Derecho y Tecnología

EL SUPLEMENTO LEGAL DE NEURONA BA

CON EL OBJETIVO DE ACOMPAÑAR EL DEBATE ACERCA DE LA EXPANSIÓN EN EL USO DE LAS TIC Y SU IMPACTO EN EL DERECHO, DESDE NEURONA BA LANZAMOS ESTE SUPLEMENTO SOBRE "DERECHO Y TECNOLOGÍA". TIENE LA COORDINACIÓN DE NUESTRO COLUMNISTA HABITUAL, EL ABOGADO, DOCENTE E INVESTIGADOR, ERNESTO LICEDA, CON UNA AMPLIA TRAYECTORIA EN ESTAS TEMÁTICAS.

AUTORES

ERNESTO LICEDA // Coordinador del suplemento legal Tecnología y Derecho de Neurona BA.

NOEMÍ OLIVERA // Abog. Docente e investigadora, fundadora y ex Directora del Grupo de Estudio de la Complejidad en la Sociedad de la Información (GECSI) de la Fac. de Cs. Jcas y Soc. UNLP.

ROLANDO J. ORTEGA HERNÁNDEZ // Doctor en Derecho Universidad de Salamanca, profesor Universidad Internacional de la Rioja, Abogado, Ilustre Colegio de Abogados de Salamanca (España).

NICOLAS ZAMBELLI // Abogado. Docente Universitario. Jefe de Trabajos Prácticos en Derechos Humanos y Garantías de la UBA.

MARINA FLAMMINI // Abog. Docente del Seminario de Digitalización del Poder Judicial Fac. Cs. Jcas. y Soc. UNLP.

ROBERTO NELSON BUGALLO // Abog. Docente investigador, Fac. de Cs. Jur. y Soc., UNLP; Fac. de Derecho, UBA; Fac. de Cs. Sociales, UNCPBA.

LEONARDO MONTI // Abog. docente adscripto en Derecho Procesal Penal en la Univ. Nac. de Córdoba y en la Univ Cat. de Córdoba.

EDGARDO VILLORDO // Abog. Mg. en Desarrollo Humano y en Gobierno y Economía Política Especialista en DDHH y Abog. Digital por la UNAM.

Recibimos comentarios y sugerencias vía mail a: neurona.buenosaires@gmail.com

PRÓLOGO

Por Ernesto Liceda

A esta altura de la inmersión (o ahogamiento) en la sociedad de la información debemos empezar a trabajar con la desnaturalización de algunas frases célebres. Una de mis favoritas, y reiterada hasta el hartazgo, es aquella que reza "estamos frente a un cambio sin precedentes". Es evidente que, en lo que respecta a avances en las tecnologías de la información, la época en la que vivimos realmente no tiene precedente, pero ello no implica que el cambio en sí no los tenga. Desde que se descubrió el manejo del fuego hasta nuestros días, la historia de la humanidad está plagada de cambios sin precedentes (CsP), la invasión de Roma por parte de los pueblos germanos, la invasión y colonización de América, la invención de la imprenta, la de la máquina a vapor, la revolución francesa, y muchos etc. han generado CsP en la sociedad, y por ello cada uno es precedente del posterior.

¿Qué podemos aprender de otros CsP de la historia que podamos tener en cuenta para el presente? En principio, muchos de estos fueron acompañados de cambios en la estructura de poder, en algunos casos cambiando de manos y en otros mejorando aún más la situación de sectores ya hegemónicos. Por otra parte, la desnaturalización de lo que antes era natural, que el Estado estuviese a cargo de un rey y que su primogénito lo continuara en el cargo era un hecho divino o natural, hasta que dejó de serlo. Otro de los factores es, justamente, la naturalización de fenómenos que son no tan naturales, pero que la reiteración los convierte en algo similar a un terremoto o un huracán "lo que se sube a Internet es imposible bajarlo". La particularidad, o una de ellas, de la naturalización es la ausencia general de ¿por qué? ¿está bien que así sea? ¿es realmente inevitable?

Esto equipara un fenómeno creado por nosotros a lo que debió ser el movimiento de las estrellas para los primeros hombres. Por último, la disputa simbólica por el lenguaje y los significados. La libertad de expresión es un concepto que fue acuñado en la relación Estado-ciudadano y que actualmente está presente en toda disputa sobre daños a la dignidad de las personas mediante diversos medios de comunicación (redes sociales, buscadores, etc) que claramente son privados ¿Qué comprende hoy este derecho? Las políticas de uso, o las múltiples licencias que se aceptan, ¿atentan contra la libertad de expresión? ¿la no eliminación de mensajes de odio, de violencias de género, de cuestiones íntimas la respetan? Son algunas de las preguntas que debemos ir pensando.

