESCO.

Gilbert Ceballos, J. (1997). *Introducción a la sociología.* Santiago de Chile: LOM ediciones.

Grande, M. C. (2015). Tecnologías de la Información y la Comunicación: evolución del concepto y características. *International Journal of Educational Research and Innovatio*(6), 218-230.

Granero, H. (2019). *E-Mails, chats, WhatsApp, SMS, Facebook, filmaciones con teléfonos móviles y otras tecnologías: validez probatoria en el proceso civil, comercial, penal y laboral.* Buenos Aires: Albremática.

Guzmán Flores, T. (2008). Las Tecnologías de la Información y la Comunicación en la Universidad Autónomo: Propuesta Estratégica para su integración. Universitat Rovira I Virgili.

Hansgross. (2022). *Amped Five*. Obtenido de Hansgross- Criminalística Cibernética: https://hansgross.com.pe/amped-five/

HelpTwitter. (s.f.). *Glosario Twitter*. Obtenido de Twitter: https://help.twitter.com/es/resources/glossary

Hernández, A. (2021). Acceso, usos y problemas en la educación virtual: una aproximación a las experiencias de estudiantes y docentes durante la cuarentena obligatoria en Argentina. *Revista Pacha, 1*(4), 68-75.

INDEC. (201). *Ciencia y Tecnología. Acceso y uso de Tecnologías de la Información y la Comunicación. EPH* (Vol. 5). Buenos Aires: Ministerio de Economía.

INDEC. (2020). *Informes Técnicos. Ciencia y Tecnología* (Vol. 4). Buenos Aires, BUenos Aires: Ministerio de Economía. Argentina.

INDES. (12 de Abril de 2019). *La Argentina es el país con mayor talento en tecnología del mundo.* Obtenido de INDES ELERNING & WEB: https://indesgroup.com/category/business/

Instagram. (s.f.). *Cómo garantizamos que Instagram sea un espacio seguro y tolerante*. Obtenido de https://about.instagram.com/es-la/safety

INTERPOL. (2022). *Reconocimiento facial.* Obtenido de https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial

Kemp, S. (27 de Enero de 2021). *Digital 2021: Global Overview Report.* Obtenido de Datareportal: https://datareportal.com/reports/digital-2021-global-overview-report

Linares, M. (2020). Delitos informáticos en el Código penal argentino. *Revista chilena de Derecho y Ciencia Política, 11*(2), 122-144.

Lorenzo, J. (2020). *Mejores herramientas gratuitas de informática forense.* Obtenido de redeszone: https://www.redeszone.net/tutoriales/seguridad/mejores-herramientas-gratuitas-informatica-forense/

Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Revista Ius et Praxis, 24*(1), 159-206.

Majó, J. y. (2002). *La revoliución educativa en la era de Internet.* Barcelona: Cisspraxis.

Masuda, Y. (1984). *La sociedad informatizada como sociedad post-industrial.* Madrid: Fundesco.

Mattelart, A. (2002). *Historia de la Sociedad de la Información.* Barcelona: Paidos.

Ministerio de Justicia y Derechos Humanos. (2017). Protocolo unificado de los ministerios públicos de la República Argentina: guía para el levantamiento y conservación de la evidencia. Buenos Aires: SAIJ.

Miró Llinares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio.* Madrid: Marcial Pons Ediciones Jurídicas y Sociales S. A.

Novick, M. y. (2021). *El desafío de las TIC en Argentina.* Santiago de Chile: Naciones Unidas.

Núñez, R. (1999). *Manual de Derecho Penal. Parte Especial.* Córdona: Marcos Lerner Editoda.

Ontoria, A. (2006). *Aprender con mapas mentales: una estrategia para pensar y estudiar.* Madrid: Narcea.

Ortiz, F. (1995). *La Sociedad de la Información* . Madrid: Fundesco.

PBU. (2021). *Prestación Básica Universal y Obligatoria (PBU) para celulares, internet, televisión por cable y telefonía fija.* Obtenido de https://www.argentina.gob.ar/servicio/solicitar-prestacion-basica-universal-y-obligatoria-pbu-para-celulares-internet-television

Peñaloza, B. (2019). Mendoza: hacia un Código Procesal Penal adecuado para la investigación de ciberdelitos. *XIX Simposio Argentino de Informática y Derecho (SID2019).*

Pérez Cascella, R. (28 de diciembre de 2017). *La moderna prueba documental electrónica y digital. Observar el mundo virtual para mejorar el servicio de justicia y evitar el atraso generacional.* Obtenido de microjuris.com: https://aldiaargentina.microjuris.com/2018/07/26/la-moderna-prueba-documental-electronica-y-digital-observar-el-mundo-virtual-para-mejorar-el-servicio-de-justicia-y-evitar-el-atraso-generacional/

Pérez, A. (2020). *Las políticas de las grandes plataformas sobre Discurso de Odio durante el Covid-19.* Montevideo: UNESCO.

