TRABAJO FINAL

ESPECIALIZACIÓN EN DERECHO PENAL Y CIENCIAS PENALES

ALUMNO: CENCI MATIAS GERARDO

D.N.I. Nº: 35.968.954.-

LEGAJO: FADE 637122

INDICE:

I.- INTRODUCCIÒN……..2

I.II.- ¿De qué hablamos cuando hablamos de "evidencia digital"?.....7

I.III. Un breve acercamiento a la informática forense……..9

II.- SISTEMA DE GARANTIAS Y EVIDENCIA DIGITAL ……10

II.I Algunas consideraciones sobre el derecho a la privacidad en la Argentina y las técnicas especiales de investigación en la era digital.

II.II Privacidad, intimidad y secreto en las comunicaciones……15

III.- EVIDENCIA DIGITAL Y TUTELA JUDICIAL EFECTIVA:……22

III.I Políticas Públicas Digitales.-…….25

III.II Nuestro país sigue una política criminal difusa en materia de Cibercriminalidad……28

III.III Ideas para un debate sustentable……29

III.IV A modo de epílogo……30

IV.-EVIDENCIA DIGITAL, SU REGULACIÒN PROCESAL Y COMO HERRAMIENTA DE LITIGACIÒN……...31

IV.I Análisis del articulo 153 código procesal penal de la provincia del Neuquén, información digital……..…33

V. INTIMIDAD VERSUS LIBERTAD PROBATORIA……...37

VI.- EVIDENCIA DIGITAL – CIBERCRIMEN Y LA CRIMINOLOGIA:……42

VII.- CONCLUSION……47

VIII.- BIBLIOGRAFIA…….....…..48

I.- INTRODUCCIÒN:

La transición de la era analógica a la era digital comenzó muy tímidamente en las dos últimas décadas del siglo XX, y cobró una vertiginosa aceleración en las dos primeras décadas de este siglo XXI.

En el mundo jurídico, más precisamente en el sistema de administración de justicia de la República Argentina, la irrupción de las tecnologías de la informática y la comunicación (TICs) comenzó a tornarse cada vez más evidente e indispensable desde el año 2011.

En ese año se sancionó la ley 26.685 que persigue como fin último la implementación del expediente electrónico. Como consecuencia de su sanción la Corte Suprema de Justicia de la Nación a través del dictado de una verdadera cascada de acordadas comenzó gradualmente a intentar compatibilizar el sistema de administración de justicia con un sistema acorde a la era digital. Asimismo los Ministerios públicos también han comenzado un proceso de modernización y adaptación a las nuevas tecnologías de la informática y la comunicación (TICs).

En el caso puntual del MPF en los últimos años ha buscado comenzar a adaptar sus técnicas de investigación a la era digital. Tal es así que se creó en el año 2015 la "Unidad fiscal Especializada en Ciberdelincuenca", lo cual resultaba indispensable, y durante el año 2016 se aprobó el documento "guía de obtención, preservación y tratamiento de evidencia digital", el cual resulta ser un instructivo, tanto para la causa de criminalidad convencional o criminalidad informática, en donde deba colectarse prueba digital.

A su vez, su contraparte el Ministerio Público de La defensa ha implementado el sistema de gestión defensapública.net; y en el último año a fin de incrementar su seguridad informática, ha dictado a través del departamento de informática tres protocolos destinados a: 1 "política de contraseñas" 2.- política de pantallas limpias y bloqueo por inactividad" y 3.- "procedimientos de administración de lista de distribución de correos electrónicos"

A esta actividad el Poder Judicial de la Nación, del Ministerio Publico Fiscal y El ministerio Público de la Defensa, debe sumarse la intensa actividad legislativa de la que se

destaca en 2011 la sanción de la ley 26.685, y una serie de reglamentaciones desde su sanción y hasta la actualidad que intenta de alguna manera regular y subsanar la falta de una legislación lo suficientemente sólida y pragmática como para contener un tema que pone a nuestro ordenamiento jurídico en la necesidad de actualizarse constantemente.

Todo ello exhibe claramente lo indispensable y vital que se torna la regulación normativa de la prueba digital, en un sistema de administración de justicia que ha comenzado su trasformación a la era digital. En primer lugar, debido a las características específicas que posee la evidencia digital, electrónica, intangible, que la distinguen y diferencian claramente de la prueba física, corpórea o tangible.

Esta postura también es compartida por profesor Marcos SALT, quien entiende que: "Hoy la regulación procesal de la evidencia digital resulta imprescindible. La "no regulación" ha generado avallasamiento de garantías por vía de la jurisprudencia bajo el paraguas del principio de libertad probatoria." [1]Debido a que "El sistema penal moderno avanza hacia un estado en el que no será posible prescindir de elementos tecnológicos y la evidencia digital. Dentro de cinco años no va a existir investigación en donde no haya evidencia digital involucrada"[2]

Además porque el empleo de la libertad probatoria, y el uso analógico e las reglas de la prueba física, corpórea o tangible, a la pruebas digital, electrónica o intangible, no resulta adecuado.

Resulta por demás ilustrativo el ejemplo otorgado por SALT "…si en el registro y secuestro de evidencia en entornos digitales yo pretendo utilizar las normas del secuestro de evidencia física o la jurisprudencia de la CSJN, seguramente las soluciones a las que arribe no van a ser siempre las más adecuadas. Por ejemplo, pensemos el caso de hallazgos casuales y toda la doctrina de la plain view. No podemos aplicar la doctrina de la Corte de la misma manera para un ámbito físico que para un ámbito digital. Si allano esta aula en la que estamos sentados para buscar un elemento físico, obviamente por más que busque y busque solo vamos a encontrar lo que está en el ámbito físico en este momento. Si el registro lo realizo sobre una computadora, voy a poder encontrar lo que está alojado digitalmente en este momento, lo que estaba hacu un año, lo que estaba hace cinco años, lo que se trató de borrar, lo que introdujo un usuario anterior de la computadora, y voy a poder encontrar todo, de manera tal que el hecho de la incorporación de dates accidentales

[1] SALT, La relación entre persecución de los delitos informáticos y el derecho penal internacional. Delitos informáticos. Aspectos de derecho penal internacional, en "Revista informática y Delito. Reunión Preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP), mar. 2014, p. 239

[2] SALT, La relación entre persecución de los delitos informáticos y el derecho penal internacional. Delitos informáticos. Aspectos de derecho penal internacional, en "Revista informática y Delito. Reunión Preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP), mar. 2014, p. 241

encontrados en un sistema informático no puede ser regulado de la misma manera que en el caso de la evidencia física. [3]

Por ello, atento a la diversa naturaleza de la prueba digital, respecto de la prueba física, resulta indispensable su regulación específica.

Pero además, en segundo orden de ideas, la regulación normativa de la prueba digital resulta imperiosa e indispensable, no solo debido a sus características específicas que la distinguen de la prueba física convencional, sino por sobre todo porque ello constituye una garantía para la concreción del debido proceso, el derecho de defensa en juicio y el juicio justo. "Legislar y generar nuevos marcos normativos sobre este tema no tiene por qué significar siempre ir contra las garantías. Por el contrario, una buena regulación de estas nuevas herramientas puede permitir un uso adecuado de las necesidades de una investigación moderna y respetuosa de las garantías individuales.[4]

El avance en nuevas técnicas de investigación a través de la vigilancia electrónica, ponen de manifiesto lo indispensable de la regulación de la prueba digital en el área específica del derecho procesal penal, a los fines de garantizar que las medidas procesales implementadas no implique una violación de las garantías constitucionales del debido proceso, derecho de defensa en juicio, el principio de reserva, la inviolabilidad del domicilio, los papeles privados y el derecho a un juicio justo.

Sin embargo ante la ausencia de regulación, se sugiere que a los fines de garantizar el debido proceso, la obtención de prueba digital, ya sea mediante su preconstitución de parte o mediante pericia ordenada judicialmente, y su ulterior preservación y conservación, se realice en las formas bajo los protocolos que han sido descriptos anteriormente.

Ello permitirá en primer lugar, confirmar la integridad e inalterabilidad de la prueba digital obtenida, y en segundo orden, facultará el control de las partes tanto en la etapa preliminar, como durante la etapa de juicio oral, garantizando de esta forma el debido proceso.

Podemos afirmar con cierto grado de probabilidad que la regulación de la prueba digital se convertirá cada vez más indispensable y vital, no solo por estar en juego garantías constitucionales del acusado, sino porque desgraciadamente la administración de justicia en su conjunto y el Estado nacional mismo comenzarán a requerir ineludiblemente de ella.

---

[3] SALT, La relación entre persecución de los delitos informáticos y el derecho penal internacional. Delitos informáticos. Aspectos de derecho penal internacional, en "Revista informática y Delito. Reunión Preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP), mar. 2014, p. 24º y siguiente.-

[4] SALT, La relación entre persecución de los delitos informáticos y el derecho penal internacional. Delitos informáticos. Aspectos de derecho penal internacional, en "Revista informática y Delito. Reunión Preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP), mar. 2014, p. 240 y siguiente.-

Una prueba clara y manifiesta es que la sociedad de la información y la era de la revolución digital del siglo XXI, la protección de su sistema digital de control de tránsito, servicio de telecomunicaciones, suministro de energía eléctrica, gas, agua. Sistema aeroportuario, aduanero, cambiario, financiero y de la misma administración de justicia, estará en juego e cuento a su seguridad e integridad en el ciberespacio.

Ello se debe a que: "El ciberespacio se ha convertido en una especie de quinto elemento. El filósofo griego Empèdocles sostenía que nuestro mundo estaba formado por una combinación de cuatro elementos: tierra, aire, agua y fuego (…) los estados han tenido que desarrollar componentes específicos de las fuerzas armadas para cada uno de estos elementos: el Ejército de tierra, la fuerza aérea, la armada, y, con carácter singular los bombardeos o guerreros del fuego (…) todas las grandes potencias han añadido hoy, a los tres ejércitos tradicionales y a los combatientes del fuego, un ejército cuyo ecosistema es el quinto elemento: el ciberjèrctio, encargado de la ciberdefensa, que tiene sus propias estructuras orgánicas, su Estado Mayor, sus cibersoldados y sus propias armas: supercomputadoras preparadas para librar la ciberguerra digital en el ámbito de internet. [5]

La protección del ciberespacio es hoy vital para el desarrollo de las sociedades modernas, a tal punto que hace tan solo un década ha comenzado a desplegarse una nueva forma d confrontación, la denominada ciberguerra a través de ciberataques.

En miras de ello se ha sostenido que "El proceso penal tiene por fin inmediato el descubrimiento de la verdad objetiva o histórica, para lo cual rige en forma amplia el conocido principio de libertad probatoria: todo se puede probar y por cualquier medio, excepto las limitaciones del sistema jurídico general. Cualquiera puede ser el medio para demostrar el objeto de prueba, ajustándose al procedimiento probatorio que más se adecue a su naturaleza y extensión" [6]

Dicha finalidad implica entender que "hoy en día el concepto de justicia es casi sinónimo con el de hallazgo de la verdad o, cuando menos, este implica un elemento básico de aquel, sin el cual no se puede comprender el concepto de valor que ella menta" [7]

La inteligencia artificial (IA) como uno de los exponentes máximos de las nuevas tecnologías ha dejado de ser una cuestión de ciencia ficción y se ha convertido en realidad. En la actualidad, se utilizan sistemas de IA en múltiples ámbitos de la vida, entre ellos en

[5] RAMONET, El imperio de la vigilancia. Nadie està a salvo de la red global de espionaje, 2016, p. 16 y siguiente.
[6] CS, L. 223. XXXIV, dictamen del procurador Dr. González Warcalde, en la causa 117/94. Recurso de hecho "Luque, Guillermo D. y Tula, Luis R. s/ homicidio preterintencional".
[7] MAIER, Julio B. J., "Derecho procesal penal", Ed. Ad-Hoc, Buenos Aires, 2015, t. III, "Parte general, actos procesales", p. 66.

derecho. Se emplean en mayor medida en tareas jurídicas propias del derecho privado, pero su uso ya ha llegado también al derecho público, en concreto al derecho penal, existiendo ya en la sociedad internacional países que comienzan a utilizar sistemas de IA para prevenir, investigar e incluso perseguir hechos delictivos.

Las nuevas tecnologías de la información y la comunicación, en adelante TIC, se han impuesto, en los últimos años, en el ámbito de la seguridad nacional, la vigilancia de fronteras y la investigación de delitos y persecución del crimen organizado en todo el mundo. La proliferación de este tipo de medidas de investigación tecnológica asegura una mayor efectividad de las actuaciones llevadas a cabo por los gobiernos nacionales y los cuerpos de seguridad de los Estados; sin embargo, también son altamente intrusivas en la esfera de los derechos fundamentales de los ciudadanos

La intimidad o privacidad está amparada y protegida por las garantías constitucionales, pero sin lugar a dudas, para poder condenar a una persona es necesario recolectar prueba que demuestre de manera notoria su participación en el delito del cual se la acusa. Muchas de esas pruebas se encuentran en ámbitos propios de la persona, como su domicilio, archivos digitales, etc. Es por eso que las garantías tienen como objetivo proteger a la persona de posibles abusos e intromisiones arbitrarias en su espacio personal.

Dicha circunstancia fue anoticiada tiempo atrás por los países desarrollados, quienes celebraron en Budapest, Hungría, el 23 de noviembre de 2001 la "Convención sobre la Ciberdelincuencia". Allí se destacó la imperiosa necesidad de generar mecanismos de cooperación internacional efectivos en pos de luchar contra la delincuencia cibernética. La Argentina, mediante la sanción de la ley 27.411, aprobó la mentada Convención, lo que implicó la puesta en marcha de las reformas legislativas procesales a tal fin, aunque aún nos hallemos en un incipiente estado de ese proceso.

Pese a algunos acercamientos por parte del Poder Judicial y del Ejecutivo, nuestra legislación carece de una estructura organizada para la recolección de la prueba que las nuevas conductas delictuales implican, obligando a los operadores judiciales a ampararse en costumbres internacionales que se cristalizan por la imperiosa necesidad de perseguir a los responsables.

La propuesta del presente trabajo será reflexionar acerca de algunas de las problemáticas que actualmente se presentan no no solo respecto del derecho procesal penal y la litigaciòn sino también en torno a las garantías constitucionales, política criminal y abordado desde la criminología. Específicamente focalizaré el análisis en el derecho a la intimidad y el principio de libertad probatoria.

Como podrá advertise hasta aquí, los alcances en materia penal de la evidencia digital son sumamente abarcativos y es posible analizarla desde prácticamente todos los estadios y ramas del derecho constitucional, penal, procesal penal, como herramienta de litigación, medio de prueba, entre otras. Trataré de exponer mediante preguntas y respuestas de simple lectura mi visión sobre la realidad de nuestro país. También procuraré señalar algunos vacíos en materia de políticas públicas y, principalmente, describir los desafíos a los cuales

nos enfrentamos en materia de política criminal, nuevas tecnologías, teoría fáctica, jurídica probatoria y el abordaje de la misma como garantía constitucional y sus implicancias dentro del proceso y la litigación. Durante este recorrido presentaré hechos históricos fundamentales. También discusiones que, aún de rigurosa actualidad, permiten delinear escenarios futuros. Configurado tal panorama de lo que sucede en Argentina y el mundo podremos empezar a pensar y debatir nuevas políticas que sirvan a la sociedad.

I.II.- ¿De qué hablamos cuando hablamos de "evidencia digital"?

Para comenzar, corresponde realizar una breve mención acerca de lo que hoy se entiende como evidencia digital, el cual es un concepto básico en el mundo tecnológico, más inexistente en el ámbito normativo o jurídico. Podemos ubicar el surgimiento de su recolección en el marco de procesos penales para comienzos de los años 90 en los Estados Unidos. Los datos más antiguos datan de 1993, específicamente, cuando el FBI realizó la *International Law Enforcement Conference on Computer Evidence.* Ya desde aquel entonces quedó planteada la necesidad y urgencia sobre la implementación de técnicas forenses que permitan generar un marco jurídico en la utilización de evidencia digital como prueba en los procesos penales.

Dicha conferencia, que luego fue reiterada desde 1995 hasta 1997, culminó con la creación de la *International Organization on Computer Evidence* (IOCE), lo cual dio lugar a la conformación del grupo SWGDE *(Scientific Working Group on Digital Evidence)*, portavoz de la IOCE.

Para el año 2000, la IOCE (EE. UU.) y la Association of Chief Police Officers —ACPO— (Reino Unido) desarrollaron una serie de principios tendientes a permitir la incorporación de pruebas digitales en los estrados judiciales. Así, esta evidencia era entendida como la "información de valor probatorio almacenada o transmitida en forma digital".

El criminólogo Eoghan Casey, parafraseando a su profesor W. Jerry Chisumm[8], definió a la evidencia digital como "*any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of offense such as intent or alibi*". Esta definición, a mi criterio, es la más completa, orgánica y una de las más acertadas.

Dicho en español, entonces, la evidencia digital no es ni más ni menos que todo dato que esté almacenado o sea transmitido mediante la utilización de computadoras (en sentido amplio) que soporta o bien rechaza una teoría acerca de *cómo ocurrió* un delito o bien aborda los elementos críticos de este, como ser la intención (dolo) o su coartada. Pareciera,

[8] En "Criminal Profiling: An Introduction to Behavioral Evidence Analysis", Ed. Academic Press, San Diego, California, 1999.

entonces, que la evidencia digital se asimila en gran medida a cualquier elemento de prueba susceptible de ser secuestrado en un procedimiento judicial.