En el presente suplemento, se encuentran temas muy diversos pero todos ellos, a mí entender, sumamente interesantes.

En el artículo "Autorregulación, Responsabilidad e Inteligencia Artificial" la Prof. Abog. Noemí Olivera quien, entre varias otras cosas fuera Directora (y creadora) del Grupo de Estudio de la Complejidad en la Sociedad de la Información (www.gecsi.unlp.edu.ar) y varias veces presidenta del Simposio de Informática y Derecho de las Jornadas Argentinas de Informática (SID-JAIIO) de la SADIO, presenta un análisis sobre los conflictos derivados de la posible autorregulación de la Inteligencia Artificial, la responsabilidad frente a terceros y su uso en la toma de decisiones judiciales.

En "La Seudonimización de Datos Personales en las Resoluciones Judiciales Argentinas", Rolando J. Ortega Hernández -Doctor en Derecho Univ. de Salamanca, profesor Universidad Internacional de la Rioja- y Nicolas Zambelli –Abogado, miembro de la cátedra de Derechos Humanos y Garantías de la UBA- , contrasta el modo de trabajar los datos personales que son objeto de tratamiento en España y en el fuero federal argentino.

También se presenta "La Dignidad y la Digitalización del Poder Judicial" de la Abog. Marina Flammini y quien suscribe sobre el acceso a los datos personales desde la Mesa de Entradas Virtual (MEV) de la prov. de Buenos Aires. Este trabajo, que es un avance en el marco del Proyecto I+D J183 de la UNLP: "Servicio de justicia y gestión en contexto de las tics…" llevado adelante por el GECSI, busca generar conciencia sobre la grave situación de vulnerabilidad en la que nos encontramos.

Por otra parte, el Prof. Abog Roberto N. Bugallo, de amplísima trayectoria en lo que refiere a derechos humanos y derecho a la comunicación y la información nos presenta "Dos Sentencias Interesantes". Realiza un análisis pormenorizado de dos sentencias diferentes pero atravesadas por cuestiones de suma relevancia en la actualidad, las redes sociales, la violencia de género y el discurso de interés público protegido.

Cerrando el suplemento Edgardo Villordo de Chaco, abogado, Mg. en Desarrollo Humano y en Gobierno y Economía Política Especialista en DDHH y abog. digital por la Unam entre otras y Leonardo Monti de Córdoba, Abog. y docente adscripto en Derecho Procesal Penal en las Univ. Nacional y Católica de dicha provincia, realizan un trabajo sobre el hostigamiento digital, conocido también como Stalking, analizando su desarrollo en fueros internacionales y su regulación como contravención en la provincia de Córdoba.

AUTORREGULACIÓN, RESPONSABILIDAD E INTELIGENCIA ARTIFICIAL

NOEMÍ OLIVERA

Abog. Docente e investigadora, fundadora y ex Directora del Grupo de Estudio de la Complejidad en la Sociedad de la Información (GECSI) de la Fac. de Cs. Jcas y Soc. UNLP.

Desde los tempranos tiempos en los que el desarrollo de las TIC hizo posible la realización de actividades pasibles de tener consecuencias jurídicas, la consiguiente demanda de respuestas al Derecho en torno a qué trato se debería dar a las problemáticas derivadas o derivables de tales actuaciones dio lugar a variadas respuestas que fueron desde la demanda de regulación específica, a la asimilación de situaciones a otras ya reguladas o, por fin, a la autorregulación.

El término "autorregulación" no es unívoco. Con él se alude tanto a las situaciones en las que, dado un contrato, las partes pactan las reglas a las que se someterán en el marco de su vigencia como a una situación muy particular, cual es que el titular de los derechos sobre cierta tecnología, determine por sí las reglas que impone a quienes devendrán en usuarios de ella; a su vez, esta "autorregulación" puede estar incorporada -embeded- en el producto o no.

Cincuenta años después, ante la utilización profusa de IA estamos casi en el mismo lugar; la única diferencia que se advierte a primera vista es que ya no es tan frecuente la demanda de legislación, ahora el énfasis está puesto en las características que debería asumir esa autorregulación.

El derecho, por enmarañado que pueda parecer, no es más que un sistema destinado a "conservar" un cierto estado en la sociedad, sancionando a quienes alteran el orden establecido y reparando el daño sufrido por el obrar de otro. Para ello se han ido desarrollando, desde antiguo, sofisticados sistemas de imputación de responsabilidad. Se pretende con ellos que el autor responsable de un daño se haga cargo, ante la sociedad, del perjuicio causado y restaure el estado de cosas, según sea el caso, mediante sanciones penales o indemnizaciones.