PoloTIC. (s.f.). *Utilizarán drones para tareas de seguridad en Mendoza.* Obtenido de https://poloticmendoza.org/2020/01/13/utilizaran-drones-para-tareas-de-seguridad-en-mendoza/

Prensa Gobierno de Mendoza (2018). *Mendoza es la primera provincia en implementar la base de datos de ADN.* Obtenido de Gobierno de Mendoza: https://www.mendoza.gov.ar/prensa/mendoza-es-la-primera-provincia-en-implementar-la-base-de-datos-de-adn/

Prensa Gobierno de Mendoza (2021). *El sistema TETRA garantiza las comunicaciones en todo el territorio provincial.* Obtenido de https://www.mendoza.gov.ar/prensa/el-sistema-tetra-garantiza-las-comunicaciones-en-todo-el-territorio-provincial/#:~:text=El%20Sistema%20de%20Comunicaciones%20de,7%20d%C3%ADas%20de%20la%20semana.

Poder Judicial Mendoza. Suprema Corte de Justicia. Departamento Aula Virtual. Obtenido de http://www.jus.mendoza.gov.ar/web/departamento-aula-virtual/informatica

Rayón Ballestero, M. y Gómez Hernández, J. (2020) Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense. XLVII (1) 12-29

Rifkin, J. (1996). *El fin del trabajo. NUevas tecnologías contra puestos de trabajo: el nacimiento de una nueva era.* Barcelona: Paidós.

Rivoir, A. y. (2019). *Tecnologías digitales: miradas críticas de la apropiación en América Latina.* Buenos Aires: CLACSO.

Rivolta, M. (2012). Medios de prueba electrónicos: estado de avance en la legislación argentina. *SAIJ*.

Rodríguez Rosario, M. (2020). La justicia en la sociedad del conocimiento y la información. *Revista de la Facultad de Derecho de la Universidad Nacional de Córdoba, 2*(XI), 12-34.

Roibón, M. (23 de enero de 2019). *La estafa informática en el Código Penal Argentino.* Obtenido de Revista Pensamiento Penal on line: https://www.pensamientopenal.com.ar/doctrina/47322-estafa-informatica-codigo-penal-argentino

Roig, R. M. (2015). Internet como medio de información, comunicación y aprendizaje. En J. y. Barroso, *Nuevos escenarios digitales.* Madrid: Pirámide.

Saez Capel, J. (2001). *Informática y delito.* Buenos Aires: Peoa XXI Editores.

Sain, G. (2017). El Derecho Penal aplicado a los delitos informáticos: Una política eficiente para el cibercrimen? *SAIJ*.

Santiago, R. y. (2018). La Web 2.0 en escena. *Pixel-Bit*(41), 19-30.

Serrano Marín, V. (2002). La Sociedad de la Información y el Conocimiento. *Revista Mexicana de Ciencias Políticas y Sociales, XLV*(185). Obtenido de Revista Mexicana de Ciencias Políticas y Sociales: http://www.miaulavirtual.com.mx/ciencias_sociales/Revista_UNAM/RevistaUnamPDF/RMCPYS%20NUM-185.pdf

SIJUM (2021) Servicio de Información Judicial Mendoza. El poder judicial quiere llegar a la digitalización total en 2021. Obtenido de http://www.jus.mendoza.gov.ar/web/sijum/-/el-poder-judicial-quiere-llegar-a-la-digitalizacion-total-en-2021

Sorbo, H. (2013). Delitos informáticos. Aspectos a tener en cuenta de la Ley 26.388. *Doctrina Penal, 32*, 27-56.

Sunkel, G. (2016). Las Tecnologías de la Información y la Comunicación (TIC) en la educación en América Latina: una exploración de indicadores. *Revista de la Cepal, 16*(9), 5-16.

Taruffo, M. (2008). *La Prueba. Filosofía y Derecho.* Madrid: Marcial Pons.

Temperi, M. (2018). Delitos informáticos y cibercrimen: alcances, conceptos y características. En R. Parada, *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet* (págs. 49-68). Buenos Aires: Erreius.

TIC, P. (2021). *Polo TIC Mendoza.* Obtenido de https://poloticmendoza.org/

Touraine, A. (1969). *La sociedad post-industrial.* Barcelona: Ariel.

Twitter. (s.f.). *Centro de ayuda*. Obtenido de Twitter: https://help.twitter.com/es/rules-and-policies/twitter-rules

UFECI. (s.f.). *Acerca de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI).* Obtenido de https://www.mpf.gob.ar/ufeci/

UNICEF. (s.f.). *Ciberacoso: Qué es y cómo detenerlo. Lo que los adolescentes quiene saber acerca del ciberacoso.* Obtenido de UNICEF: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

UNIDIVERSIDAD. (Septiembre de 2021). Finalmente, el ministro de Seguridad fue a la Legislatura a dar explicaciones. págs. Disponible en: https://www.unidiversidad.com.ar/finalmente-el-ministro-de-seguridad-fue-a-la-legislatura-a-dar-explicaciones.

Vaninetti, H. (2018). *Preservación y valoración de la prueba informática e identificación de IP*. Buenos Aires: La Ley.

Wasserman, S. y. (2013). *Análisis de redes sociales: Métodos y aplicaciones.* (I. 978-84-7476-631-8, Ed.) Madrid: Centro de Investigaciones Sociológicas.

Índice