Hoy en día, cualquier operador o investigador judicial o de las fuerzas de seguridad realiza investigaciones en fuentes abiertas (OSINT, por sus siglas en inglés, *open-source intelligence*), con el objetivo de obtener aquella información que está disponible en internet respecto de todos los seres humanos y la cual no requiere de ningún otro acto más que el colocar nombre y apellido de determinado sujeto en un buscador online. Ahora bien, la clave está en tratar de identificar cuándo es posible validar aquellos datos obtenidos a través de las TIC [9]en un proceso penal, para así incorporarlos y usarlos, por ejemplo, para probar la intención de un imputado o bien su inocencia.

Actualmente este tipo de "prueba tecnológica o informática" —denominada "evidencia digital" o "evidencia informática"— surge de la mano de las nuevas modalidades mediante las cuales los seres humanos comenzaron a cometer ilícitos: el cibercrimen, entendiendo esto como cualquier delito que se comete mediante, a través o con la intervención —en algún momento del *iter criminis*— de medios electrónicos.

Al utilizar el autor a la tecnología como medio o fin, la prueba a recolectarse es, en mayor o menor medida, "digital", puesto que para acceder a ella se debe ingresar a una "nube" o dispositivo electrónico. El concepto de evidencia física comienza entonces a perder relevancia.

Es decir que no solo la evidencia digital puede ser obtenida como resultado de un allanamiento y del peritaje de un dispositivo informático. Tal como se precisó, es posible recabar este tipo de prueba al momento de realizar la investigación, recolectando datos *(logs)* que los seres humanos vamos dejando cada vez que ingresamos a una conexión de red. El problema que subyace es que los métodos de resguardo que esta prueba requiere, en miras de lograr ser validada en un debate oral, son tangencialmente distintos a aquella a la que alude la normativa procesal vigente.

Si bien la evidencia digital es muy rica en información y nos permite incluso obtener la posición de una persona en un determinado momento, sus pulsaciones o incluso la hora en la que se fue a dormir, su contracara es que es altamente volátil y fácilmente alterable, por lo que implica desafíos desde el punto de vista jurídico, extremo que requiere de elementos de seguridad informática que permitan demostrar que aquello que se obtuvo en un entorno digital es auténtico.

A lo largo de la confección de este trabajo se han encontrado voces que de alguna manera intentan colocar a internet dentro de un proceso penal como los denominados medios de prueba (documental, pericial, testimonial, objetos, declaración de partes, informativa), sin embargo es necesario destacar que el sistema de internet va más allá de ser considerado un mero soporte documental representativo de una realidad fáctica, se lo concibe como un

[9] Las tecnologías de la información y la comunicación (TIC) son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (ya sea como imagen, como sonido, en versión de texto, etc.). Su ejemplo más claro es "internet".

fuente de información práctica y preferentemente disponible que además permite comunicarse a millones de personas, recibir correos, utilizar programas, efectuar, búsquedas en todo el mundo, hacer publicidad, transacciones, por ello no debe ser considerado un ·medio" de prueba sino como una "fuente" de prueba debiendo establecerse el procedimiento que permita obtener la información de la red al proceso.

I.III. Un breve acercamiento a la informática forense

Con el objetivo de tener una breve noción de lo que implica lograr la validez de la evidencia digital, seguidamente haré referencia a algunas medidas que deben tomarse para asegurar y validar una prueba de este tipo en un proceso judicial. Adelanto, desde ya, que ello requiere del conocimiento de un experto en la materia, puesto que este tipo de evidencia debe ser resguardada mediante mecanismos de *seguridad informática*, y para su análisis y cotejo debe realizarse primero una *copia o imagen forense* [10] de su original mediante *softwares* autorizados al efecto.

Para obtenerla, lo correcto es realizar el "espejo" o clon del dispositivo, es decir, una copia completa, sector por sector *(bit a bit)*, del medio de origen. En consecuencia, se obtiene una réplica perfecta de la estructura y contenido del dispositivo a peritar (incluyendo los espacios no utilizados). Esta copia se realiza con el fin de preservar su original, para que no sea contaminado mediante su análisis, ya sea en sede policial o judicial.

Posteriormente, corresponde autenticar dicha evidencia (imagen forense) mediante el cálculo de firmas digitales, empleando para ello la utilización de algoritmos de *hash* de los bits clonados durante el proceso —ello permite asegurar que su contenido no ha sido alterado—, lo cual posibilita la manipulación de la prueba sin riesgo de contaminación. En caso de modificación, el valor *hash* que fue asignado será distinto, motivo por el cual siempre debe trabajarse sobre la copia clonada (copia forense). Es decir, la firma garantiza la integridad y autenticidad de la evidencia digital recolectada.

Todo ello implica que, a falta de sistemas operativos correspondientes y formación en la materia, los operadores judiciales se vean atados de pies y manos para realizarla, necesitando siempre de un experto en informática forense con el objetivo de no contaminar la prueba.

Tip número uno: siempre realizar la imagen forense de cualquier dispositivo electrónico secuestrado y autenticar la evidencia recolectada mediante herramientas de cifrado para crear valores *hash*.

[10] Es un archivo o conjunto de archivos que contiene la estructura y contenidos completos de un dispositivo de almacenamiento de datos (como ser un disco duro, CD, DVD, pendrive, memoria flash, SD, etc.).

En el caso contra Ricardo Jaime[11], las evidencias recolectadas terminaron no siendo útiles, puesto que se constató que, por no habérselas resguardado mediante los mecanismos de seguridad informática forense, se contaminó la prueba, lo que conllevó la nulidad de los peritajes oportunamente realizados.

Es así que hoy en día todo procedimiento penal, para culminar con el dictado de una sentencia, requiere la incorporación de nuevas herramientas que permitan probar o refutar los hechos imputados. Cobran entonces especial relevancia los dictámenes periciales y las testimoniales que los expertos puedan brindar ante los magistrados para esclarecer el funcionamiento de sistemas que escapan al ámbito jurídico.

La tecnología ha incidido de manera tal en la vida de los seres humanos que se ha desparramado por todo el ámbito del derecho penal, dando surgimiento, incluso, a "nuevas conductas" (o nuevos medios para cometer las mismas conductas). A modo de ejemplo, piénsese en el hackeo de cuentas bancarias, las extorsiones digitales, el *phishing* —fraude informático mediante correos electrónicos—, *sexting* —envío de mensajes eróticos o sexuales por celular—, *grooming*, la tenencia, producción o distribución de material sexual infantil, entre otras, todas las cuales, para consumarse, requieren entornos digitales o la utilización de la tecnología en algún instante de su *iter criminis* y para probarse válidamente en un juicio, la evidencia digital.

La intromisión del mundo digital en la cotidianeidad de todos nosotros ha sido tal que fue necesario introducir, mediante la sanción a la ley 26.388, en el Cód. Penal de la Nación, conductas tales como el daño informático, el fraude informático y la protección de datos personales, entre otros tantos. Posteriormente, mediante la ley 26.904, se sancionó también como delito el *grooming*.

Como puede advertirse sin mayor esfuerzo, el denominador común para sostener un procedimiento penal válido respecto de todas estas conductas es la necesidad de recolectar la prueba que subyace de tales delitos: nuevamente la "evidencia digital".

II. SISTEMA DE GARANTIAS Y EVIDENCIA DIGITAL.

Algunas consideraciones sobre el derecho a la privacidad en la Argentina y las técnicas especiales de investigación en la era digital

El sistema jurídico argentino, en cuanto a las personas particularmente consideradas, se compone de normas en forma de mandatos y prohibiciones (art. 19, CN). Pero también, en muchos casos de actividades fuertemente regladas o en situaciones conflictivas, existen normas permisivas para evitar confusiones y delimitar el ejercicio de derechos en casos particulares. En todos los demás supuestos, en los que la ley nada dice, se constituye una zona de libertad de todos los habitantes (art. 19, CN), que gozan de derechos preexistentes a

[11] www.cij.gov.ar/nota-9170-La-C-mara-Federal-confirm—la-anulaci-n-de-peritaje-sobre-mails-en-causa-contra-Jaime-.html.

la Constitución misma (art. 33, CN). Distinto es el problema de cuándo y en qué circunstancias la ley puede reglar una actividad (art. 19, CN, cuando perjudique a terceros). Tratándose de funcionarios públicos la cuestión se invierte, ya que solo están facultados a hacer lo que la ley y los reglamentos dictados en consecuencia les permiten hacer, delimitando su actuación dentro del ámbito de su competencia institucional.

El derecho a la privacidad y su protección frente a injerencias arbitrarias ha sido consagrado a nivel internacional en el art. 12 de la Declaración Universal de los Derechos Humanos, en los arts. V, IX y X de la Declaración Americana de los Derechos y Deberes del Hombre, en el art. 17 del Pacto Internacional de los Derechos Civiles y Políticos y en el art. 11 de la Convención Americana de Derechos Humanos. Por otro lado, las garantías y derechos individuales previstos en la conjunción de los arts. 19 y 33 de la CN, son anteriores a la conformación del Estado y no necesitan su reconocimiento expreso, sino que están implícitos. Ya el decreto de Seguridad Individual del 23 de noviembre de 1811 establecía: "... Todo ciudadano tiene un derecho sagrado a la protección de su vida, de su honor, de su libertad y de sus propiedades. La posesión de este derecho, centro de la libertad civil y principio de todas las instituciones sociales, es lo que se llama seguridad individual. Una vez que se haya violado esta posesión ya no hay seguridad, se adormecen los sentimientos nobles del hombre libre y sucede la quietud funesta del egoísmo. Solo la confianza pública es capaz de curar esta enfermedad política, la más peligrosa de los Estados, y solo una garantía, afianzada en una ley fundamental, es capaz de restablecerla..."

El corpus de derechos individuales que permiten establecer límites a la potestad del Estado en este ámbito de libertad exige que la intervención en esos derechos siempre sea fundada en ley dónde se prevean aquellas circunstancias que habiliten y justifiquen el ejercicio de la autoridad estatal. Entonces, ¿cuál es el alcance de las restricciones? El art. 30 de la CADH establece: "Las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas". La OC 6/86 de la Corte IDH ha establecido por unanimidad que la palabra "leyes" en el mencionado artículo "significa norma jurídica de carácter general, ceñida al bien común, emanada de los órganos legislativos constitucionalmente previstos y democráticamente elegidos, y elaborada según el procedimiento establecido por las constituciones de los Estados Partes para la formación de las leyes".

De lo expuesto se extrae que las limitaciones deben cumplir las siguientes condiciones: 1) que se trate de una restricción expresamente autorizada por la Convención y en las condiciones particulares en que ha sido permitida; 2) que los fines para los cuales se establece la restricción sean legítimos, que obedezcan a razones de interés general y no se aparten del propósito para el cual se establecieron; 3) que tales restricciones estén dispuestas por las leyes y se apliquen de conformidad con ellas (párr. 18); 4) que no basta la conveniencia o utilidad, sino que también debe ser estrictamente necesaria en una sociedad democrática, de modo que justificará la pretensión de proteger a las mayorías de una conducta considerada por ellas ofensiva (párrs. 77-81).

En la legislación local existen limitaciones formales relativas a la protección de la intimidad, la vida privada, la salud e incluso la propiedad particular, bienes cuya afectación

solo está permitida bajo condiciones formales rigurosas. Por ejemplo, la protección del domicilio, mediante la regulación de las condiciones del allanamiento de morada; en la protección del secreto de las comunicaciones con otras personas, mediante la regulación de las condiciones para interceptar y abrir la correspondencia (comprendidas las comunicaciones escritas por medios modernos) o las comunicaciones telefónicas (también el registro de llamadas entrantes y salientes) o inalámbricas, o mediante el deber impuesto por la propia ley penal de guardar el secreto, según ciertas relaciones de confianza; en la protección de la propiedad, mediante las reglas que reglamentan el secuestro.

En lo relativo a las comunicaciones, por regla general, las leyes procesales argentinas permiten su interceptación cualquiera fuere el medio tecnológico empleado para conectarse. En este contexto, la intimidad significa un ámbito de reserva dentro del cual el mismo portador de ese interés jurídico sustrae el contenido material de la comunicación con otros del conocimiento de otras personas que no intervienen en ella o no tienen autorización para acceder a ese contenido. Una injerencia extraña en ese ámbito, de alguna persona no autorizada, privada o pública es en principio ilegítima, salvo que la ley lo autorice. Parece necesario en estos casos, la autorización judicial, como mínimo recaudo formal a cumplir por el investigador para legitimar la medida y sus consecuencias hacia futuro, y que las condiciones para conceder la autorización estén determinadas por la ley, conforme al principio *nulla coactio sine lege*.

De hecho, en cuanto a la apertura y examen de la correspondencia, la ley prevé que debe ser el juez, *por sí mismo*, quien lleve adelante esa tarea en presencia del secretario (art. 235, Cód. Proc. Penal de la Nación, según ley 23.984), dada la especial naturaleza de su contenido y el grado de afectación que la medida implica. Si bien el principio de libertad probatoria admite que todos los hechos del proceso pueden acreditarse por cualquier medio de prueba, ello no debe interpretarse como una habilitación a las autoridades gubernamentales para hacer todo lo que creativamente se les ocurra. Rige el principio general: las injerencias deben estar previstas por ley.

El criterio para determinar si una injerencia es arbitraria o no, está dado por la proporcionalidad entre la medida intrusiva y el fin que esta persigue. Para que la actividad de los órganos estatales sobre los individuos sea considerada proporcional debe verificarse la necesidad previa o concomitante de la injerencia y una posterior ponderación de bienes (costos y beneficios que alguien debe soportar o gozar) en conflicto. La injerencia debe ser idónea, y no debe haber otra medida subsidiaria que produzca menos daño en los derechos.

La declaración de ilegalidad o inconstitucionalidad de todas las injerencias que haya sufrido una persona tendrá sentido solo cuando aquellas fueron el origen del descubrimiento de pruebas de la comisión de un delito. Es decir, debe haber una relación entre la injerencia arbitraria y la adquisición de prueba para declarar la invalidez de esta última. La causa probable debe tener relación con el delito que se sospecha, no se admiten discordancias. Este aspecto también se relaciona con la prohibición constitucional de las "expediciones de pesca", a través de las cuales se invade toda zona de privacidad de aquella persona que se sospecha que está cometiendo un delito, con la finalidad de encontrar o mejor dicho "pescar" pruebas de su comisión, y que no requieren "indicios vehementes de culpabilidad". Ese método viola la exigencia constitucional de existencia previa de "causa probable" para

actuar sobre la persona y sus derechos. El conjunto de los actos preventivos de la autoridad debe respetar los estándares que se mencionaron y la calidad procesal que las leyes exijan según el caso.

Como se ve, el problema no se limita solamente a la previsión legal porque la norma procesal puede entrar en conflicto con la Constitución si se autoriza un criterio de actuación subjetivo a las autoridades, una autorización en blanco que impida el control judicial posterior y no dé seguridad a los ciudadanos sobre qué pueden mantener en su privacidad y qué no.

Párrafo aparte merecen las nuevas técnicas especiales de investigación para delitos complejos, que tienen una estrecha relación con los principios que se vienen enunciando y son tema de debate en la agenda procesal.

Por otra parte, quedaron fuera de la reforma las medidas de vigilancia electrónica que estaban previstas en el texto inicial del Proyecto: "a) Vigilancia acústica: escucha y grabación en forma no ostensible, a través de medios técnicos de las conversaciones privadas del imputado que tengan lugar fuera del domicilio de cualquiera de los Interlocutores; b) Vigilancia remota sobre equipos informáticos: es la utilización no ostensible de un *software* que permita o facilite el acceso remoto al contenido de ordenadores, dispositivos electrónicos, sistemas informáticos, bases de datos o instrumentos de almacenamiento masivo de datos informáticos. El fiscal que solicita esa medida debe precisar los datos o archivos informáticos que procura obtener y la forma en que se procederá al acceso o captación, la identificación del *software* a utilizar, y a Individualización de los ordenadores, dispositivos electrónicos, sistemas informáticos, bases de datos o instrumentos de almacenamiento masivo de datos informáticos que serán objeto de la medida; c) Vigilancia a través de dispositivos de captación de imagen: es la captación y grabación de imágenes del imputado en espacios públicos en forma no ostensible por cualquier medio técnico; d) Vigilancia a través de dispositivos de seguimiento y de localización: es la que utiliza de manera no ostensible dispositivos o medios técnicos de seguimiento y de localización, debiendo especificar el fiscal que lo solicita el medió técnico a emplear. Las medidas contempladas en este artículo no serán autorizadas respecto de terceros ajenos a la investigación. Sin perjuicio de ello podrán llevarse a cabo aun cuando tuvieren efectos inevitables sobre terceros ajenos a la investigación".

A nivel nacional, mediante la ley 27.482 se modificó el Código Procesal Penal de la Nación incorporándose al tít. VI, del Libro Cuarto de la Primera Parte del Código aprobado por el art. 1º de la ley 27.063, el art. 175 bis, que contempla técnicas especiales de investigación, que solo podrán ser solicitadas al juez por el Ministerio Público Fiscal y para los casos que allí se establece. Pueden mencionarse el agente revelador, el informante, el agente encubierto y la entrega vigilada, sin perjuicio de que ya se encontraban vigentes mediante la ley 27.319 de delitos complejos que aquí se incorporó.