Ahora bien, si se ahonda en las propuestas y sus fuentes, nos encontramos con que, en el caso de la IA, quienes más enfáticamente promueven la autorregulación están del lado de los desarrolladores. La pretensión es poder llegar a predeterminar las reglas de juego sin intervención exógena. El problema es que "los desarrolladores" a quienes la cuestión preocupa no son simples informáticos egresados de universidades nacionales, sino los mayores creadores y usuarios de inteligencia artificial, empezando por el grupo GAFA. Veamos algunas de las propuestas que se han realizado hasta ahora.

1.- Algunos postulan que, habiendo dotado al algoritmo de una cierta ética, el creador no responderá por las consecuencias inesperadas y no queridas que se puedan derivar del aprendizaje y puesta en práctica de la IA. Menudo problema, podríamos llegar a encontrarnos ante situaciones en las que, producido un severo daño, sea a las personas, a las cosas o aún ambiental, no se pueda imputar responsabilidad a nadie, no habrá un patrimonio afectado a reparar ese daño. Eso, más allá de cómo se llegará a probar que las consecuencias fueron inesperadas y no queridas ¿se deberá ofrecer un listado de las consecuencias efectivamente esperadas y queridas? Ello ofende hasta mis limitados conocimientos en materia de

complejidad, base del sistema.

La primera cuestión a resolver ante este planteo es, entonces, la referida a la ética de la IA. Va de suyo que tal pretendida ética no será autogenerada por la IA, sino que le será incorporada por el programador, quien puede compartir la moral predominante en la sociedad en un dado momento o no. Entre los primeros aprendizajes de quienes estudian Derecho se cuenta aquello de que, cuando una norma alude a que un dado acto "no sea contrario a la moral y las buenas costumbres" no fija un parámetro rígido y omnivalente, sino que ello debe ser interpretado en relación al tiempo y lugar donde dicho acto tuvo lugar. La ética es una disciplina de la filosofía que estudia la moral, la que, a su vez, se ocupa de las acciones de las personas de cara al bien y el mal, sean éstas individuales o colectivas. Bien aclara el Diccionario de la R.A.E. en la 4a acepción del vocablo moral: "Que concierne al fuero interno o al respeto humano, y no al orden jurídico". ¡Pero, siguiendo esta línea de propuestas, el creador podría eximirse de responsabilidad -en el marco del régimen jurídico- si puede probar que programó el algoritmo para que sea lo que, a su juicio y sólo a su juicio, sería bueno!

2.- Otros promueven el reconocimiento de la "personalidad electrónica" de la IA. A fin de dilucidar el contenido y alcance de esta propuesta, partamos del hecho de que la personalidad no es un hecho de la naturaleza, sino un concepto jurídico. En otras palabras, personas son los entes que el derecho diga que lo son y, hasta el presente, en nuestro ordenamiento jurídico existen dos clases de personas, las humanas y las jurídicas -ello, sin considerar la discusión doctrinaria sobre la posible existencia de personas no humanas, animales, por ejemplo-. En los sistemas jurídicos vigentes en la civilización occidental de nuestros días todos los seres humanos son personas; no siempre fue así, pensemos en los esclavos.
Las personas jurídicas son, en tanto, organizaciones que el legislador considera valiosas para la sociedad o el mercado y, al reconocerlas en tal carácter, permite que sus miembros alcancen el más preciado beneficio que de ellas se deriva, cual es la diferenciación patrimonial. Uno es el patrimonio de la persona jurídica, otros son los de sus miembros. Es cierto que los miembros no quedan absolutamente desvinculados de la responsabilidad patrimonial ya que, agotado el patrimonio de la persona jurídica, los acreedores pueden atacar el de los socios, salvo en el caso de las entidades que reconocen la limitación de la responsabilidad de sus miembros cuando se ha integrado efectivamente el capital aportado. Dicho así, parece que estoy aludiendo a casos excepcionales, y es cierto que ello fue tenido en vista por el legislador primigenio; pero en nuestros días una amplísima mayoría de las sociedades comerciales se constituyen como SA, SRL o SAS en busca, precisamente, de la limitación de la responsabilidad. Y esta situación es, incluso, alentada por el legislador de nuestro tiempo con el alegado propósito de "proteger los intereses del mercado" -dicho de otro modo, para facilitar la acción de los actores del mercado que persiguen maximizar el beneficio evitando asumir riesgos-.

Veamos cómo se plantearía la cuestión si se reconociera la existencia de las "personas electrónicas". Al tiempo de la creación de una IA se la debería dotar de un conjunto de reglas que hagan posible su actuación en el mundo jurídico. Esto es, tal IA deberá tener nombre, domicilio, un conjunto de especificaciones que pongan límites a su obrar en tal carácter y, por fin, un patrimonio suficiente para poder afrontar el resarcimiento o la reparación del perjuicio que pueda causar a un tercero. Primera pregunta, ¿quién determinará estas cuestiones? Sólo hay dos opciones, o lo hace el programador por sí o programa el algoritmo para que él mismo lo realice. En suma, lo hace el programador. Otra vez, estamos ante un caso en el que, desde la fuente originaria de una dada situación jurídica, se predisponen las reglas que deberán aceptar quienes interactúen con el actor, la IA, en este caso. Esto no es autorregulación, sino imposición de las propias reglas.

Ahora bien, ¿cómo se puede prever la magnitud del patrimonio necesario para afrontar una consecuencia inesperada? En ámbitos europeos se alienta la contratación de seguros, pero, otra vez,

¿cómo podrán las aseguradoras establecer el valor asegurado y las primas a pagar? Más aún, ¿quién contratará y pagará dicho seguro?

La "interpósita persona" viene siendo utilizada hace años para alejar a los titulares de los intereses económicos de los acreedores derivados de la actuación realizada en su interés. Es así como hemos asistido a la proliferación de personas jurídicas constituidas, cual mamuschkas jurídicas, con la sola pretensión de evitar que los verdaderos dueños del negocio asuman su responsabilidad frente a los perjuicios derivados de su obrar o el de sus representantes. ¿Podemos aceptar la emergencia de una "persona electrónica" para alejar a los creadores -insisto, quienes sean titulares de los derechos y obligaciones, no necesariamente los programadores, de quienes han sufrido daños en el marco de la actuación de una IA creada por o para ellos? ¿No será hora de ponernos a pensar en modelos novedosos que protejan y alienten el desarrollo de las creaciones, sin desproteger a quienes pudieran haber sido víctimas de las consecuencias inesperadas del obrar de una dada IA?

3.- Por fin, mientras algunos autores plantean la falta de responsabilidad del programador dada la "independencia de la IA", otros proponen que la IA puede reemplazar al juez en las sentencias. Consideremos una situación posible:

- Un programador con profundas convicciones religiosas crea una IA y le atribuye "su" ética. Tal IA es utilizada para dictar sentencia en un caso en el que una niña abusada pretende interrumpir su embarazo -ILE prevista en el Código Penal desde 1921-. ¿Cómo superará la IA el dilema entre regirse por su ética o aplicar el régimen legal vigente? Entre humanos, conocida la posición del juez, se lo puede recusar. ¿Cómo podrán los justiciables acceder al conocimiento de "la ética" de la IA?

Se ha propuesto que las características que debería, en definitiva, asumir esta IA dictadora de sentencias, deberían resultar del trabajo de un equipo interdisciplinario. A mi juicio esto no haría más que multiplicar la problemática en función de la variedad de especialistas convocados a determinarla.

Por otra parte, reconocida que fuera la personalidad electrónica de la IA, bien podría suceder que resultara denunciada, actora o demandada en un juicio. ¿Qué parámetros éticos deberían prevalecer ¿los de la IA jueza? ¿lo de las IA cuyo accionar ha dado lugar al litigio?

Como se advierte, sería posible seguir hasta el infinito imaginando situaciones en las que las IA realicen acciones con consecuencias jurídicas. Tengo para mí que este ejercicio es escasamente fructífero. No somos algoritmos corriendo en ultra procesadores.

Sería más útil empezar a pensar en las características que debería tener el sistema jurídico que debe regir sobre las realidades sociales y tecnológicas de nuestro tiempo, en vez de seguir alentando la introducción de reformas o interpretaciones extensivas de un sistema que fue apto para la sociedad de la revolución francesa y la revolución industrial.

LA SEUDONIMIZACIÓN DE DATOS PERSONALES EN LAS RESOLUCIONES JUDICIALES ARGENTINAS

ROLANDO J. ORTEGA HERNÁNDEZ [1]

NICOLAS ZAMBELLI [2]

[1] Doctor en Derecho Universidad de Salamanca, profesor Universidad Internacional de la Rioja, Abogado, Ilustre Colegio de Abogados de Salamanca (España)

[2] Abogado. Docente Universitario. Jefe de Trabajos Prácticos en Derechos Humanos y Garantías de la UBA

Es común, si entras en la página web del poder judicial argentino, poder buscar las causas en curso por el nombre de las partes. Este acceso, salvo ciertas excepciones se puede realizar para la mayoría de las causas, por tal motivo se puede observar las actuaciones en curso, y muchas resoluciones judiciales. Dicha práctica obedece al principio de publicidad de los actos públicos, o emanados del poder público.

El principio de transparencia y publicidad que debe permear a todo un sistema jurisdiccional nos plantea algunas interrogantes en cuestiones relacionadas con los derechos a la intimidad y privacidad. Dichas interrogantes se potencian debido a la exposición de los datos personales en Internet, dónde podría pensarse que dicha exposición resultaría considerablemente más contraproducente para la protección de los datos personales que el propio principio de publicidad de los actos públicos. Por estas razones debemos tener en cuenta la afectación a los derechos de creación relativamente reciente relacionados con la protección de datos personales, su publicidad y su tratamiento.