Por otro lado, en cuanto a la interceptación de las comunicaciones, en el art. 25 se sustituyó el art. 143 del Código aprobado por la ley 27.063, y se estableció: "Siempre que resulte útil para la comprobación del delito, el juez podrá ordenar, a petición de parte, la interceptación

y secuestro de la correspondencia postal, telegráfica, electrónica o cualquier otra forma de comunicación o de todo otro efecto remitido por el imputado o destinado a este, aunque sea bajo nombre supuesto.

"Se procederá de modo análogo al allanamiento"

"La intervención de comunicaciones tendrá carácter excepcional y solo podrá efectuarse por un plazo máximo de treinta [30] días, pudiendo ser renovada, expresando los motivos que justifican la extensión del plazo conforme la naturaleza y circunstancias del hecho investigado.

"La solicitud deberá indicar el plazo de duración que estime necesario según las circunstancias del caso. El juez controlará la legalidad y razonabilidad del requerimiento y resolverá fundadamente (...).

"(...) Las empresas que brinden el servicio de comunicación deberán posibilitar el cumplimiento inmediato de la diligencia, bajo apercibimiento de incurrir en responsabilidad penal.

"Si los elementos de convicción tenidos en consideración para ordenar la medida desaparecieren, hubiere transcurrido su plazo de duración o esta hubiere alcanzado su objeto, deberá ser interrumpida inmediatamente".

Los capítulos referidos a vigilancia remota de dispositivos electrónicos ya habían sido excluidos al otorgarle media sanción al texto del proyecto en el Senado luego de un extenso debate con la opinión de expertos y de organizaciones civiles y de derechos humanos. El derecho a la privacidad en la era digital no es un tema menor.

Al respecto, el Consejo de Derechos Humanos de la ONU, mediante la res. 34/7 del 22/03/2017, puso de relieve que la vigilancia y/o la interceptación ilegales o arbitrarias de las comunicaciones, así como la recopilación ilegal o arbitraria de datos personales, al constituir actos de intrusión grave, violan el derecho a la privacidad y pueden interferir con otros derechos humanos, incluido el derecho a la libertad de expresión y a abrigar opiniones sin injerencias, y el derecho a la libertad de reunión y asociación pacíficas, y ser contrarios a los preceptos de una sociedad democrática, en particular cuando se llevan a cabo extraterritorialmente o a gran escala. Asimismo, que los Estados deben respetar las obligaciones internacionales de derechos humanos en lo referente al derecho a la privacidad cuando intercepten las comunicaciones digitales de las personas y/o reúnan datos personales y cuando exijan a terceros, incluidas las empresas, su divulgación. Finalmente, se exhorta a los Estados a que "a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales; b) Adopten medidas para poner fin a las violaciones del derecho a la privacidad y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos; c) Examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé

cumplimiento pleno y efectivo a todas sus obligaciones en virtud del derecho internacional de los derechos humanos; d) Establezcan o mantengan mecanismos nacionales de supervisión, de índole judicial, administrativa o parlamentaria, que cuenten con los recursos necesarios y sean independientes, efectivos e imparciales, así como capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado; (...) i) Se abstengan de exigir a las empresas que adopten medidas que interfieran con el derecho a la privacidad de manera arbitraria o ilegal (...)" .

Finalmente, en materia de delitos informáticos, el rápido y constante avance y modificación de las Tecnologías de la Información y la Comunicación (TIC) siempre va delante de las reformas legislativas, por lo que la tarea de los investigadores es más dificultosa y requiere de suma cautela. En cuanto a las técnicas de investigación que se emplean y su relación con la afectación a los derechos constitucionales en materia de datos personales, existe una categorización sobre ellos aceptada a nivel internacional. Según sea el grado de injerencia o afectación que generan las medidas de investigación penal, se requerirá orden judicial o no para su acceso. La doctrina utiliza la metáfora de una escalera para ejemplificarlo de una manera más clara. Veamos.

Sobre la base se posicionan aquellos datos considerados de acceso público, de forma irrestricta y por cualquier persona, sin vulnerar ninguna barrera técnica o jurídica. Es ampliamente aceptada por la jurisprudencia la introducción de estos datos a una investigación criminal en curso sin que ello implique una intromisión arbitraria en la privacidad o intimidad del imputado. Luego, en un primer escalón, se encuentran los datos del abonado o de identificación de usuario o titular de la cuenta-servicio a consultar. Es toda información (generalmente datos personales), que posea un proveedor de servicios, relacionada con el abonado, que no sean ni datos de tráfico ni datos de contenido. Si bien son datos de carácter personal, que avanzan sobre una primera barrera de privacidad de la persona investigada, se podrá acceder a ellos sin contar con el consentimiento del titular para aquellos casos de ejercicio de funciones propias del Estado (art. 5.2.b de la ley 25.326) e incorporarlos a una investigación criminal con una orden del fiscal a cargo, sin necesidad de autorización judicial. En el segundo escalón, se ubican los datos de tráfico, también conocidos como asociados o transaccionales. Puede interpretarse que los registros de un servidor que guarda las comunicaciones electrónicas entrantes y salientes son un listado de datos de tráfico, toda vez que incluyen la dirección IP de origen y destino, fecha, hora y ruta de la comunicación . Definición que también se aplica a las "listas sábanas" de las llamadas telefónicas. Será necesario contar con la orden del juez competente para acceder a ellos. Por último, en el tercer escalón, se ubican los datos de contenido. Se tratan del propio mensaje que el emisor envía a uno o más receptores, cualquiera sea el medio utilizado (carta, fax, llamada telefónica, WhatsApp o correo electrónico). Es el nivel de afectación más profundo y supera todas las barreras de intimidad del titular, por lo que deberá contarse con orden judicial debidamente fundada para acceder a ellos.

II.II Privacidad, intimidad y secreto en las comunicaciones.

Más allá del estrecho vínculo que los uno, estos conceptos no tienen el mismo alcance. En nuestra materia, dado el constante roce entre las actividades que despliegan los funcionarios

policiales en la prevención y represión del delito y la libertad personal, nos hemos habituado a utilizar intimidad, ámbito de protección personal, vida privada o esfera familiar como sinónimos, otorgándoles el mismo alcance a la hora de analizar especialmente las exclusiones probatorias y demás planteos invalidantes.
Incluso a propi CSJN en el conocido caso ·PONZETTI DE BALBIN", enlaza libertad individual, privacidad e intimidad sobre un ámbito de autonomía individual constituida por sentimientos, hábitos y costumbres, las relaciones de familia, la situación económica, creencias religiosas, salud mental y física, en suma, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad, están reservadas al propio individuo y cuyo conocimiento y divulgación por extraños significa un peligro real o potencial para la intimidad.
La necesidad de prevenir la comisión de delitos se encuentra en constante tensión con la necesidad de preservar ámbitos reservados para el desarrollo de la persona y la protección de su dignidad. Esta tensión se potencia con las nuevas tecnologías y el mayor potencial de daño que pueden causar, a la par de constituir una herramienta inigualable de rastreo y vigilancia de todas las actividades humanas.

- PRIVACIDAD:

Tiene un sentido amplio y de mayor alcance que la intimidad y se refiere a diversos aspectos que hacen al desarrollo de la persona, sus gustos, pensamientos, actividades, preferencias, hobbies, lo que en su conjunto arrojan un perfil del sujeto en cuanto a sus preocupaciones, necesidades o proyectos. Estas cuestiones aisladamente quizás n tengan significado per en su conjunto marcan la personalidad del sujeto, lo definen como un ser único e individual.
La CJSN ha dicho qu el art. 19 de la CN establece la existencia de una esfera privada de acción de los hombres en la que no puede inmiscuirse ni el Estado ni ninguna de las formas que los particulares organizan como factores de poder, constituyendo el orden y la moral públicos y los derechos de terceros el poco flexible límite que circunscribe el campo de la inmunidad de acciones privadas.
En este sentido ha señalado que el Estado debe garantizar y promover el derecho de los particulares a programar y proyectar su vida según sus propios ideales de existencia.

La garantía contra injerencias arbitrarias a la privacidad se vincula a la persona independientemente del espacio físico en que desarrolle la actividad. La Corte nacional entiende que privacidad no solo comprende la esfera doméstica, el círculo familiar y de amistad, sino otros aspectos de la personalidad espiritual o física de las personas tales como su integridad corporal o la imagen y nadie puede inmiscuirse en la "vida privada" de una persona ni violar áreas de su actividad destinadas a no ser difundidas sin su consentimiento o el de sus familiares autorizados y solo la ley podría justificar la intromisión siempre que medie un interés superior en resguardo de la libertad de otros, la defensa de la sociedad, las buenas costumbres o la persecución de un crimen [12]

[12] CSJN, 11/12/83 "PONZETTI DE BALBIN". De este modo la privacidad es un elemento clave en la vida en democracia, independientemente del espacio en que las actividad des humanas se desarrollan y de la naturaleza de los instrumentos usados para indicarla y abarca: a) el secreto de los actos privados; b) el

Según la Corte de los EE.UU "la cabaña más frágil del reino" tiene absolutamente las mismas garantías de privacidad que la mansión más majestuosa
El TEDH, por su parte ha señalado que "vida privada" es una noción amplia al sostener que sería demasiado restrictivo limitar la noción a un "círculo interno" en el cual el individuo puede vivir su propia vida personal como èl elige y excluir de ella completamente al mundo exterior. En efecto, para el tribunal, el respeto por la vida privada también debe comprender, hasta cierto punto, el derecho a establecer y desarrollar relaciones con otros seres humanos. [13]
Así, para el TEDH la vida privada abarca la integridad física y moral de la persona[14], puede engloabar aspectos de la identidad física y social de un individuo[15] incluyendo elementos como la identificación sexual, el nombre, la orientación sexual y la vida sexual, los que considera dentro de las esfera de la protegida por el art.º de la CEDH, también protege el derecho al desarrollo personal y a establecer y mantener relacione con otros seres humanos y el mundo exterior, descartando que el derecho a la vida privada puede englobar el derecho a la muerte asistida, lo que para el TEDH llevaría consigo la negación de la protección que el convenio trata de ofrecer.
Vemos entonces que "privacidad" no es un concepto rígido, estático, vinculado a un sitio o aspecto específico sino a un conjunto de aspectos que hacen al desarrollo de la personalidad humana lo que desdibuja en la idea de ubicar exclusivamente a la privacidad dentro de una actividad, perfil, ámbito o sitio determinado, más la conforma el conjunto de actividades, posturas, formas de hacer, ser o pensar que pueden o no exteriorizarse pero que, en sí forman parte de lo que la persona hace, cree, crea o piensa.

- <u>INTIMIDAD</u>:

Como presupuesto de libertad personal, es el ámbito físico y espiritual en donde el sujeto se desarrolla. Es el ámbito reservado de la persona en donde desarrolla sus diversas facetas y que autoriza a excluir a terceros de su conocimiento, difusión o divulgación. [16] La

---

secreto en las comunicaciones; c) el derecho a la propia imagen; d) el derecho al nombre; e) el secreto profesional (Romero Villanueva – Grisetti, Còdigo Procesal de la Nación.

[13] TEDH 16/12/92 "NIEMITZ VS. ALEMANIA". E l tribunal no hace diferencia entre actividades profesionales o comerciales para excluirlas del concepto de vida privada, incluso ha cubierto las llamadas telefónicas comerciales como privadas. Respecto de la palabra "hogar" la ha extendido a los locales comerciales, dándole una connotación más amplia: "domicilio" lo que permite llevarla a la oficina profesional. E ese sentido el Tribunal busca proteger al individuo de toda injerencia arbitraria por parte de las autoridades públicas se trate de un hogar, una oficina o un local comercial.

[14] TEDH, 26/3/85, "X. e Y. v. PAISES BAJOS", 4, serie A, Nº 91, P. 11, AP. 22.

[15] "MIKULIC V. CROACIA" Nº 53176/1999 sec. 1, 7/2/02 TEDH en su interpretación extensiva del concepto "ida " privada del art. 8 del Convenio europeo para la protección de los derechos y de las libertades fundamentales en la sent, del 16/2/00 dictada en el caso "Amann v. Suiza", que "el término 'vida privada' no se debe interpretar de forma 'restrictiva', de forma que este "engloba el derecho del individuo de crear y desarrollar relaciones con sus semejantes" sin que "ninguna razón de principio permita excluir las actividades profesionales o comerciales"

[16] NINO refiere a la intimidad como la esfera personal que está exenta del conocimiento generalizado de terceros distinguiéndola de privacidad la que define como la posibilidad irrestricta de realizar acciones

injerencia o perturbación de este ámbito nuclear lesiona el proyecto existencial personal contrariando la garantía de inmunidad contenida en el art. 19 de la CN tal como lo ha reconocido la CSJN en "Comunidad Homosexual Argentina" y "Albarracini Nieves", entre otros. Se la entiende como un "poder de control" sobre la publicidad de la información relativa a la persona y la familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público. Se garantiza así el derecho al secreto, a que los demás no sepan qué somos o qué hacemos, vedando que terceros sean particulares o poderes públicos, decidan cuáles son los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, cualquiera sea el contenido de ese espacio.[17]

Ahora bien, una cosa es afirmar que las personas tienen derecho a un ámbito de reserva personal excluido de la injerencia ajena, y otra cosa bien distinta consiste en determinar el contenido y alcance de esa tutela constitucional. En principio, existe unanimidad en que el domicilio personal constituye sin hesitar un ámbito privado en el cual el individuo puede desarrollar su potencialidad de manera aislada o junto a otros que integran el núcleo familiar[18]. El término "vida privada" debe ser interpretado de manera extensiva, ya que en él se engloba el derecho de todo individuo de generar y desarrollar relaciones con sus semejantes, entre las que se incluyen las relaciones profesionales y comerciales [19]. Sin embargo, la doctrina judicial nacional ha establecido algunas excepciones dignas de mención, por ejemplo, el camarote de un barco ha sido asimilado al concepto de "domicilio", pero se ha afirmado que la expectativa a la privacidad se limita solo respecto de las conductas de otros tripulantes o de terceros, pero no así del capitán de la embarcación que, en el cumplimiento de sus funciones (arts. 120, 130 y 131 de la ley 20.094), tiene acceso franco al interior del camarote, así como autorizar al ingreso de funcionarios de seguridad.[20]

Asimismo, los datos almacenados en un teléfono celular (contactos, fotos, vídeos) están alcanzados por la tutela constitucional del derecho a la intimidad y la expectativa a la privacidad, en cuyo caso cualquier injerencia arbitraria por parte de las autoridades públicas habrá de desencadenar la nulidad de toda fuente de prueba que pueda ser utilizada en contra

---

privadas que no puedan dañar a otros por más que se cumplan a la vista de los demás y sean conocidas por estos (fundamentos de derechos Constitucional, 1992, 9. 325)

[17] STD 134/1999, del 15 de JULIO. Así la intimidad es una reserva de conocimiento de un ámbito personal al que se denomina privado y que administra su titular. Ese ámbito se devalúa ante la intromisión ajena. De este modo, la intimidad se vincula con la "libertad", con la "calidad mínima de vida humana", STC 231/1988, del 2 de diciembre, STC 89/2006, del 27 de marzo. ·El derecho a la intimidad personal, consagrado en el art. 18.1 de la CE (…) se configura como un derecho fundamental estrictamente vinculado a la propia personalidad y que deriva de la dignidad de la persona que el art. 10.1 de la CE reconoce e implica "la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana" (STC, del 23 de marzo, STC 241/2012, del 17 de diciembre).

[18] CSJN, Fallos 298:723 (Mieres); 306:1752 (Fiorentino); 328:149 (Ventura).

[19] TEDH, "Amann c. Suisse", (Requete nº 27798/95), del 16/2/00, parág. 65, con cita de los precedentes "Niemietz c. Allemagne", del 16/12/92, serie A nº 251-B, pp. 33-34, parág. 29, y "Halford c. Royaume-Uni", del 25/6/97, Recueil des arrets et décisions 1997-III, p. 1015-1016, parág. 42; "P.G. et J.H. c. Royaume-Uni", del 25/12/01, parág. 56.

[20] CSJN, Fallos 311:2171.

del afectado, siendo imperioso en estos casos la habilitación derivada de una orden judicial. Sin embargo, este principio rector en materia de tutela de derechos constitucionales como la intimidad y la expectativa a la privacidad ha sido morigerado en algunos supuestos, por ejemplo, en el caso de delitos sexuales sufridos por menores de edad mediante el uso de sistemas de comunicación informáticos (*grooming*, exhibiciones sexuales, distribución de material pornográfico), en cuyo caso el consentimiento prestado por el titular del ejercicio de la responsabilidad parental respecto de la clave de acceso al dispositivo electrónico de la menor con el propósito de reunir prueba de cargo contra el acusado no requiere orden judicial previa[21] ya que se deriva del ejercicio legítimo de un derecho y deber al mismo tiempo de los progenitores por salvaguardar la integridad psicofísica de sus hijos.