Es de entender que la Sociedad de la Información (SI) en la que el mundo desde hace más de 20 años estaría inmerso ha suscitado la necesidad de una continua adaptación. Esta necesidad ha generado un caos en la interpretación de contextos antiguos relacionados con el derecho contrastado con la inmediatez de respuestas requeridas para la adaptación a situaciones presentes. Debemos por tales motivos tener en cuenta que, no es lo mismo acceder a un expediente desde la sede de un juzgado en dónde, sólo el interesado accede a las actuaciones judiciales que poder acceder desde una página web donde la exposición de los datos personales y el riesgo de su tratamiento indebido es exponencialmente mayor.

De tal forma, nos podemos plantear varias hipótesis referidas al tratamiento de protección de datos personales en la implementación de un sistema de gestión integral y automatizado en el ámbito jurisdiccional. En primer lugar se trata de identificar como se podría balancear y garantizar una administración de justicia transparente sin menoscabar los derechos de protección de datos personales y que la enmarque en un contexto jurídico internacional.

En este sentido, se ha venido planteando en Argentina la posible aplicación de criterios de tratamiento de datos personales en la publicación de las resoluciones judiciales. Tales criterios estarían referidos a los derechos de acceso, rectificación, cancelación, oposición, incluso de la portabilidad de datos personales. Claro está que, la aplicación de los criterios internacionales de protección de datos personales, deben ser ponderados y balanceados con una administración de justicia transparente de forma que la protección de datos personales se pueda equilibrar con la propia publicidad de los actos emanados de los Poderes Públicos.

Por estas razones, podría ser muy positivo aplicar

las prácticas de disociación, anonimización o seudonimización de los datos personales en las resoluciones judiciales. Esta práctica, ya está consagrada en España, establecida directamente en el artículo 235 bis de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ), que señala "…el acceso al texto de las sentencias, o a determinados extremos de las mismas, o a otras resoluciones dictadas en el seno del proceso, sólo podrá llevarse a cabo previa disociación de los datos de carácter personal que los mismos contuvieran y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda. En todo caso se adoptarán las medidas necesarias para evitar que las sentencias y el resto de las resoluciones dictadas en el seno del proceso puedan ser usadas con fines contrarios a las leyes…". Por ejemplo, en España cuando se accede a las bases de datos jurisprudenciales están publicadas todas las sentencias, con número de sentencia y recurso, incluso aparece el nombre del juez o magistrado ponente, sin embargo, lo único que no podemos ver es el nombre real de las personas involucradas. De tal manera, podemos observar el procedimiento y los fundamentos jurídicos aplicados pero no los datos personales. Para efectos de este artículo se englobarían los términos de anonimización, seudonimización y disociación como técnicas similares o análogas aunque pueden tener distintas connotaciones.

Los procedimientos de anonimización, disociación y seudonimización de datos personales en las resoluciones judiciales pueden resolver muchas cuestiones cuando se trata de datos de carácter sensible. En general, como es sabido, los datos de carácter sensible serían los datos referidos a ideología política, orientación e identidad sexual, salud entre otros. El tratamiento de dichos datos requiere medidas de seguridad alta. También podemos observar que en Argentina en cuestiones penales y de familia se toman medidas para seudonimizar estos datos utilizando nombres distintos. Ahora bien, los datos de carácter personal dejan de ser datos sensibles cuando son disociados de la persona que posee estas situaciones o datos. Por otra parte, en las sentencias, existen algunos datos que no son evidentes pero que se pueden atribuir por el relato de los hechos y que posiblemente no puedan ser catalogados como datos de carácter sensibles. Más importante aún, desde el punto de vista de quienes escriben este artículo, sería el hecho de que la seudonimización y anonimización de datos personales automáticamente establece una especie de muro contra la vulneración a la intimidad de las personas. En este sentido, señala el considerando (28) del Reglamento Europeo 2016/679 de 27 de abril de 2016 general de protección de datos; "La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos…"

En ese contexto, mediante la Acordada Nro. 15/2013, la Corte Suprema de Justicia de la Nación Argentina ha establecido, por un lado, la publicación y acceso general en todos los expedientes en trámite por ante Poder Judicial Federal salvo, como excepción, las relativas al fuero de familia y/o penales. Esto es, cualquier expediente tributario, civil, contencioso administrativo, comercial, por citar solo algunos, tiene -con un solo acceso web- posibilidad de vista a quien así lo requiera, siempre y cuando, no incumba los fueros ya predichos o bien los propios justiciables lo soliciten expresamente ante el Magistrado actuante. En cuyo caso, solo podrán ver los expedientes vía web los netamente autorizados, los letrados de las partes y los auxiliares de la justicia (peritos, administradores, notarios, etc.).