En general, podemos afirmar que el concepto de "intimidad" no solo incluye al derecho de estar solo, sino también las relaciones intersubjetivas que mantiene el individuo en el ejercicio de su autodeterminación personal que carecen de lesividad hacia terceros y que constituyen el núcleo básico de la expresión de su forma de ser, pensar y actuar. En este sentido, entonces, no debe extrañarnos que las relaciones sexuales con un tercero hayan sido abarcadas por el derecho a la intimidad y la expectativa a la privacidad dimanante de su ejercicio[22]

Hoy en día la definición de privacidad debe abarcar la autodeterminación informativa respecto de los datos personales, la libertad de comunicación telemática como expresión de valor del significado y el impacto de las nuevas tecnologías en la vida moderna[23]. El correo postal ha perdido en gran parte su importancia pretérita frente al avance de los medios telemáticos, donde el sujeto también se construye en una dimensión espacio-digital que debe ser amparada en igual forma y con el mismo vigor que la libertad de comunicación escrita. Por este motivo, la primera conceptualización del término "privacidad" en el doctrina y jurisprudencia norteamericanas identificada con el "derecho de estar solo o a no ser molestado" ("the right to be let alone")[24] ha experimentado un giro copernicano ante la nueva realidad tecnológica que ofrece la era digital[25]. Mientras que el dominio individual sobre la esfera de privacidad en el siglo XIX aseguraba en gran medida la posibilidad de excluir intromisiones ajenas, en la actualidad ese margen de acción ha quedado claramente reducido *por mor* de las nuevas técnicas desarrolladas por el avance tecnológico que auguran en un futuro próximo la maximización del control social por parte del Estado y los especialistas. El tratamiento y almacenamiento de datos personales obtenidos de los registros digitales de los usuarios de las redes telemáticas en la moderna sociedad imponen

[21] STS, Sala de lo Penal, Resolución Nº 864/15, del 10/12/15 (Ponente Antonio Del Moral García).

[22] CSJN, Fallos 325:2520 (Maradona); "Lawrence v. Texas", 539 U.S. 558 (2003). En este sentido, Fillia/Sueiro/Monteleone/Nager/Rosende, "Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación (ley 26.388)", LA LEY, 2008-E, 938.

[23] TEDH, "Amann c. Suisse", parág. 70 y 80. Respecto del almacenamiento y tratamiento de datos personales por parte de los organismos de seguridad públicos, cfr. "P.G. et J.H. c. Royaume-Uni", del 25/12/01, parág. 57. Al respecto, Muñoz Conde, Derecho penal. Parte especial, p. 256; Riquert, Protección penal de la intimidad en el espacio virtual, p. 51 y ss., p. 195 y ss.

[24]Warren/Brandeis, "The Right to Privacy", Harvard Law Review, Vol. IV (1890), Nº 5

[25] CSJN, Fallos 314:1517 (Vago), considerandos 5º y 8º. Al respecto, FERREYRA, "¿Tienes un correo electrónico para comunicarte? Observaciones en torno a la equiparación, en el ámbito del ordenamiento constitucional, de la correspondencia enviada por correo electrónico (e-mail)", JA 2004-I, p. 1188

un nuevo paradigma al concepto de privacidad, ya que la intimidad no puede ser entendida y limitada a los conceptos de "domicilio" y "papeles privados"[26] para graficar las manifestaciones más remotas de este ámbito de intimidad[27]. Por el contrario, se hace necesario, aunque resulte una empresa difícil, extender ese concepto a otras áreas adyacentes que reflejan también la condición de posibilidad del ejercicio de la autodeterminación individual exenta de toda injerencia arbitraria (por ejemplo, la propia imagen) [28]

En síntesis, las acciones privadas están definidas de modo negativo por el art. 19 de nuestra Constitución y ampara tan solo un aspecto de la esfera de la intimidad personal referida a las conductas autorreferenciales, pero a ello debe agregarse que la tutela constitucional se extiende a la expectativa a la privacidad o confidencialidad de esas conductas solipsistas como las intersubjetivas.[29] El derecho a la expresión de ideas y su correlato con la libertad de comunicación engarzan de manera directa con el ámbito de tutela penal previsto por este artículo 153 del Código Penal argentino.

El derecho a la intimidad y la expectativa a la privacidad imponen en la moderna sociedad informática el empleo de un criterio dinámico para apreciar su contenido y alcance[30]. En la actualidad, los medios técnicos existentes de acuerdo al grado de evolución alcanzado por nuestra sociedad tecnológica obligan al intérprete a adoptar una postura cautelosa que permita ampliar las zonas de privacidad en lugar de restringir su espacio. Mientras que el ámbito de lo privado podía identificarse en el siglo XIX con el domicilio, las comunicaciones escritas y los papeles privados, en la actualidad ese enfoque aparece desnaturalizado por el avance de los medios tecnológicos[31]. Piénsese, por ejemplo, que existen una multiplicidad de datos sensibles (laborales, médicos, financieros, sociales, religiosos, políticos, etc.) que están alcanzados por el concepto de intimidad y el derecho a la expectativa a la privacidad[32], siendo necesaria su tutela jurídica efectiva contra conductas que menoscaban su integridad y disponibilidad (v. gr., "skimming")[33]. En la era digital, las

[26] CSJN, Fallos 46:36 (Charles Hnos.).

[27] Por ejemplo, incluyendo las comunicaciones telefónicas, cfr. CIDH, caso "Tristán Donoso vs. Panamá". Excepciones Preliminares, Fondo, Reparaciones y Costas, sentencia del 27/1/09, Serie C, Nº 193, párr. 55.

[28] CSJN, Fallos 298:723 (Mieres); 306:1892 (Ponzetti de Balbín).

[29] BIDART CAMPOS, "Tratado elemental de derecho constitucional argentino", t. I-B, p. 61; NINO, "Fundamentos de derecho constitucional", p. 304 y ss., pp. 307 y ss.

[30] Maurach/Schroeder/Maiwald, Strafrecht. BT 1, 9. Aufl., Müller, Heidelberg, 2003, parág. 29 I 8, Saldaña, "La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de la información personal en los Estados Unidos", pp. 88 y ss.; García González, "Protección penal de la intimidad: El art. 197, 1°, del Código Penal", Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet, Javier García González (coord.), Tirant lo blanch, Monografías, N° 696, Valencia, 2010, pp. 113 y ss.

[31] Hilgendorf/Frank/Valerius, Computer-und Internetstrafrecht, p. 11 y ss.

[32] Así lo reconoce de manera expresa la doctrina del Tribunal Constitucional español (SSTC, Nº 98/2000, del 10/4/00; Nº 186/2000, del 10/7/00; Nº 170/2013, del 7/10/13). En este sentido, STS, Sala de lo Penal, N° de Resolución 553/2015, del 6/10/15 (Ponente Juan Ramón Berdugo Gómez de la Torre). Por su parte, el TEDH, "Iliya Stefanov v. Bulgaria", (Application nº 65755/01), del 22/8/08, parág. 42, ha señalado que los documentos profesionales, el ordenador y los datos almacenados integran el ámbito de reserva personal excluido de injerencias arbitrarias.

[33] Bachmann/Goeck, "Strafrechtliche Aspekte des Skimmings - zugleich Anmerkung zu BGH, Urt. v. 17.2.2011 - 3 StR 419/10", JR 10/2011, pp. 425 y

relaciones intersubjetivas se han incrementado de manera exponencial y, en igual medida, las posibilidades siempre latentes de vulnerar la intimidad y la expectativa de exclusión de la injerencia ajena. Al respecto, se habla de la necesidad de una "convergencia de medios" ("Konvergenz der Medien") para explicar el proceso de adaptación técnico, empresarial y jurídico de las nuevas formas de comunicación en la sociedad de la información [34]

En los últimos tiempos, la confidencialidad de los datos electrónicos abarca no solo los correos electrónicos, sino también los datos almacenados en sistemas telemáticos como en los ordenadores y teléfonos digitales. A continuación, analizaremos el delito de acceso indebido al correo electrónico regulado por el art. 153 del Código Penal en relación con los casos cada vez más frecuentes de ejercicio arbitrario del derecho de dirección y control de la empresa por parte de sus directivos que se proyecta en la praxis en la revisión del correo electrónico de sus dependientes.

En materia de tutela penal de la intimidad, y más allá de lo arduo de la empresa de brindar un concepto material de intimidad adecuado a los tiempos modernos que corren, podemos afirmar que la ley constitucional resguarda el derecho a la intimidad y la privacidad de un modo amplio. La intimidad puede ser definida a partir de una contextualización meramente autorreferencial basada en el derecho de estar solo, pero ella resulta claramente insuficiente en la actual era de la información y la comunicación digital. Las condiciones de posibilidad de ampliar el horizonte de nuestra esfera de privacidad a partir de los adelantos tecnológicos nos enseñan que la privacidad se extiende sin duda alguna a todas aquellas relaciones intersubjetivas no dañinas para terceros por parte de sujetos responsables. En este marco de ejercicio de esta autonomía personal, el Estado tiene el deber de no practicar injerencias indebidas en el ámbito de la vida personal de cada uno de los integrantes de la comunidad organizada, al mismo tiempo que debe prevenir y reprimir los atentados por parte de funcionarios públicos o particulares contra esa zona de autonomía personal.

En particular, los arts. 153 y 153 bis del Código Penal argentino sancionan las injerencias arbitrarias de terceros en el ejercicio del derecho de comunicación intersubjetivo y la confidencialidad de los datos como expresión social de ese ámbito de privacidad. Al titular del bien jurídico penalmente tutelado se le asegura un ámbito propicio para el ejercicio de su libertad de comunicación como parte esencial de su personalidad humana. A su vez, se le garantiza que ese derecho podrá ser ejercido de manera razonable y excluida de las intromisiones ajenas.

Las nuevas tecnologías aplicadas a los sistemas de comunicación (sistemas telemáticos) han obligado a la ley penal a armonizar esa tutela mediante la incorporación del correo electrónico como objeto de la acción de violación de secretos. Los medios de intrusión de la privacidad en los sistemas informáticos también han sufrido un cambio fundamental que maximiza las posibilidades de injerencias ajenas sin posibilidad de detección temprana.

[34] SCHOCH, "Konvergenz der Medien. Sollte das Recht der Medien harmonisiert werden?", JZ 2002, pp. 798 y ss.

La privacidad como interés jurídicamente tutelado no se restringe al ámbito personal o familiar, sino que también incluye otros ámbitos sociales, en especial, el de las relaciones laborales. En el marco de la moderna sociedad de la información, hoy ya se ha acuñado el término "autodeterminación informativa" para designar el derecho de toda persona de controlar el sentido y alcance de los datos sensibles que circulan por las redes telemáticas. No existe causal alguna de justificación que pueda legitimar en el estado actual de cosas la vigilancia informática de los dependientes, menos aún bajo el ropaje de un presunto derecho de control de la actividad empresarial. Si bien la privacidad es un bien jurídico disponible por parte de su titular, debe existir un marco regulatorio adecuado para evitar

caer en excesos, en particular, cuando las relaciones laborales están signadas por una marcada desigualdad entre el empleador y el empleado. Cualquier medida de injerencia en el ámbito personal del afectado debe estar autorizada judicialmente, al mismo tiempo que esa medida debe guardar relación de necesidad, idoneidad y proporcionalidad con lo injusto cometido o sospechado. Cualquier infracción al derecho a la privacidad personal debe ser resarcida económicamente de manera adecuada, mientras que al Estado le corresponde el deber de adoptar las medidas necesarias para evitar que la intimidad de las personas en un Estado social y democrático de Derecho sea objeto del escrutinio público.

III.- EVIDENCIA DIGITAL Y TUTELA JUDICIAL EFECTIVA:

De manera general, la Inteligencia Artificial (IA), se puede definir como el "término usado para referirse a cualquier *software* capaz de ejecutar una tarea normalmente asociada a un humano, al requerir de cierta inteligencia"[35]. De forma más técnica, es "la combinación de algoritmos planeados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano"[36]

El uso de este tipo de inteligencia encuentra su fundamento en dos acontecimientos:

Por un lado, en la aceleración de las tecnologías de la información, impulsada, en los últimos años, por la irrupción de capacidades de almacenamiento de datos masivos, auspiciada por la computación en la nube y el paradigma de los grandes datos *(big data)*, así como por la aparición de una nueva profesión, la del científico de datos *(data scientist)*.

Por otro lado, en la confluencia tecnológica que ha resultado extraordinaria gracias al avance en las redes de telecomunicaciones, la velocidad y el ancho de banda, que han permitido trabajar remotamente a través de flujos electrónicos multimedia, video y audio.

A ello hay que unir que nuestras ciudades son cada vez más inteligentes (paradigma de smart cities), las cámaras de seguridad, las estaciones meteorológicas, los indicadores de

[35] MORELL RAMOS, J., "La Inteligencia Artificial en el día a día de un abogado: qué le va a enseñar y cómo lo cambiará", Revista del Consejo General de la Abogacía Española, 108, febrero 2018, p. 7.
[36] IBERDROLA, "¿Qué es la Inteligencia Artificial", Iberdrola, Te interesa, Tecnología, p. 2, disponible en https://www.iberdrola.com/te-interesa/tecnologia/que-es-inteligencia-artificial.

polución, los semáforos, las farolas... se han llenado de sensores permanentemente conectados, lo que se ha acentuado por la producción ingente de información consecuencia de la omnipresencia de dispositivos móviles personales [37]

En este escenario, donde los datos están por todos lados, inundándonos, se hace cada vez más difícil para el ser humano tomar de decisiones, pues los patrones que pueden diseñar para facilitarle tal tarea se van complicando, resultando su gestión un trabajo adicional. Para solucionar estos inconvenientes, los investigadores de las disciplinas informáticas se han volcado en desarrollar una parte de la IA, especialmente lo que se conoce como aprendizaje automático (Machine Learning), que constituye un campo de investigación en el que destaca el diseño de algoritmos basados en redes neuronales [38]. Ello ha ido seguido de una optimización denominada aprendizaje profundo (Deep Learning), que abre la puerta a confiar en sistemas que emulan capacidades humanas significativas, como el reconocimiento de imágenes, voz y movimiento.

Las autoridades judiciales penales y los equipos policiales, que tradicionalmente han manejado volúmenes importantes de información relacionados con la criminalidad, están empezando a mirar con interés este tipo de tecnologías inteligentes que les plantean alternativas a la hora de mejorar la garantía de la seguridad pública y la eficacia en la obtención de resultados en las investigaciones penales. Evidentemente, los gobiernos impulsan estas labores, aunque no se haga de manera igualitaria en todos los países o áreas geográficas. A esta tendencia pertenecen los modelos que se presentan a continuación, que responden a un sistema de vigilancia policial predictiva (predictive policing), consistente en tomar datos de fuentes diversas, analizarlos y utilizar los resultados para prevenir, evitar y responder de manera más efectiva a futuros delitos

Las nuevas tecnologías de la información y la comunicación, en adelante TIC, se han impuesto, en los últimos años, en el ámbito de la seguridad nacional, la vigilancia de fronteras y la investigación de delitos y persecución del crimen organizado en todo el mundo. La proliferación de este tipo de medidas de investigación tecnológica asegura una mayor efectividad de las actuaciones llevadas a cabo por los gobiernos nacionales y los cuerpos de seguridad de los Estados; sin embargo, también son altamente intrusivas en la esfera de los derechos fundamentales de los ciudadanos.

Los gobiernos y las organizaciones supranacionales están intentando ponerse al día en la regulación de estas medidas de vigilancia, pero su proliferación y la velocidad a la que se desarrollan y se propagan ha derivado en una importante insuficiencia normativa. La falta

[37] CANO CARRILLO, J., "Arquitecturas distribuidas de gobierno electrónico con ciberseguridad crítica", tesis doctoral, Ed. UNED, Madrid, 2015, p. 45, disponible en http://e-spacio.uned.es/fez/eserv/tesisuned:IngInd-Jscano/CANO_CARRILLO_Jesus_Salvador_Tesis.pdf.

[38] En este contexto, un algoritmo se define como una fórmula matemática tecnológicamente automatizada, una secuencia de instrucciones que se lleva a cabo para transformar la entrada en la salida. Algunos de estos algoritmos incorporan sistemas de aprendizaje automático (ML algorithms), siendo los programas de Machine Learning un modelo general con parámetros modificables. Al asignar diferentes valores a estos parámetros, el programa puede hacer diferentes cosas. Cfr. BABUTA, A. - OSWALD, M. - RINIK, C., "Machine Learning Algorithms and Police Decision-making. Legal, Ethical and Regulatory Challenges", Withehall Report 3-18, RUSI and University of Winchester, 2018, p. 2.

de leyes de cobertura deja la puerta abierta a la comisión de atropellos contra los derechos fundamentales de millones de personas en todo el mundo. En Europa, se adoptaron medidas legislativas de protección para los derechos fundamentales basados en la necesidad y proporcionalidad de la intromisión de los Estados en la esfera de intimidad y privacidad de las personas. Un claro ejemplo de ello es la directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12/07/2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (directiva sobre la privacidad y las comunicaciones electrónicas) [39]

La proliferación del crimen organizado y del terrorismo han legitimado a los Estados a la hora de tomar medidas tecnológicas de control y vigilancia muy intrusivas en la intimidad y la privacidad de los ciudadanos. La incapacidad de los Estados nacionales para dar respuesta a los conflictos sociales contemporáneos ocasionados por problemas económicos (lavado de activos, terrorismo y narcotráfico), medioambientales o tecnológicos (cibercrimen y pornografía infantil) escapan al control y a la regulación local [40]. Frente a esta necesidad, la toma de decisiones fundamentales que, antes se concentraban hacia el interior de los Estados se desplazó al ámbito de las relaciones internacionales dando lugar a la celebración de la "Convención de Budapest" sobre cibercrimen, reconociendo estas nuevas formas de criminalidad y la necesidad de adoptar medidas legislativas, ejecutivas y judiciales para luchar contra ellas.