Debemos aclarar que, la no publicación virtual de estos casos no incluye la no referencia al nombre e identificación de las personas litigantes. A saber, no se discute al acceso al expte por parte del público en general o las causas reservadas a las partes en procesos sensibles; lo que se confronta, en realidad, es la imposibilidad de que, una vez con posible acceso al expte o con obligatoria publicación de la sentencia, no sean los litigantes individualizados por siglas o con caracteres que alteren su real identidad, su privacidad

como justiciable. Esto es, salvo sea expresamente solicitado por una de las partes, los nombres en el expediente aparecerán correctamente referidos, siendo solo la única excepción que el litigante, la víctima o el damnificado/a sea menor de edad.
De esta manera, en Argentina, salvo sea autorizado por el Juez mediante expresa solicitud previa, se continúa incluyendo la totalidad del nombre del imputado o damnificado, de la persona que accede a un simple divorcio vincular, al actor o bien al propio demandado que se ve en la imposibilidad de impedir que su nombre se pueda fácilmente identificar del propio expediente, con eventual vista de miles de colegas, ciudadanos y profesionales ajenas a la contienda y en simple búsqueda de doctrina y jurisprudencia.

En ese contexto, señala el Artículo 1 de la Acordada ya citada que todas las sentencias federales deben ser publicadas, según corresponda, sin afectar los derechos personalísimos de los involucrados. Así, ex ante, si la víctima del hecho es menor, si bien su nombre no será publicado, si lo serán todos los demás intervinientes dentro del expediente de manera completa, identificable y muchas veces con nombres propios, siendo la única solución a tal disyuntiva, la de solicitar expresamente al Magistrado interviniente su no inclusión al momento de su publicación. Tal es el caso que, si un imputado no solicita dicha reserva de su nombre de forma prematura, al momento de dictarse sentencia condenatoria o absolutoria, su nombre es publicado de manera global mediante web page en el Centro de información Judicial (C.I.J.).

Tan natural es la situación que, en la práctica, casi la totalidad de los fallos que hoy en día estudiamos a la hora fundar un nuevo y semejante pleito, los mismos son reconocidos en la jerga tribunalicia por los nombres propios de los intervinientes que, incluso, muchas veces, siquiera saben que son “famosos” en el ámbito judicial una vez terminado su propio proceso.

Sin perjuicio de lo expuesto, la Ley 25.326 tiene por objeto, tal cual lo informa la propia norma, la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

De estos dos extremos, la Acordada 15/13 CJSN y la 25.326, encontramos la disyuntiva sobre sí como sociedad enmarcada e inmersa en varios Tratados Internacionales en materia de Derechos Fundamentales (Declaración Americana, Convención Americana de Derechos Humanos entre varios otros de raigambre constitucional desde el año 1994), debemos hacer prevalecer el acceso a la información pública o los derechos personalísimos de los justiciables.

En este orden de ideas, los autores, así como muchas otras personas del ámbito jurisdiccional y académico, entienden que es necesario por lo menos una discusión académica y parlamentaria, en cuanto a la posibilidad de anonimización, seudominizacion de los datos personales en las resoluciones judiciales en Argentina.

LA DIGNIDAD Y LA DIGITALIZACIÓN DEL PODER JUDICIAL

MARINA FLAMMINI[1]

ERNESTO LICEDA

[1] Abog. Docente del Seminario de Digitalización del Poder Judicial Fac. Cs. Jcas. y Soc. UNLP

La digitalización del expediente judicial en la Provincia de Buenos Aires ha generado una expansión en lo que respecta al derecho de acceso a la información pública y a la transparencia de los actos de gobierno, todo ello por medio del uso de distintas tecnologías de la información y la comunicación. Pero ello no impide plantear que lo hizo en desmedro de derechos personalísimos como la intimidad y la privacidad, ambos hoy comprendidos en el derecho a la dignidad de las personas.

En la provincia de Buenos Aires, el uso de la informática en la publicidad de los procesos judiciales vio su inicio en torno a la Mesa de Entradas Virtual -en adelante MEV-, plataforma que permite el acceso a distintas causas en todos los fueros pero con algunas diferencias en lo que respecta al modo en que se puede acceder a ellas. Para ello, evidentemente era necesario que todos los juzgados y tribunales comenzaran a dotar a dicha plataforma de la información necesaria. En virtud de ello, la Suprema Corte de Justicia provincial, dictó la Resolución Nº31/991, mediante la cual se dispuso que en los juzgados civiles y comerciales y en los tribunales del trabajo se realice la carga completa de datos de los expedientes judiciales en el sistema de gestión e información, a fin de permitir conocer el estado de cada trámite cumplido.

Así, se aseguró que el derecho a la información de litigantes y letrados, en relación a las causas que tramiten por ante cualquiera de los órganos jurisdiccionales de la Provincia de Buenos Aires, quede efectivamente asegurado por medio de la MEV. Pero, paralelamente, permitió el acceso a prácticamente todos los expedientes a cualquiera que cuente con un usuario en dicho sistema. De esta manera la Suprema Corte de Justicia de la provincia creó, con o sin intención, un sistema de control ciudadano de los actos realizados por el Estado, impensado para el poder judicial hasta no hace mucho tiempo.

Mediante esta posibilidad, los ciudadanos podrían ejercer un control sobre los reclamos presentados ante el poder judicial, de las decisiones de este y de los tiempos que conllevan los procesos. Díaz Cafferata planteaba que “el derecho de acceso a la información pública es una figura relativamente novedosa, y con una configuración parcialmente distinta en los diferentes sistemas jurídicos que la han receptado”, tal vez podamos incluir en dicha definición que no sólo puede tener diversas configuraciones sino que también puede ser un efecto colateral.

Pero como planteamos anteriormente esta nueva posibilidad de control no está exenta de problemas. Debemos tener presentes algunas clasificaciones sobre la información. Vivant realiza una clasificación basada en tres tipos de vínculos entre la información y el nivel de acceso. La información reservada, que puede ser de interés público o privado, cuenta con controles en sus niveles de accesibilidad y para poder acceder a ella es necesario solicitar permiso. La información accesible, a la que se puede acceder, aunque no necesariamente se deba acceder. Y la información común o pública, que no puede ni debe retenerse y pertenece al ámbito público (fundamentada en la publicidad de los actos de gobierno, control de los jueces, transparencia, etc.).

Una primera distinción es en lo que respecta al acceso a los datos teniendo en cuenta el fuero al que correspondan los expedientes. Por un lado el fuero de familia donde la intimidad personal y del grupo familiar es central en prácticamente todas las causas. Por esto se utiliza un sistema de acceso restringido, donde aquel que necesite ingresar deberá solicitarle el permiso correspondiente. Serán los legitimados para acceder al expediente las partes, sus letrados, el Ministerio pupilar y terceros debidamente autorizados. La resolución de la Suprema Corte de Justicia nº 545/06 estableció un sistema de protección de datos por el cual el acceso informático a la causa es autorizado por el Juzgado, con la finalidad de controlar que la causa sea consultada sólo por los legitimados. En cuanto a las sentencias, se mantiene la privacidad y a los efectos de difundir los criterios y sentar jurisprudencia se lleva a cabo un proceso de disociación de las personas involucradas mediante la utilización de iniciales para los nombres y apellidos.

En cambio, en el fuero penal, si bien predomina el principio de publicidad, el mismo siempre podrá ser reevaluado durante la etapa de investigación cuando el hecho de dar a publicidad las actuaciones pueda hacerla peligrar. Pero, en lo que respecta al acceso mediante la MEV a la causa y a los elementos probatorios sucede algo similar al fuero de familia, debe solicitarse la autorización y en principio sólo podrán acceder el imputado, su defensa, los auxiliares designados en el proceso judicial pero no así terceros.

Por lo antes expuesto se decidió llevar adelante un trabajo de campo exploratorio para determinar las posibilidades de acceso mediante la MEV a distintos expedientes judiciales de los fueros civil y comercial; laboral y administrativo, establecer también algunos niveles de seguridad de la información con los que cuenta al momento del ingreso al sistema y a la toma de vista de los expedientes. En esta etapa no hemos avanzado aún sobre los sistemas de seguridad de la información acerca del almacenamiento, modificación o eliminación de los datos entre otros.

Es preciso tener en cuenta que la MEV permite la creación de dos tipos de perfiles, uno con el rol de abogado donde se deben cargar, aparte de los datos “comunes”, los datos referidos a la matrícula profesional y el otro con un rol particular donde estos últimos datos no son requeridos.

Para llevar adelante el trabajo de campo exploratorio se procedió, en primer lugar, a establecer algunas palabras claves que se utilizaron en las distintas búsquedas dentro del sistema. Es preciso mencionar que en esta etapa del proyecto de investigación el equipo decidió no dar a conocer las palabras clave seleccionadas para no colaborar en la violación de la dignidad de las personas involucradas en causas judiciales en los fueros laboral, administrativo y civil y comercial.