Sin lugar a dudas, estas novedosas formas de criminalidad requieren de nuevas técnicas de investigación. En efecto, la prueba digital puede encontrarse en una computadora ubicada en el interior de un domicilio, donde se realice un allanamiento, o la cuestión puede practicarse mediante otras formas novedosas de investigación. La información puede no estar en la computadora del acusado sino alojada en servidores externos de las empresas que ofrecen los servicios utilizados por aquel. Pensemos en los correos electrónicos, los archivos guardados en la "nube" o las claves de acceso a cuentas. En estos casos, las fuerzas de seguridad pueden solicitar directamente a la empresa la entrega de dicha información, procedimiento del cual el acusado puede no estar ni enterado.

Argentina carece de políticas públicas claras en materia de ciberseguridad y delitos informáticos. Las decisiones que se han tomado sobre este aspecto, de importancia capital para la denominada era digital, no responden a una necesidad social detectada y evaluada como tal; ni siquiera a una planificación estatal.

[39] Diario Oficial L 201 de 31/07/2002, ps. 0037-0047.

[40] Ver FERRAJOLI, Luigi, "Crisis de la Democracia en la Era de la Globalización", en Anales de la Cátedra Francisco Suárez: Derecho y Justicia en una sociedad global, Granada, 2005, p. 39, quien considera la existencia de una "crisis de la legalidad tanto ordinaria como constitucional" y la define como "la crisis del valor vinculante asociado a las reglas por los titulares de los poderes públicos". Ver también FERRAJOLI, Luigi, "Derechos y garantías. La ley del más débil", Trotta, Madrid, 2009, p. 15.

En términos conceptuales es necesario remitirnos a lo que el profesor Binder denomina: Políticas de Gestión de Conflicto. Por ende, tomaré a la política criminal y las políticas de ciberseguridad como especies de política pública. [41]

III.I POLÍTICAS PÚBLICAS DIGITALES:

En todos los ámbitos de gobierno se avanza en la informatización y digitalización de documentos y procesos, a través de políticas públicas que buscan transparentar gestiones y brindar un mejor servicio a los ciudadanos. Existen también iniciativas que favorecen y tienden a conectar digitalmente los ámbitos de nuestras vidas. A nivel de infraestructura tenemos grandes adelantos con el plan federal de Internet y los satélites propios Arsat[42] ; legislativamente contamos con la Ley 27.078[43] (ley de Argentina digital) que favorece el desarrollo de las Tecnologías de la información y la comunicación (en adelante TIC); dentro de las administraciones públicas se van creando plataformas de servicios para gestiones en línea, tal el caso del proyecto Ciudadano Digital en Córdoba CIDI, que permite, tras la validación de la identidad con datos biométricos, la realización de gran cantidad de trámites, o la reciente aprobación de la ley 10590 que incorpora en córdoba la historia clínica digital. Aunque celebremos estas iniciativas vale plantearse un interrogante esencial: al momento de la elaboración ¿consideraron que se debe dar una respuesta favorable al ciudadano en caso de que la tecnología falle o sea vulnerada? Es decir ¿pueden garantizar una respuesta acorde ante un perjuicio o delito cometido con o a través de las tecnologías? Es indispensable evaluar si este tipo de iniciativas están elaboradas bajo un marco planificado de políticas públicas y si se construye pensando en ―seguridad‖ y en armonía con otras áreas referentes a la seguridad de la información. Resulta fundamental dar respuesta a esta pregunta, pues están en juego diversos derechos humanos.

[41] Definición de Políticas Públicas de Knoepfel, Peter en "Análisis y Conducción de las Políticas Públicas" : Allí la refiere como ―una concatenación de decisiones o de acciones, intencionalmente coherentes, tomadas por diferentes actores, públicos y ocasionalmente privados, cuyos recursos, nexos institucionales e intereses varían - a fin de resolver de manera puntual un problema políticamente definido como colectivo. Este conjunto de decisiones y acciones da lugar a actos formales, con un grado de obligatoriedad variable, tendientes a modificar el comportamiento de grupos sociales que, se supone, originan el problema colectivo a resolver (grupos-objetivo) en el interés de grupos sociales que padecen los efectos negativos del problema en cuestión (beneficiarios finales). Tomo esta definición ya que considero que aquellas que no tienen en cuenta a otros sectores más que el Estado, en el proceso de tomas de decisiones, no pueden ser útiles en esta sociedad donde son las mismas personas que demandan cada vez más ser escuchadas y que se gestionen formas eficientes de participación.

[42] http://www.arsat.com.ar

[43] http://servicios.infoleg.gob.ar/infolegInternet/anexos/235000-239999/239771/texact.htm

Otra pregunta que debemos hacernos es qué (más) debería pasar para que se debata democráticamente una necesidad pública de este estilo. A partir de tal debate podríamos definir aspectos cruciales, tales como el nivel de privacidad que los ciudadanos necesitamos frente la seguridad que se demanda, o cuáles son las garantías de protección por parte del Estado ante la implementación de sistemas informáticos, cuáles son nuestras infraestructuras críticas, o porque se aceptan las reglas económicas que permiten tener en el mercado tecnología barata al alcance de muchos, pero sin ningún estándar mínimo de seguridad. Es justamente la falta de costumbre de los debate con la participación de los múltiples sectores en este tipo de políticas digitales, que hace que cuando se traslade una situación al ámbito del derecho penal, punitivo y represivo, las medidas terminan siendo ineficientes o mucho peor, desproporcionadas en relación al derecho que se quiere resguardar incluso, con la posibilidad de afectar otros.

Argentina llegó a la sanción de la ley 26.388, llamada ley de Delitos Informáticos en el año 2008 sin un una política criminal clara, más guiada por acontecimientos mediáticos que por una planificación federal.

En Argentina la política criminal, entendida esta como al segmento de la Política de Gestión de Conflictividad que organiza el uso de los instrumentos violentos del estado para intervenir en la conflictividad sobre la base de los objetivos generales y metas, que está fija. (Binder Pág. 186) y las TIC llevan una relación muy reciente y poco madura, basada en la capacidad que tiene el Estado en utilizar las nuevas tecnologías como parte de la violencia para prevenir o investigar ciertos hechos delictivos.

La utilización de TIC en la investigación de hechos delictivos supone una nueva forma de ejercicio de violencia que tiene el Estado (que denominaré “Violencia Digital Estatal) para conseguir finalidades sociales definidas en las políticas públicas. Los delitos informáticos fueron el resultado del uso de esas nuevas tecnologías, en un primer momento en el accionar criminal por las ventajas que otorgaba, provocándose vacíos que se dieron sin un marco adecuado de discusión y acompañamiento en materia de gestión pública. Precisamente por el potencial que tienen las TIC en afectar múltiples derechos en caso de ser utilizadas como parte del uso de la violencia, es el binomio ―política criminal y nuevas tecnologías‖ el que debe ser puesto bajo la lupa.

Tomando el desafío que menciona Alberto Binder de ―encontrar una forma de control de la criminalidad que nos aleje del uso de instrumentos autoritarios y que nos permita construir herramientas eficaces‖, se vuelve esencial abordar el uso de las tecnologías de la información y comunicación utilizadas en los hechos o en la investigación criminales y específicamente de los hechos que hacen referencia a lo que llamamos delitos informáticos.

Junto a este desafío viene el de la tendencia a la creciente legislación penal para afrontar problemas digitales, es decir que se pretende una expansión de la legislación penal, sin

antes evaluar otros sectores del derecho y sin medir las consecuencias de llegar a soluciones que constituyan un derecho penal simbólico ante los riesgos que generan las nuevas tecnologías de caer en el punitivismo o en un derecho penal del enemigo . Se vuelve esencial tratar estos temas porque a lo largo de estos años no sólo hemos asistido a los desafíos que se plantean en las investigaciones criminales; también hemos comprobado que derechos esenciales pueden ser vulnerados con facilidad, a través de los medios digitales, como las novedosas técnicas de investigación penal utilizando software espía, allanamientos a distancia, dispositivos de geolocalización, etc. En definitiva, hablamos de herramientas que tienen un potencial nunca antes visto, y el mismo no está siendo analizado dentro de una discusión de legitimidad de política criminal

La ley 26388 llamada de ―Delitos Informáticos‖ vino a incorporar dos cosas importantes para poder dar respuesta a todos los desafíos que se presentaban hasta ese momento. Uno de los aciertos fue la incorporación del artículo 2, que agrega dos párrafos al artículo 77 del código penal y amplía la comprensión sobre los conceptos de firma, documento, certificado, suscripción al ámbito digital. El segundo acierto es que el resto del articulado incorpora un plexo normativo a nuestro código penal con modalidades delictivas cometidas a través de medios digitales (128, 153, 155, 157 176 inciso 16, 183, 184 y 255) y delito propios digitales (153 bis y 197). Todo esto además permitió poder ir cumpliendo con estándares que se solicitaban a niveles internacionales para la firma de convenios globales de cooperación como el de cibercriminalidad de Budapest

La ley fue un parche. Así lo mencionaba uno de sus autores: No estamos sancionando una ley de delitos informáticos que crea nuevas figuras penales. Simplemente estamos adaptando los tipos penales a las nuevas modalidades delictivas que encuentran a la informática como medio de la acción típica. Estamos previendo algunos delitos vinculados con el engaño o el fraude, o que afectan la integridad sexual, como por ejemplo la pornografía por Internet, que antes no existía"

En Argentina las formas de intervención del Estado en materia de cibercrimen y delitos informáticos no son uniformes, aunque todas resultan válidas a la hora de dar respuestas a problemáticas concretas de la ciudadanía. Podemos identificar pedagógicamente entre tres modelos de intervención a la hora de abordar el fenómeno de la llamada delincuencia informática o digital: un modelo concentrado, uno desconcentrado y uno mixto. No es el propósito analizar en detalle su funcionamiento, sino ver su posición dentro del organigrama (decisión estratégica) y mencionar las posibilidades de actuación con las dependencias técnicas de las cuales dependerá la recolección u obtención de la evidencia digital

1. <u>Modelo concentrado Fiscalías Especializadas de la Ciudad Autónoma de Buenos Aires:</u>

El modelo es concentrado ya que se tomó una decisión de política criminal para que haya dependencias encargadas de la investigación de hechos delictivos con competencia exclusiva para esta clase de delitos. Es decir que se concentran las investigaciones, apostando por la especificidad de la materia y la especialización de unidades fiscales.

2. Modelo desconcentrado Ministerio Público Fiscal de Córdoba

A diferencia de la CABA, el Ministerio Público Fiscal de Córdoba no posee fiscalías de Cibercrimen, ya que cuenta con fiscalías especializadas en temáticas más amplias, como ―delitos contra la integridad sexual‖ y ―delitos complejos‖, dentro de las cueales existen competencias específicas para la parte digital. Por ejemplo la Fiscalía de Delitos Complejos 51 tiene por instrucción particular de Fiscalía General52 competencia exclusiva en toda la provincia en materia de Phishing. La fiscalía especializada en delitos contra la integridad sexual 53 aborda toda la temática en materia de pornografía infantil y grooming 54 . Además, en virtud de una decisión de política criminal focalizada, en 2014 se creó el ― Área de coordinación y seguimiento de cibercrimen 55 , orgánicamente bajo la órbita de la Fiscalía General de la Provincia a cargo de la Fiscal Adjunta Dra. María Alejandra Hillman.

3. Modelo Mixto Ministerio Público Fiscal de la Nación

En 2015 el Ministerio Público Fiscal de la Nación creó la ― Unidad Fiscal Especializada en Ciberdelincuencia ‖ 58 . Interviene en casos de ataques a sistemas informáticos y en delitos cuyo medio comisivo principal o accesorio incluya la utilización de sistemas informáticos, con especial atención en el ámbito de la criminalidad organizada, y crímenes en los que sea necesario realizar investigaciones en entornos digitales. Dentro de sus competencias está la de recibir denuncias y realizar investigaciones preliminares y genéricas. Es decir que no sólo da apoyo a las fiscalías o unidades fiscales (como el caso de Córdoba), sino que tiene facultades para recibir denuncias y realizar medidas de investigación (fiscalía especializada de la CABA).

IIII.II Nuestro país sigue una política criminal difusa en materia de Cibercriminalidad

Actualmente en materia de delitos informáticos existen muchas iniciativas de reformas de leyes de fondo (para incorporar otros tipos penales), forma (buscando acompañar los desafíos de los medios de prueba), artículos de criminología y criminalística (con investigaciones de los perfiles criminales y elaborando novedosas técnicas forenses digitales), pero no hay iniciativas que logren crear los marcos necesarios que debería guiar todas estas actividades, es decir el marco adecuado para políticas públicas o política criminal en material de delitos informáticos. Esto conduce a una primera conclusión: en nuestro país la política criminal que se lleva adelante en materia de cibercrimen y ciberseguridad está siendo construida por distintas disciplinas (la dogmática penal, la

criminología y el derecho procesal penal) o saberes prácticos, lo cual conlleva ventajas y desventajas[44]. En el caso de la ciberseguridad es aún mayor la ausencia de este tipo de políticas, ya que recién en los últimos años se vienen tomando decisiones que podrían orientarse. Siguiendo la línea en la cual no se visualiza una política criminal determinada y que se traduce en una falta de objetivos claros (quizás porque nunca se indagó en los mismos), encontramos el panorama indicado para resaltar el peligro que puede conllevar la ―libertad con la que las instituciones están haciendo uso, o utilizarán en un futuro, nuevas tecnologías como resultado de la facultad del uso de la violencia digital estatal. Esta libertad puede ser peligrosa, ya que tiene el potencial de afectar derechos si no poseen el marco de legalidad que merecen. Es por ello que no pudiendo ver cuáles son claramente los objetivos en la construcción y uso de la violencia digital estatal, es primordial la construcción de los mismos y empezar a hablar de sistemas de monitoreo y/o evaluación que las que toda política pública debería tener

IIII.III Ideas para un debate sustentable

La elaboración y desarrollo de políticas públicas en materia de ciberseguridad y delitos informáticos debe tener en cuenta sus condiciones de consenso, corrección y factibilidad, para su formación, implementación, impacto y evaluación. Esta elaboración debe considerar la variedad de instituciones que históricamente han interactuado (Policía, Servicio Penitenciario, Justicia), pero también aquellas del novedoso mundo virtual. Allí se producen interacciones con empresas privadas, con organismos de respuesta de incidentes o laboratorios de naturaleza mixta. Por ende, la nueva política criminal debería adaptar los modelos para incluir como socios a los nuevos actores, incluso aquellos que no tienen domicilio legal en el país, ya que son un eslabón cada vez más utilizado. Esta construcción de políticas debe hacerse en base a intereses compartidos que permitan dirigir las acciones de los actores para un mismo lugar. Todas estas instituciones, organismos, dependencias u oficinas (de naturaleza pública, privada o mixta) deberían orientar sus saberes prácticos a la política criminal definida en el marco de un entendimiento común, lo que implica que es fundamental que exista diálogo entre ellas. Esta política como forma de intervención del estado en los asuntos de los ciudadanos debe ser pensada como intervención de excepción (por ser realizada con violencia), por lo que cada área u oficina que quiera realizar sus aportes debe hacerlo en este marco excepcional, por ejemplo a la hora de incorporar un nuevo medio de investigación digital no puede este ser pensado como un instrumento a utilizar sin medir sus consecuencias, sino que debe ser pensado solo en el caso de que no exista otra alternativa que brinde mayores garantías a las partes en los casos particulares. Vale la pena remarcar que la elaboración de política criminal en un sistema federal no es

[44] Algunos autores mencionan que la dogmatica penal, la criminología y el derecho procesal penal, no son las disciplinas adecuadas para ocuparse de la PC, y cuando lo hacen la han empobrecido. Op. cit. Binder,Pag. 141

sencilla, pues las provincias tienen autonomía en diversas cuestiones y fijan de acuerdo a sus realidades las prioridades. Es por ello que la construcción de estas políticas debería darse a través de grupos interdisciplinarios que aseguren la máxima representación de las provincias. Los grupos que se formen y representen intereses nacionales deben estar integrados por profesionales especializados de todo el país, o asegurar su participación remota o su derecho a ser oído con mecanismos a tales fines. Sólo con todas las voces podemos asegurar debates democráticos y resultados legítimos En los debates sobre ciberseguridad o delitos informáticos no se suele encontrar la participación, siquiera las visiones, de aquellos que se dedican a la construcción de políticas públicas. Esta es una deficiencia que debemos asumir.

III.IV A modo de epílogo:

Resulta urgente un debate sobre la construcción de una política criminal basada en el uso de tecnologías de la información y comunicación (pensada en la forma de violencia digital estatal). Que sea una política que guíe el uso de la violencia (no lo prohíba) que el propio Estado utiliza a través de las nuevas tecnologías en contra de los ciudadanos con mecanismos que aseguren el respeto de todos los derechos. Necesitamos saber cuál es el objetivo de esas políticas para que todos los actores puedan guiar sus acciones hacia ella. También es indispensable evaluar los costos sociales que implica cada decisión ante la implementación de una política, más aun si el costo significa una intromisión en los derechos de los ciudadanos. Y es justamente cuando no hay debate, cuando no vemos o escuchamos todas las voces y todas las necesidades es que aumentan los riesgos de violar derechos fundamentales. Este tipo de políticas debe garantizar (con ayuda de las nuevas tecnologías) que cada ciudadano interesado pueda ser oído para que la decisión final no quede en manos de grupos de profesionales favorecidos históricamente por la cercanía a los centros de toma de decisiones. En esta materia en particular, pensar una política nacional, e incluso local exige romper con el paradigma de toma de decisiones vigente e implementar mecanismos de participación federales. Todas estas discusiones en torno a las herramientas digitales, usadas por los estados y las empresas privadas, se centran en gran medida en la búsqueda y obtención legitima de datos (datos que pertenecen muchas veces a las esferas privadas de las personas, ámbito protegido constitucionalmente). Esto vuelve esencial el respeto, cuidado y protección de los datos personales, más aún en un mundo donde reina la inteligencia artificial, minería de datos, big data y el blockchain; un mundo que cambiará el paradigma de los datos personales y traerá una nueva visión de ellos. Quiero expresar que apuesto fervientemente al uso de nuevas tecnologías en el ámbito de los Ministerios Públicos y de los Poderes Judiciales del país, no sólo por su capacidad de hacer más agiles los procesos formales internos, sino por su potencial para realizar aportes significativos en el desarrollo de las investigaciones. Estos aportes se verían reflejados en un diferente

control de la criminalidad, una reducción de la violencia y, en el mejor de los casos, la transformación o extinción de determinados fenómenos criminales.

IV.- EVIDENCIA DIGITAL, SU REGULACIÒN PROCESAL Y COMO HERRAMIENTA DE LITIGACIÒN:

Al igual que la prueba material, la evidencia digital se enfrenta a problemas de admisibilidad, autenticidad y legalidad. De ese modo, de manera preliminar puede ser rechazada si no logra establecer su utilidad – pertinencia-, su autenticidad, o legalidad. Ahora bien, si ingresa al juicio puede carecer de valor probatorio por su baja credibilidad o compromiso con el tema debatido.

En nuestro medio, los códigos procesales no prevén ni regulan en general este tipo de evidencia y en la práctica, no se cuestiona demasiado el origen y autenticidad de la evidencia electrónica, más bien, se suele discutir si fue correctamente extraída o si no ha sido objeto de alteración o manipulación en especial cuando se prestan video filmaciones de cámaras predispuestas, capturas de fotografías o conversaciones en pantallas.

Es dable señalar que, al analizarse una evidencia, sea cual fuere, los jueces ven el contexto en que se presenta, los hechos debatidos, las afirmaciones de las partes y el resto del material. No se toma esa evidencia de modo fragmentado, individual, tampoco es algo fijo, más bien dinámico, evoluciona paso a paso, se va armando un rompecabezas que empezó en la estructuración de la teoría del caso, en los planos fácticos que fue organizada.

En este sentido, por más que una parte presente un documento digital que pueda ser declarado auténtico, supongamos un video de una persona caminando en las profundidades del atlántico, deteniéndose a fumar un cigarrillo en el lecho oceánico, ningún juez en su sano juicio le otorgará valor a esa evidencia. Por ello, toda evidencia, por más confiable y contundente que sea, debe aparecer guiada por el letrado en un contexto de razonabilidad y encontrar asiento en el relato, con sentido común y lógica. Las pruebas digitales por más modernas que sean tampoco hablan por sí solas, deben ir enmarcadas dentro de un discurso persuasivo sobre hechos relevantes. La práctica nos muestra cómo se desperdicia un material valioso por ausencia de estrategia en el armado de caso y el pésimo modo de presentan video o un audio, por n hacer una pregunta a tiempo, oportuna, precisa.

Cuando se pretende introducir una evidencia en juicio es importante saber, en primer lugar, si es posible hacerlo, y, en su caso, cómo. Esto nos lleva a verifica cuales son los parámetros con los que contamos en la ley que regula el procedimiento penal.

Por su parte y solo a título de marco referencial, debo señalar que la Convención de Budapest establece los siguientes medios de prueba: 1) aseguramientos de datos: como medida cautelar que permite a las autoridades ordenar a los titulares o administradores de

sistemas informáticos que tengan alojados datos que puedan ser de utilidad para la investigación y que los preserven por un plazo determinado, en particular, dice, cuando sean susceptible de pérdida o modificación, fijando un máximo de noventa días, renovables, para la conservación de esos datos hasta que las partes puedan obtener la revelación de los mismos (art. 16) b) orden de presentación de datos: prevé la facultad de las autoridades de ordenar a los proveedores de servicios de internet o titulares de cualquier sistema de alojamiento de información en formato digital que entregue o informe datos que tengan en su poder. Puede solicitar: tipo de servicio utilizado, disposiciones técnicas del servicio, período, identidad, dirección postal, situación geográfica, número de teléfono, facturación, paso y cualquier otro dato del servicio o prestación, ubicación donde se encuentran los equipos de comunicación según el contrato de prestación o servicio (art. 18) C) Registro y secuestro de datos informáticos; prevé la posibilidad de registrar o tener acceso a todo el sistema informático o datos informáticos en èl almacenados, dispositivos de almacenamiento informáticos. Podrán adoptar medidas a propósito de confiscar u obtener un sistema informático, una parte o un medio de almacenamiento, realizar y conservar una copia de esos datos, preservar la integridad de los datos, hacer inaccesibles o suprimir los datos del sistema informática.

En nuestro país, salvo escasas excepciones, los códigos procesales locales[45] no contienen una regulación específica del tema, incluso cuando la tienen, como el caso de nuestra provincia, no resultan del todo precisas. En general cuando se tratan el secuestro o registro lo hacen sobre "cosas", "efectos", "rastros" pero no sobre "datos", con algunas excepciones. Es que las leyes aparecen constantemente superadas por las nuevas tecnologías en su evolución y aplicación incluso, antes de ser sancionadas.

Ante esta situación, la primera pregunta obligatoria es: ¿Qué sucede con los medios no previstos expresamente en el CPP? Alcanza la regulación genérica de los códigos procesales que fijan el principio de "libertad probatoria", permitiendo el acceso de "otros" medios, "siempre que o conculquen garantías constitucionales de personas o afecten el sistema institucional" fijando como pautas de admisión, la misma de aquellos medios que resultan "más acordes a los previstos en este Código.

Desde la regulación procesal encontramos:

a) Los códigos prevén el principio de libertad probatoria. Bajo el criterio tradicional de la libertad probatoria se entendió que todo se puede probar por cualquier medio, sin

[45] A modo de ejemplo podrían citarse los arts. 251.252, Y 253 del CPP JUJUY, 181 del CPP CHUBUT, 234,235, Y 236 del CPPBA, 203, 207, 208 del CPP-LA PAMPA, 171 del CPP-SANTA FE, 150, 151, 153 CPP- NEUQUEN. Incluso en el orden federal, véanse arts. 224 y 230 bis del CPPN. La regulación es similar, se prevé a interceptación de correspndencia en algunos casos. En general, en el marco de la regulación "secuestros". Li limitación sobre medio de purbea pasa por verificar su licitud y pertinencia en tanto que la estricta legalidad no se aplica, sino, màs bien, la analogía procesa para aquellos no previstos acudiendo al principio de "libertad probatoria"

embargo, entiendo que ese "todo" debe incluir hechos penalmente relevantes controvertidos y por "cualquier medio" refiere a la pertinencia o relevancia del medio empleado. Con ello habría que repensar esa idea o forma de trabajar que permite o busca que "todo" ingrese y después se ve para qué sirve, si es que sirve para algo.

b) Excluyen la prueba que sea obtenida contrariando la ley. Esta es una constante que tiene que ver con incumplimiento, de requisitos que hacen al modo de obtención de la evidencia, el incumplimiento de reglas o afectación de un principio constitucional protegido a través de una garantía.

c) Vedan técnicas que signifiquen una intromisión sobre la intimidad del domicilio, la correspondencia, las comunicaciones, los papeles y los archivos privados sin orden judicial, en sintonía con el punto precedente.

d) Regulan concretamente la interpretación de correspondencia para la comprobación del delito. Algunos códigos incluyen la interpretación y el secuestro de correspondencia telegráfica y electrónica. Esta previsión ha permitido en la práctica aplicar analógicamente esos recaudos a las comunicaciones electrónicas. Aún así , debe repararse que se trata de "interceptar" una comunicación en proceso, por tanto, una vez que ha llegado a su destinatario, la ha leído, archivado o borrado, o bien, antes de ser enviada, no sería propiamente dicha una "interceptación" sino que se estaría registrando un equipo en búsqueda de un "papel privado", un archivo , un dato o información en un ámbito constitucionalmente protegido, aspecto que se vincula a una requisa en términos de injerencia probatoria.

e) Fijan pautas para la intervención telefónica y demás comunicaciones agregando, en ciertos casos, las condiciones para intervenir y/o interceptar mensajes de correos electrónicos que pertenezcan al imputado y/o sus comunicaciones on line, sea internet o intranet. Aquí , aplicamos el mismo criterio señalado precedentemente, si es una comunicación verbal en proceso sea de telefonía, videoconferencia, skype, whatsapp, la orden judicial tendrá, en principio, como objetivo captarla y registrarla, en cambio, si se trata de una comunicación que ha sido archivada, que debe ser recuperada, copiada, enviada o resguardada, supongamos un video, una grabación, un archivo de voces de una comunicación, estaremos frente a un dato digital protegido y que puede ser obtenido a partir de una requisa del contenido del dispositivo que lo contiene.

f) Muy pocos prevé el registro de un sistema informático y la incautación, copiado o preservación de datos informáticos o electrónicos de interés para la investigación o secuestros de componentes del sistema.

IV.I ANÀLISIS DEL ARTICULO 153 CÒDIGO PROCESAL PENAL DE LA PROVINCIA DEL NEUQUÈN, INFORMACIÒN DIGITAL:

Cuando se hallaren dispositivos de almacenamiento de datos que por las circunstancias del caso hicieran presumir que contienen información útil a la investigación, se procederá a su secuestro, y de nos es posible, se obtendrá una copia. O podrá ordenarse la conservación de los datos contenidos en los mismos, por un lazo que no podrá superar los noventa (90) días. Quien deba cumplir esta orden deberá adoptar las medidas necesarias para mantenerla en secreto. También podrá disponerse el registro del dispositivo por medios técnicos y en forma remota.

A cualquier persona física o jurídica que preste un servicio a distancia por vía electrónica, podrá requerírsele la entrega de la información que esté bajo su poder o control referida a los usuarios o abonados, o los datos de los mismos. La información que no resulta útil a la investigación, no podrá ser utilizada y deberá ser devuelta, previo ser puesta a disposición de la defensa, que podrá pedir su preservación. Regirán las limitaciones aplicables a los documentos.

Vemos aquí como el CPP neuquino de alguna manera, intenta regular con cierto detalle la posibilidad de obtener evidencia digital en al medida que fiscalía entienda que es útil la información que se pueda obtener por este medio. Lo cierto es que el artículo establece como regla el secuestro de los equipos informático donde se encuentran los datos pertinentes y, excepcionalmente, ante la imposibilidad de hacerlo, sea por las características de los equipos o porque se desconoce dónde se encuentran o están en otros países, la realización de una copia la digital de estos datos.

Ahora bien, está claro que Neuquén en este sentido ha dado un paso más que la mayoría de los CPP del resto de las provincias, pero vemos como esta regulación no termina de concretar una idea lo suficientemente sólida y con la menor cantidad de fisuras posible, siendo que la idea de regulación es que se secuestren los equipos para que estos puedan ser peritados, lo que no dice expresamente el artículo es quien lo va a peritar, de qué forma y cómo se va a resguardar esa información. Así por ejemplo, es posible que el dueño del equipo informática haya borrado la información para ocultar pruebas en su contra, lo cual, resulta efectivo para burlar a operadores inexpertos, que quizás ni siquiera se den cuenta de que los datos buscados han estado alguna vez allí, sin embargo, los peritos informáticos ante un examen minucioso de los dispositivos de almacenamiento de datos, con un software adecuado, pueda darse cuenta de la realización de estas operaciones e incluso, en muchos casos, hasta es factible la recuperación.

Sin perjuicio de que lo referenciado en el párrafo precedente sería la manera más correcta de manipular la información digital, lo cierto es que el artículo del CPP neuquino si bien vanguardista no deja de hacer agua en algunas cuestiones realmente preocupantes. En

primer lugar no se menciona expresamente en el artículo que la información debe ser manipulada por personal experto en el tema, es decir cualquier miembro de la fiscalía podría acceder a la información y extraerla, manipularla, borrarla, o eliminarla sin inconvenientes, asimismo no se estableció cual será el protocolo al que quedará sujeto este procedimiento y el proceder del personal que requiere ese secuestro, siendo que queda claro que no pueden aplicarse aquí las mismas reglas que para la evidencia material o física.

Entiendo que le intento por regular la obtención de la información digital, si bien es un inicio, ciertamente quedó en solo eso, en la práctica son realmente escasos los planteos que se hacen con relación a la forma de obtención de este tipo de evidencia, y la violación a la intimidad de la persona que está siendo sometida a un proceso, la falta de directrices y reglas en cómo y quién va a manipular este tipo de información sensible, deja abierta la puerta a que el ultraje y afectación de prerrogativas constitucionales sea la consecuencia directa y se provoque por parte del estado en su afán de obtener evidencia sólida un afectación, en ciertos casos, aún mayor de la que se intenta sancionar.

Asimismo, la norma también prevé además de la posibilidad de secuestrar los equipos informáticos o copiar los datos informáticos, la posible conservación de los datos contenidos en estos equipos, de nuevo sin identificar de qué forma, que software debe utilizarse, quien debe resguardar esa información, de qué manera, quien tendrá acceso y demás cuestiones que hacen a una debida cadena de custodia de esa información. Entiendo que este punto es de significativa importancia, siendo que generalmente quienes conservan los datos es personal policial sin ningún tipo de especialidad en la materia o si la tienen es realmente escasa, de nuevo la falta de reglamentación en la materia tiende a ser para los investigadores un arma de doble filo.

De esta manera, la medida se dispone como un depósito judicial, por el cual, el depositario carga con todas las responsabilidades que emergen de esta figura, tal y como si se le hubiera confiado la custodia de alguna cosa, además de cargar con la obligación de mantener la confidencialidad de estos. Una vez más, el omitir identificar protocolos, personal especializado, y/o mecánica de resguardo de la información digital, pone en una delicada posición a quien asuma la custodia y resguardo de esa evidencia digital quien se encontrara asimismo sin ningún protocolo de actuación que indique cómo y de qué forma tiene que desplegar tal tarea.

Luego la norma hace referencia a que el depósito de la información no debe ser indefinido, siendo que la norma ha establecido como máximo el plazo de noventa días, lo cual tiene su sentido, puesto que la preservación de la información implica la indisposición total o parcial del sistema de almacenamiento de datos informáticos que son ocupados por los datos custodiados. Si bien esto sería la menor de las falencias, si queremos hilar un poco más fino, como observación entiendo que el hecho de fijar un plazo de noventa días de forma genérica en ciertos casos resulta excesivo y sumamente perjudicial, como todo va a

depender del contenido de la información y de que trata la evidencia digital, recordemos que una PC (personal computer) puede almacenar en detalle la vida de una persona y el secuestro de tales datos que no revisten interés a lo que se investiga tiene que volver inmediatamente a la esfera de dominio de su dueño, sin la necesidad de tener que esperar 3 meses su devolución. Lo que se impone en este sentido es que el artículo debió hacer referencia a una entrega inmediata dependiendo de lo sensible del contenido de datos, en aquellos casos que lo secuestrado nada aporta a la investigación y sin embargo perjudica y violenta la intimidad de su dueño. Tendemos a pensar que personal capacitado con protocolos establecido y la puesta en funcionamiento de sistema especializado permiten un examen rápido, eficaz y con la menor intromisión posible en la intimidad de la persona que posibilite una disposición del material secuestrado mucho antes que noventa días.

Ante ese cuadro la primera pregunta que cabe hacerse es si respecto de los medios no previstos expresamente en el CPP, alcanza la regulación genérica que fija como principio general la "libertad probatoria" que establecen los ordenamientos procesales o bien, ese principio solo aplica para "medios" probatorios, los que deben distinguirse de las "injerencias" probatorias, las que necesariamente deben ser previstas por la ley.

Esta disyuntiva tiene dos consecuencia inmediatas: 1) si permitimos aplicar la analogía y consideramos que todos son medios de prueba de igual tenor, no existirían problemas en asimilarlos; 2) por otra parte, si distinguimos entre medios de pruebe e injerencias probatorias, la respuesta sería otra y resulta apropiado contar con una disposición legal específica para cada injerencia probatoria.

En lo que hace a la forma de ingreso al plenario, la evidencia digital es equiparada a prueba documental e ingresada a partir del mismo procedimiento, tal como sucede en los Estados Unidos de América, o bien, como se viene haciendo en nuestro país aunque sin examen exhaustivo sobro acreditación de evidencia, intangibilidad, método empleado para la obtención y resguardo o técnicas de análisis.

De misma forma, en cuanto a la autenticidad de la evidencia, el principal problema con que se encuentra la evidencia electrónica y digital es la falta de protocolos de actuación en el área judicial como la ausencia d uniformidad y consenso en la comunidad científica tanto sobre el proceso como sobre la validación, no solo de los resultados obtenido sino también de las herramientas y las técnicas utilizadas para obtenerlas. Esto lleva a sostener, sin perjuicio de aplicar los criterios locales sobre 2libertad probatoria" y "libre valoración de las pruebas", que no debemos perder de vista la trascendencia que tiene la acreditación de una evidencia antes de permitir su ingreso o valoración. Ese proceso implica y determina qué tipo de información permitimos que ingrese al juicio y el grado de calidad que tendrá. En este punto se pondrá en la mira: a) herramientas utilizadas, b) el procedimiento empleado c) la cadena de custodia; d) la legalidad en la obtención y presentación de la evidencia. X.

Constituye una excelente base o punto de partida para el tratamiento de la evidencia digital, el estudio efectuado por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), que sugiere y recomienda en su borrador el documento: "Estudio exhaustivo sobre el delito cibernético", como estándar de actuación en las técnicas forenses de investigación destinadas a la obtención, recolección, peritaje, y conservación de la prueba digital, "la creación de copias bit a bit" de la información almacenada y borrada, el "bloqueo de escritura" para garantizar que la información original no sea cambiada, y resúmenes criptográficos de archivo (hashes), o firmas digitales, que pueden mostrar cualquier cambio de información"[46]. Si bien a nivel nacional en los últimos años se ha dictado numerosos protocoles a nivel provincial y nacional, sobre técnicas de recolección, peritaje y conservación de evidencia digital, desgraciadamente hasta la fecha no existe en nuestro orden jurídico una regulación normativa específica sobre evidencia digital.

Ninguno de los códigos procesales a nivel nacional ha incorporado en el capítulo referente a medios de prueba, un apartado destinado a la regulación de la prueba digital. Incluso el reciente Código Procesal Penal Federal (ley 27.063, modif por ley 27.482) que fue elaborado sobre la base del Código Procesal Penal (ley 27.063) de corte acusatorio – adversarial, realizando la inclusión e incorporación de las reformas procesales penales implementadas durante el período 2015-2018 no dedica un apartado específico destinado a la regulación de la prueba digital.

Por este motivo, en la actualidad se realiza la adquisición, pericia y conservación de evidencia digital aplicando analógicamente las reglas jurídicas de los medios de prueba física, siguiendo como orientación rectora en cada jurisdicción los recientes protocolos dictados en materia forense digital.

Asimismo, es menester destacar que los distintos dispositivos de almacenamiento de información requieren técnicas de investigación forenses distintas. Así es que la obtención, peritaje y conservación de evidencia digital difiere en su técnicas de investigación forense a aplicar, ya sea que se trate de: 1. El análisis forense informático. 2. El análisis forense móvil. 3. Técnicas forenses de red.

Como desgraciadamente hasta la fecha no existe una regulación normativa de la prueba digital, realizada a través de una reforma procesal penal, veremos cómo sea realizada la adquisición, obtención, preservación, pericia y conservación de evidencia digital aplicando analógicamente las reglas jurídicas de los medios de prueba física tal y como fuera referenciado en los párrafos precedentes.

V. Intimidad versus libertad probatoria

[46] UNODC United Nations Office on Drugs and Crime. Oficina de Naciones Unidas contra la droga y el Delito "Estudio exhasutivo sobre el delito cibernético" (borrador de febrero de 2013) Naciones Unidas, Nueva York, 2013 p. 179.

"If there is any place where nature has no rule, it is in cyberspace. If there is any place that is constructed, cyberspace is it" [47].

"Otra de las trabas que soporta la averiguación libre de la verdad histórica, en virtud de limitaciones constitucionales expresas, deriva del derecho a la intimidad, reconocido desde la revolución liberal como otro de los bastiones de la dignidad humana. Ante él retrocede al menos relativamente, la investigación de la verdad como meta del procedimiento. Nuestra constitución, en el punto, reza: 'El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación' (art. 18)".[48]

Tal como explica el profesor Maier, existen varios tipos de *intimidades*, la del *domicilio*, la *personal* y la de las *comunicaciones*. Es esta última la que aquí nos interesa. "(...) ciertamente la ley, desde su origen, ha progresado escasamente, pues revela su atraso en relación con los medios de comunicación existentes modernamente y al modo de capturar los contenidos de esas comunicaciones" [49]. Agrega que considera acertado que la ley interprete analógicamente a las comunicaciones escritas y aquellas remitidas por vía electrónica, puesto que no es más que un avance en el medio de comunicación, el cual continúa con su esquema inicial (emisor-mensaje-receptor). Ahora bien, dicha analogía —que en verdad es más una adaptación—, **¿puede utilizare con la evidencia digital?.-**

El Tribunal Europeo de Derechos Humanos [50] ha sostenido que, sin importar lo público que pueda ser el ámbito donde me encuentre, siempre existe y así debe respetarse un ámbito de privacidad de todos los sujetos. En sentido similar lo ha sostenido el Dr. Nino[51], al explicar que existen tres tipos de ámbitos: el público, el privado y el íntimo.

Conforme el principio de *nulla coactio sine lege*, sin perjuicio de a quién le confíe el Código la investigación penal (juez de instrucción o Ministerio Público Fiscal), es correcto que pueda ser secuestrado, analizado y peritado todo registro en soporte digital o informático, así como elementos de prueba en los cuales pueda entenderse que existen rastros del delito. Puesto que los nuevos testigos ya dejan de ser seres humanos que perciben a través de sus sentidos, para ser televisores con wifi, máquinas Nintendo que almacenan chats, *routers*, celulares, servidores alojados en el extranjero, pendrives, etcétera.

Ahora bien, aunque "(...) en principio existe un número abierto en materia probatoria, no existe un número abierto en lo que se llaman medidas de coerción o de injerencia que determinan la incorporación de elementos probatorios. Esta cuestión es importante para poder diferenciar aquellas medidas de coerción que suponen la incorporación de pruebas,

---

[47] LESSIG, Lawrence (1999).

[48] MAIER, Julio B. J., "Derecho procesal penal", ob. cit., p. 639.

[49] Ibidem, p. 207.

[50] TEDH, "Peck vs. United Kingdom", disponible en: www.merlin.obs.coe.int/iris/2003/6/article2.en.html.

[51] NINO, Carlos S., "Fundamentos de derecho constitucional - Análisis filosófico, jurídico, y politológico de la práctica constitucional", Ed. Astrea, Buenos Aires, 2002, 2ª reimp.

de aquellas que solo tienden a la obtención de los fines del proceso y que, solo en forma mediata responden a una finalidad probatoria" [52]

Por su parte, vemos que, sin perjuicio de no emanarse conceptualmente el concepto de evidencia digital, el art. 216, CPPN, prescribe que "el juez de instrucción comprobará, mediante la inspección de personas, lugares y *cosas*, los rastros y otros efectos materiales que el hecho hubiere dejado (...)", por lo tanto, dentro del concepto de cosas y rastros —*(logs)*— podemos ubicar a la evidencia digital y, mediando orden judicial pertinente, estar habilitados a su secuestro e inspección.

En similar sentido se expresa el nuevo CPPF, al especificar en su art. 229 que el Ministerio Público Fiscal deberá dirigir la investigación preparatoria, procurando "(...) recoger con celeridad *los elementos de cargo o de descargo* que resulten útiles para averiguar la verdad".

El repaso que se realizò en los párrafos precedentes con relación a la regulación contenida en los códigos procesales respecto de la evidencia digital y el uso de la tecnología, nos pone claramente en un callejón o línea imaginaria donde en un extremo se encuentran las nuevas tcnologìas y en el otro los operadores que deber ver, a través de las herramientas que tienen, còmo trabajar ahciendo equilibrio entre el resguardo de principios constitucionales garantizados y la protección de los ciudadanos, evitando la impunidad especialmente en delitos trascendentes. [53]

Hemos analizado entonces que a partir de la protección constitucional brindada a la correspondencia, comunicacioes y papeles privados existe un numerus apertus que permite expandir la protección hacia las nuevas tecnologías que han inovado los móviles y equipos permitiendo extender la prohibición sobre injerencia de terceros a todas las nuevas formas de comunicaciones existentes y las que puedan darse en el futuro. Bajo esta óptica la protección constitucional sobre los “papeles privados” puede aplicarse a todos los datos e información contenida en soportes digitales al igual que la interceptación de correspondencia epistolar se aplica a los mails en proceso de envío o recepción. Con lo expuesto queda claro que no se precisaría una regulación expresa para extender una protección consagrada en la ley.

Cabe preguntarnos ahora que criterio se aplica en relación a las pruebas que deben obtenerse a partir de una medida probatoria intrusiva no prevista. Si adoptamos el criterio que aplica sobre ellas el concepto de numerus clausus, ls injerencias a los derechos constitucionalmente protegidos deberían encontrarse expresamente regulados en la ley , estándar que la propia Constitución nacional ha querido otorgar al indicar en el art. 18: que “el domicilio es inviolable”, y que “…una ley determinará en qué casos y con qué justificativo podrá cederse a su allanamiento y ocupación…”

[52] BRUZZONE, Gustavo, "La nulla coactio sine lege como pauta de trabajo en materia de medidas de coerción en el proceso penal", en La justicia penal hoy..., Ed. Di Plácido, Buenos Aires, 2000, p. 107.

[53] Tal como la CSJN lo ha advertido en casos como “JOSE MINETTI Y CIA. LTDA. S.A.C.E.I c. TUCUMAN, provincia de s/ Incidente de medida cautelar” CSJN, 6/3/18, al sostener que la sociedad “busca defenderse del flagelo temible y desgarrador del narcotráfico

No obstante lo dicho, es fácil advertir que, en la actualidad, se acepta y recepta la aplicación de las fórmulas de producción de prueba analógicas que prevén los códigos procesales al amparo del principio de "libertad probatoria", cuestión que resulta prácticamente indiscutida en nuestro país, asimilándose de esta forma prácticas probatorias a injerencia. Algunos autores en cuanto distinguen un medio de prueba de una injerencia propiamente dicha[54] señalando que el primer caso no resulta necesariamente, una limitación a o intervención en los derechos o garantías del sujeto investigado, y por tanto, no requiera de una regulación expresa que establezca requisitos de procedencia como, así también, un examen de proporcionalidad entre el fin perseguido y la medida en sí, aspecto que sí se encuentra presente en las medidas que disponen injerencias a bienes personalísimos donde se encuentra en juego la libertad, el honor o la intimidad personal, y por tanto, el constituyente desde siempre a querido otorgarle un rango de protección especial.

De esta forma, partiendo de la base de que los elementos de prueba se obtienen, ordinariamente, a partir de actividades que no implican una injerencia en la vida de las personas, cuando así se requiere, la ley es la que debería establecer las condiciones en que se llevará adelante la medida tal como se aprecia en la interceptación de las comunicaciones.

Sin lugar a dudas que el panorama ideal sería contar con una ley que reglamente y arroje luz sobro como debe desplegarse una injerencia probatoria que involucra evidencia digital, es decir está claro que regular aquellos medios probatorios que impliquen una injerencia en derechos constitucionales es imperiosa, pero debemos trabajar con lo que existe y adaptar con rigurosidad las resoluciones y los procedimientos a esas exigencias.

En este contexto, es necesario la aplicación analógica, siendo que si hay algo que quedó claro a lo largo de este humilde trabajo que: 1) la evidencia digital tiene relación con absolutamente todos los delitos que contiene nuestro Código Penal, 2) la gran mayoría de los juicios se incorpora prueba digital 3) la intimidad de las personas se vuelca casi en su totalidad en un dispositivo electrónico, más que nada un celular.

Por lo que dejar afuera de una teoría del caso tanto por lado de la fiscalía como por la defensa, por el hecho, no menos grave, de no contar con legislación que permita incorporarla, ciertamente hoy en día con la significancia del contenido de esa evidencia realmente importa para una investigación o una teoría defensita una substancial elemento probatorio.

Por ejemplo la forma más apropiada para asegurar la información obtenida de computadoras, teléfonos móviles, Tablet, entre otros equipos electrónicos es mediante el procedimiento de cadena de custodia y, especialmente, con la aplicación de protocolos de

[54] SALT. Nuevos desafíos de la evidencia digital: acceso trasfronterizo y técnicas de acceso remoto a datos informáticos. 2017 p. 45.

seguridad que puedan ser replicados objetivamente sin importar quién es el funcionario a cargo de la manipulación de los elementos[55].

Vemos como a modo de guía podemos trabajar con la RES. 234/16, Protocolo de Actuación de las Fuerzas Policiales y de Seguridad en la investigación y Proceso de Recolección de Pruebas de Ciberdelitos, dada su completitud en el tratamiento de las cuestiones relativas a la identificación, selección, secuestro y preservación de la evidencia digital o electrónica, que de alguna manera podemos tomar como un reglamento y directriz a la hora de tratar con evidencia digital. Sin embargo en los juicios vemos que la evidencia digital que se introduce en casi todos los casos proviene de videos, capturas fotográficas de móviles, capturas de pantallas de fotos o conversaciones, algunos correos y archivos fotográficos de computadores personales.

Tal y como lo hemos referenciado en nuestra concepción, prima la idea de "amplitud" entendiendo que "todo" ingrese y luego vemos qué sirve y qué se descarta para probar los hechos controvertidos. Ese paradigma camba con el avenimiento de juicio por jurados donde permitir el ingreso de "todo" puede generar problemas como: a) distracción del jurado, b) sobrepeso o sobrecarga de evidencia acumulativa o confusa: c) pérdida de tiempo y consecuentemente de capacidad para atender el desarrollo de la audiencia d) costos excesivos, entre otros. Ese cambio de paradigma en la admisión y valoración de pruebas merece mayor control a la hora de permitir el ingreso de la evidencia y mucho más cuando se trata de evidencia electrónica o digital donde la facilidad en adquirirla es inversamente proporcional a la dificultad para analizar y establecer su autenticidad.

La evidencia no debería escapar al control d: a) legalidad –y en este punto especialmente el respeto por los derechos fundamentales: proporcionalidad, necesidad, utilidad, estricta necesidad-b) fiabilidad –v.gr, confiabilidad intrínseca, autenticidad e inalterabilidad, c) efectividad- v. gr, capacidad probatoria.

En la pràctica, la introducción del material se hace por medio del funcionario que obtuvo, extrajo, reprodujo, exportó desde allí se somete al agente y a la evidencia a un cuestionario intentando demostrar:

a) Que el dispositivo del que se obtuvo funciona correctamente.
b) Que el almacenamiento en ese dispositivo funciona correctamente.
c) Que el contenido del documento que se exhibe, perita, analiza y coteja es el extraído, obtenido y copiado de ese dispositivo.

[55] La jurisprudencia, criticando la forma de actuación policial, ha dicho "un documento publicado en Reino Unido por la Associatio of Chief Polica Officers Ç(ACPO, 2004, 2012) establece cuatro principios básicos para el manejo de la evidencia digital. Destacamos dos de ellos a saber: 1) ninguna acción realizada por personal de las fuerzas de seguridad debería alterar los datos almacenados en computadores o medios de almacenamiento susceptibles de ser presentados a juicio 2) para aquellas circunstancias en que fuera necesario el acceso a un dato original, almacenado en una computadora o un medio de almacenamiento, la persona "debe ser competente" para llevar adelanta esa tarea y capaz de entregarla explicando la relevancia e implicaciones de sus acciones" (CNCCC, SALA VI 31/7/18, causa 37443/2018/2/CA2).-

d) Que es íntegro y suficiente, es decir, que su contenido es exacto, idéntico y preciso, que no ha sido objeto de alteración, adulteración ni manipulación con el propósito de falsear sus datos.
e) Que ha sido extraído, conservado y recuperado correctamente, según el método técnico más adecuado para el momento en que se manipuló.
f) Que no presenta deterioro y si lo presenta, cuánto afecta al documento y cuál fue su origen.
g) La forma en que el documento ha sido creado o almacenado en el sistema, soporte o archivo presentando persona que han intervenido en su creación, generación, archivo, envío o registro.
h) Los documentos que requieren firma electrónica u otro recaudo, tendrán que presentarse conforme lo establece la ley, caso contrario, se deberá recurrir a las prácticas de autenticación con la eventual pérdida de valor probatorio.

De este modo, si bien tiene como parámetros los principios que se aplican a la evidencia material – equivalencia funcional[56] -, se trata de adaptarlos en punto a una evidencia radicalmente distinta pero que no existe una regulación adecuada, y por ello, en un esfuerzo por controlar y permitir el control de la prueba, se busca establecer su autenticidad a partir de al menos tres vías: soporte, método empelado y autor.

Recordemos que se trabaja con evidencia que, al menos que sea pasada a papel, resulta intangible, por tanto de requiere siempre: a) conservación íntegra y sin alteraciones del documento hasta su presentación; b) aptitud o posibilidad de exhibición a terceros – caso contrario carece de valor, si son caracteres indescifrables no tiene sentido presentarlos – c) recuperación del mensaje o disponibilidad para eventuales consultas. Sea en el medio que se extrajo, en las copias auténticas, idénticas, espejadas.

VI.- EVIDENCIA DIGITAL – CIBERCRIMEN Y LA CRIMINOLOGIA:

Como último tema a abordar, no quise dejar fuera de este trabajo, la implicancia que el tratamiento de la evidencia digital tiene en el campo de la criminología, esto ya por el innegable hecho de que la evidencia digital atraviesa como vimos todos los campos y aspectos de nuestro ordenamiento jurídico, la criminología entendida por tal como un campo complejo y polivalente no deja de verse de alguna manera alcanzado por las nuevas formas de delincuencias que trae aparejada la evolución sin pausa de la tegnologia que ha colocado a la humanidad en una nueva era de la que sin lugar a dudas nada ni nadie queda exento.

[56] Se habla de equivalencia funcional al equipararse las pruebas documentales a la digital. Nuestro Código Penal, en su art. 77 equipara los documentos físicos a los digitales

El desarrollo de todo el conjunto de tecnologías informáticas que empezó en los sesenta y setenta y que tuvo su espaldarazo definitivo con la creación de Internet y su posterior universalización hasta su conversión en el medio de intercomunicación social más importante de la actualidad, no tiene visos de haber firmado sus últimos avances, sino que, más bien al contrario, parece que la rapidez con la que aparecen nuevas tecnologías se ha ido incrementando exponencialmente.

Desde luego, lo han hecho los efectos sociales que han acompañado a la revolución de las TIC: gracias a la aparición de Internet y a su popularización a escala planetaria nos hemos acercado enormemente a la creación del ciberespacio virtual tal y como lo concibiera el que acuñó tal término, William Gibson, al haberse configura-do de forma paralela al mundo físico un espacio comunicativo e interactivo que, especialmente en la primera década del siglo x i, ha modificado las relaciones económicas, políticas, sociales y muy especialmente, las personales.

Hoy, la utilización de los servicios de Internet o las redes de la telefonía móvil constituyen la forma más común de comunicarse personalmente con familiares, amigos o personas del entorno laboral, y no sólo para adultos sino también para los menores de una generación que no entenderá la comunicación entre iguales sin la Red; también es Internet el vehículo por el que fluye ya la mayor parte del dinero en el mundo: todos los bancos y entidades financieras actúan por medio del ciberespacio, y cada vez son más las transacciones económicas y los negocios a pequeña, mediana y gran escala que se llevan a cabo directamente a través de este medio de comunicación global.

Además, todo parece indicar que la incidencia del ciberespacio en todos los aspectos de la vida social no va a ir disminuyendo, sino que seguirá creciendo. Conforme lideren el mundo los denominados “nativos digitales” o nacidos en la era de la web 2.0 popularizada, con los sistemas informáticos como forma de trabajo y también de diversión, con las redes sociales como forma de interactuación social, con las tecnologías móviles totalmente conectadas y con toda la información dio en la palma de su mano, el ciberespacio, como lugar de encuentro por el uso de las TIC, irá expandiéndose y la novedad del cibercrimen, como de cualquier otro elemento concatenado a ese espacio virtual que es para muchas personas aún más real que el otro, irá desapareciendo y lo único que cambiará será la concreta manifestación de éste a raíz del nuevo aspecto social digno de protección o la nueva tecnología que facilitará o modificará la forma de la comisión del delito. Porque lo que también es innegable, es que todos esos cambios sociales que estamos viviendo a raíz de los cambios tecnológicos que se están sucediendo, tienen su reflejo en la criminalidad como fenómeno social que es. Lo tienen, concretamente, en la aparición de un nuevo tipo de delincuencia aso-ciado al nuevo espacio de comunicación interpersonal que es Internet.

La evolución del cibercrimen como fenómeno criminológico ha transcurrido de forma paralela, a la evolución de los intereses sociales relacionados con las TIC: cuando el

protagonismo lo tuvieron las terminales informáticas y la información personal que ellas podían contener, aparecieron nuevas formas de afectar a la intimidad de las personas; cuando dichas terminales y la información en ellas contenida comenzaron a tener valor económico y a servir para la realización de transacciones económicas, surgieron las distintas formas de criminalidad económica relacionadas con los ordenadores y muy especialmente el fraude informático que, a su vez, evolucionó hacia el scam, el phishing y el pharmingcuando apareció Internet; finalmente, con la universalización de la Red y la constitución del ciberespacio comenzaron a surgir nuevas formas de criminalidad que aprovechaban la transnacionalidad de Internet para atacar intereses patrimoniales y personales de usuarios concretos, pero también para afectar a intereses colectivos por medio del ciberracismo o del ciberterrorismo.

Hoy, cuando el protagonismo empiezan a adquirirlo las redes sociales y otras formas de comunicación personal en las que se ceden voluntariamente esferas de intimidad y en las que se crean relaciones personales a través del ciberespacio, y que a la vez no disminuye sino que aumenta la actividad económica en Internet, asistimos a un momento álgido de la criminalidad en el ciberespacio, tanto en sentido cuantitativo dado el creciente uso de Internet en todo el mundo y por todo el mundo, como cualitativo al aparecer nuevas formas de delincuencia relacionadas con los nuevos servicios y usos surgidos en el entorno digital.

Obviamente esta evolución del cibercrimen también conlleva una evolución en sus protagonistas esenciales, los criminales y las víctimas: del ya mítico hacker estereotipado en el adolescente introvertido y con problemas de sociabilidad, encerrado en su casa y convertido en el primer ciberespacio en un genio informático capaz de lograr la guerra entre dos superpotencias usando sólo su ordenador, hemos pasado a las mafias organizadas de cibercriminales que aprovechan el nuevo ámbito para aumentar sus actividades ilícitas y sus recursos. Y al no ser los cibercrímenes únicamente los realizados con ánimo económico, también varían los perfiles de cibercriminales que cometen delitos que no son más que réplicas en el ciberespacio de los que ejecutarían en el espacio físico. Y lo mismo sucede con las víctimas. Las empresas siguen siendo objeto de victimización debido tanto al uso generalizado de las TIC en ellas como a sus recursos económicos objeto de deseo por los cibercriminales.

Pero la aparición de los cibercrímenes sociales convierten a cualquier ciudadano que se relacione en Internet, que contacte con otros, envíe mensajes, charle en foros o comparta sus fotos, en objeto de un ciberataque personal a su honor, intimidad, libertad sexual o similares bienes jurídicos. Y lo mismo sucede con otras instituciones supranacionales en relación con los cibercrímenes políticos o ideológicos cometidos con in-tención de desestabilizar un Estado o de difundir un determinado mensaje político aprovechando las posibilidades de comunicación masiva que ofrece el ciberespacio: la ciberguerra, el hacktivismo o el ciberterrorismo han convertido a los Estados, a los recursos públicos que ofrecen a los ciudadanos a través de Internet, en objetivo de ataques de denegación de

servicio, de infecciones de malware u otros que pueden llegar, como ha sucedido, a paralizar la actividad de importantes instituciones de un país.

Con lo afirmado hasta el momento estamos resaltando ya una idea importante que necesariamente se impone: la del carácter omnicomprensivo, a todo lo ejecutado en el ciberespacio, del cibercrimen. Es decir, que, frente a la primera visión que ofrecía la criminalidad informática de ser una modalidad de delincuencia muy específica, relacionada con concretas tecnologías y con reducidos usos de la misma, hoy la única visión posible, por funcional, sobre la cibercriminalidad es la de una delincuencia amplia, variada y cambiante que ni puede asociarse a una concreta tecnología o a un específico grupo de sujetos, ni limitarse a un concreto sector de la actividad social. Por el contrario la cibercriminalidad es hoy toda la criminalidad cometida en el nuevo espacio, al igual que la delincuencia tradicional es toda la ejecutada en el viejo. Es el lugar, en este caso el «no lugar», el que define y marca los eventos sociales en él realizados y el que, por tanto, configura también como distinta la delincuencia en él ejecutada. Y es ese ámbito y su carácter novedoso y cambiante lo que puede explicar la anteriormente comentada sensación de "novedad perpetua" que parece asociada al cibercrimen y puede ayudar a comprender, además, el reto político criminal al que nos enfrentamos: el de adaptar todas las estructuras políticas, jurídicas y sociales a la necesidad de protección de nuevos y viejos intereses frente a nuevas formas delictivas que son cambiantes porque lo sigue siendo el ámbito social en el que las mismas se producen.

También puede servir esta idea de que el cibercrimen no es más, ni menos, que el delito cometido en "el otro lugar", en el ciberespacio, para argumentar la perspectiva que se quiere adoptar: frente a la visión de análisis (que se ha dado desde los teóricos de la seguridad informática) del fenómeno del cibercrimen desde una perspectiva técnica, esencialmente descriptiva de los efectos (en los sistemas y en las re des) y de las causas (en términos informáticos) de los distintos ciberataques, es esencial adoptar una visión criminológica de la ciberdelincuencia en la que se analice la misma como lo que es, un evento social ejecutado por personas, individual mente o en grupo, con efectos sobre otras personas o instituciones sociales y ejecutado en un nuevo ámbito de intercomunicación social que incide en las conductas, quienes las realizan, sus efectos y en quienes sufren éstos.

Convertir el cibercrimen, en un evento irremediable en el que no nos preguntamos por su origen, por las causas del mismo, por quién y por qué lo realiza, difícilmente nos ayudará a la prevención completa y real del fenómeno. Del mismo modo, eliminar de la ecuación del ciberdelito a la víctima supone obviar que en las conductas que ella realice, en la incorporación a sus actividades cotidianas de usos seguros de interacción con ese nuevo mundo al igual que se tienen en el espacio físico, estará en gran parte la superación de este momento actual en el que el cibercrimen parece crecer irremediablemente.

En los tipos de criminales, de víctimas, y de comportamientos ilícitos en el ciberespacio, es obvia la imposibilidad de lograr la total sincronía de las descripciones y categorizaciones realizadas en este trabajo. Desde el mismo momento en que estas líneas sean leídas, estará desactualizado, pues es tanta la velocidad de mutación del ciberespacio que ya habrán surgido nuevas formas de conducta criminal, nuevos intereses sociales dignos de tutela, así como variados artículos de investigación que intenten aportar luz sobre todo ello. Y esto pese a que he tratado de ser lo más exhaustivo posible en las fuentes y de incorporar todas las formas de comportamiento "desviado" en el ciberespacio existentes hasta el momento de finalización del presente trabajo. En todo caso el que esto sea así demuestra, una vez más, la necesidad de un planteamiento más allá de la mera descripción de las conductas que surgen en Internet y justifica que se haga un análisis global del mismo pese a las evidentes diferencias existentes entre muchos de los delitos ejecutados en el ciberespaciocio. Sólo mediante una comprensión global del fenómeno que identifique los caracteres comunes del evento criminal cometido en Internet podremos mejorar la prevención de "la otra delincuencia del siglo XXI"

VIII.- CONCLUSION:

Creo haber seleccionado para la confección del presente trabajo un tema tan amplio, abarcativo y sumamente interesante una temática que integra varios aspectos del derecho. Sin temor a equivocarme, puedo asegurar que la tecnología atraviesa todos los aspectos de la vida social, nos ubicó, con la llegada de internet, en una nueva era y trasformó la sociedad moderna. El derecho penal, como se expuso, no quedó fuera de esta situación y la era digital y sus ramificaciones han calado profundo en distintas ramas penales a punto tal de significar un replanteo y resignificancia en materia político criminal, de sistema de garantía, procesal, legislativo, como herramienta de litigación y criminológica entre otros campos que no fueron tratados en este trabajo pero que sin hesitación alguna podemos decir que la evidencia digital los atraviesa.

Veo con preocupación el hecho que ante el desmesurado avance tecnológico y la falta de reacción de políticas públicas que doten al derecho penal de la suficiente solidez para responder a estos nuevos tipos delictuales y a esta nueva forma de litigar, se profundice un menoscabo y avallasamiento de garantías constitucionales en desmedro de principios y prerrogativas que hacen al debido proceso en juicio.

El uso de la tecnología, termina siempre por bridarnos facilidades a nuestra vida diaria, c

Una pandemia, como la que azoló al mundo estos ùltimos años, replanteo absolutamente todo el sentido de la audiencia, y obligó a los operadores judiciales a modificar las formas de trabajo, acomodarnos a una realidad que se instaló brutalmente y que amenazaba, y aún lo hace, el despliegue de un servicio de justicia lo más fluido y eficiente posible. Y no es

que antes de la pandemia la justicia aseguraba a la sociedad un impecable e eficaz servicio, lo que quiero significar es que la cuarentena vino a empantanar a un más un accionar judicial lento y con dificultades, en algunos casos en proceso de reforma. La tecnología resultó ser una especie de salvavidas que de alguna manera termina por imponer cambios que son sumamente necesarios, como por ejemplo la implementación del expediente digital, la posibilidad de que el MPF digitalice el legajo de investigación, la realización por medios virtuales de audiencias penales, hasta en algún punto se llegó a mencionar la posibilidad de realizar juicios de manera virtual.

Se han alzado voces a favor y en contra de la utilización casi total de la tecnología en materia penal, lo cierto es que tal y como sucede con la evidencia digital, la falta de protocolos, la casi nula legislación que existe sobre el tema, la escaza jurisprudencia y doctrina especializada y bien definida que permita brindar más claridad sobre algunos temas que al día de hoy generar controversias en torno a la evidencia digital, son algunas de las falencias que hoy tenemos que afrontar y solucionar, ante una realidad insoslayable, podemos estar a favor del uso y la intromisión de la tecnología en el derecho, lo que no podemos permitirnos es dejar de discutirlo, ignorarlo o hacer de cuenta que está de paso y que es algo de pasajero.

Como nos enseña el profesor SALT: brindarle un marco legal, legislar y reglamentar en materia de evidencia digital, no significa solo dotar al poder punitivo de más herramientas de persecución, sino que por el contrario, significa establecer las reglas de juego, significar hasta donde y de que forma el estado puede utilizar la tecnología como herramienta política criminal, sin verse afectada la intimidad de la persona investigada, es una forma de establecer los lineamientos de un la do y del otro que nos permita conocer y fijar pautas claras de cómo y hasta qué punto el estado puede acceder a datos privados, y sumamente íntimos de la persona.

Sinceramente, no veo un futuro no trágico en los tiempos que corren, si no somos capaces de estructurar políticas públicas en materia tecnológica que permita una permeabilidad aún más consagrada y comprometida entre el derecho penal y la evidencia digital, el negacionismo y la procastinaciòn en términos legislativos y de reglamentación de un fenómeno cada vez más presente en nuestra cultura no hace más que profundizar las falencias que presenta nuestro sistema en este tema.

Lo cierto es que es un trabajo arduo del que se requieren oír muchas voces especializadas en la materia que enriquezcan el debate y nos brinden nuevos horizontes, nuevos conceptos y formas que faciliten la convivencia del derecho y la tecnología. Sin embargo, la buena noticia es que nuestro país cuenta con una reconocida cantidad de autores y expertos en la materia, cuyos investigaciones fueron consultados para la elaboración del presente trabajo que han tratado este tema mucho más en profundidad, elaborando conclusiones sumamente interesantes y enriquecedoras que es necesario integrarlas y hacerlas conocer, de modo que

permitan trazar un camino y marcar el tono del debate. Será cuestión de ponerlo en la larga lista de espera que la ajustada y comprometida agenda de políticas públicas que nuestro país presenta en la actualidad.

BIBLIOGRAFIA:

1.- SALT MARCOS, “Allanamiento remoto ¿un cambio de paradigma en el registro y secuestro de datos informáticos?, en Cibercrimen II nuevas conductas penales y contravencionales. Inteligencia artificial al derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimologìA, DANIELA DUPY (DIR) – MARIANA KIEFER (COORD), B de F, MONTEVIDEO, 2018.

- La relación entre persecución de los delitos informáticos y el derecho penal internacional. Delitos informáticos. Aspectos de derecho penal internacional, en Revista informática y Delito. Reunión Preparatoria del XIX Congreso Internacional de la Asociación Internacional de Derecho Penal (AIDP)., Grupo Nacional, Facultad de Derecho UBA, Buenos Aires. Mar 2014.-
- Nuevos desafíos de la evidencia digital. Acceso trasfronterizo y técnicas de acceso remoto a datos informáticos, AD HOC, Buenos Aires, 2017.
- Obtenciòn de pruebas informáticas en extraña jurisdicción: “los conflictos del prinicipio de territorialidad en el mundo virtual sin fronteras”, en cibercrien. Aspctos de derecho pnal y procesal penal. Cooperaciòn internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicio de internet, DANIELA DUPUY (DIR) MARIANA KIEFER (COORD), B de , MONTEVIDEO, 2017.-

2.- Vigilancai Electrònica y otros modernos medios de prueba – CARLOS CHRISTIAN SUEIRO. 2DA EDICION – HAMURABI.

3.- BRUZZONE, Gustavo, "La *nulla coactio sine legue* como pauta de trabajo en materia de medidas de coerción en el proceso penal", en *Estudios Sobre Jurisprudencia Penal*, Ed. Del Puerto, Buenos Aires, 2005.

4.- GARCÍA, Luis M., "La intervención de las comunicaciones telefónicas y otras telecomunicaciones en el Código Procesal Penal de la Nación: un cheque en blanco para espiar nuestra vida privada", Ed. Ad-Hoc, Buenos Aires, 1997.

5.- GARIBALDI, Gustavo, "Las modernas tecnologías de control y de investigación del delito. Su incidencia en el derecho penal y los principios constitucionales", Ed. Ad-Hoc, Buenos Aires, 2010.

6.-KERR, Orin S., "Searches and Seizures in a Digital World", Harvard. L. REV. 531 (2005)

7.- PETRONE, Daniel, "Prueba informática", Ed. Didot, Buenos Aires, 2014.

8.-STUNTZ, William, "Local Policing After Terror", disponible en https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4611&context=ylj.

9.-SUEIRO, Carlos C., "Vigilancia electrónica y otros modernos medios de prueba", Ed. Hammurabi, Buenos Aires, 2017.

10.-CHAIA A. RUBEN., "Técnicas de Litigación penal" Ed. Hammurabi, Buenos Aires, 2020, tomo 3.-

11.-MAIER, Julio B. J., "Derecho procesal penal", Ed. Ad-Hoc, Buenos Aires, 2015,

12.- En "Criminal Profiling: An Introduction to Behavioral Evidence Analysis", Ed. Academic Press, San Diego, California, 1999.

13.- CANO CARRILLO, J., "Arquitecturas distribuidas de gobierno electrónico con ciberseguridad crítica", tesis doctoral, Ed. UNED, Madrid, 2015, p. 45, disponible en http://e-spacio.uned.es/fez/eserv/tesisuned:IngInd-Jscano/CANO_CARRILLO_Jesus_Salvador_Tesis.pdf.