Una vez elegidas las palabras clave para las búsquedas, se llevó adelante un primer ingreso a la Mesa de Entradas Virtual desde un usuario “real” con el rol de abogado. Dicho perfil ya había sido creado con bastante anterioridad y es utilizado normalmente para la revisión de expedientes en los citados fueros. Se comenzó una búsqueda de expedientes (causas) utilizando las palabras clave seleccionadas, arrojando como resultados grandes cantidades de expedientes en los distintos juzgados y fueros. Posteriormente se ingresó al azar en algunos expedientes, particularmente del fuero civil y comercial pudiendo acceder a múltiples datos personales y sensibles. Las únicas limitaciones encontradas fueron la falta de carga de la información en el sistema.

Una vez establecido el nivel de acceso que se podía lograr mediante el perfil con rol de abogado se realizó un nuevo ingreso, esta vez por medio de un nuevo usuario “real” pero sin el rol de abogado, se repitieron las búsquedas con las palabras clave seleccionadas. Los resultados fueron exactamente los mismos y el acceso a los expedientes (los mismos a los que se había accedido desde el perfil con el rol de abogado) también. Es decir, desde un usuario de rol particular y sin ningún mecanismo de autenticación sobre los datos brindados al momento de crearlo, el equipo logró acceder no sólo a los datos personales de las

partes y de terceros - como domicilio, propiedades, partidas de nacimiento, etc-, sino también a datos sensibles, tales como enfermedades, consumo de medicamentos, tiempo y lugares donde algunos de los sujetos del proceso fueron internados, entre muchos otros datos. Debemos tener presente que conforme a la ley 25326 de protección de datos personales, los datos sensibles deben ser objeto de un tratamiento diferente al de los datos personales, lo que evidentemente no ocurre en la MEV. Independientemente de ello, entendemos que el acceso irrestricto (sólo hay que crear un usuario) a los expedientes configuran una grave violación a la dignidad de los justiciables.

Un punto central a tener en cuenta, y que puede plantear serios problemas tanto para el poder judicial como para los justiciables, es lo que establece la citada ley 25326, sobre la licitud del tratamiento de datos personales, en su art. 5 inc. 2. a. "No será necesario el consentimiento cuando: Los datos se obtengan de fuentes de acceso público irrestricto"

Y he aquí el eje de la cuestión, la Mesa de Entradas Virtual del Poder Judicial de la Provincia de Buenos Aires, ¿es una fuente de acceso público irrestricto? De ser así, todos los datos existentes en ella podrían ser objeto de tratamiento por parte de terceros totalmente ajenos a las diversas causas.

Como adelanto de los resultados del proyecto podemos decir que, el sistema MEV (dejando de lado los ya citados fueros de familia y penal) puede ser considerado "una fuente de acceso público irrestricto" conforme al art. 5 inc. 2. a. ley 25326. La simplicidad con la que se puede conocer el contenido de un expediente con datos sensibles (conf. art 2 ley 25326) permite pensar que no se han tenido en cuenta la preexistencia de los límites físicos ni los resultantes de la interacción humana para el acceso a ellos. Es decir, no se reconoció el trabajo de control que podrían ejercer, de hecho, los empleados judiciales ni se pensaron medidas para mitigar dicha falta de filtros. Es necesario lograr un equilibrio entre la accesibilidad, la "transparencia" y la dignidad de las personas involucradas y sus derechos individuales. Entendemos que sería deseable la creación de protocolos de seguridad de la información donde, entre otras cosas, se determine claramente las categorías de la información (o datos), el tratamiento y los permisos de acceso. O directamente proceder a la disociación de los datos en los expedientes.

DOS SENTENCIAS INTERESANTES

ROBERTO NELSON BUGALLO
Abog. Docente investigador, Fac. de Cs. Jur. y Soc., UNLP;
Fac. de Derecho, UBA; Fac. de Cs. Sociales, UNCPBA.

La irrupción de las llamadas nuevas tecnologías de la comunicación impone a los actores jurídicos, revisar definiciones, sentencias y doctrinas que están en proceso de construcción, por eso, cuando se encuentran pronunciamientos judiciales del tema, fuerza compartirlos. Acá van dos sentencias recientes que involucran el uso de las tecnologías digitales.

INJURIAS POR TWITTER

En marzo de este año, el Juzgado Correccional de Olavarría, dictó sentencia en una querella iniciada por un docente de una escuela secundaria privada de esa localidad que se sintió afectado por unos twitters de un ex alumno. Éste, residiendo en La Plata al ver en un video las marchas en contra del proyecto de ley de despenalización del aborto, al distinguir al Director en la concentración, escribió: “XX, en marcha Provida en Olavarria. Cuando iba a la escuela (...) y él era director, un profesor acosó a una compañera nuestra. No sólo no lo echó, sino que nos dio una charla sobre cómo cuidarnos en las redes sociales, como si la piba tuviera la culpa. Hipócrita”. “Mucha gente difundiendo este tweet. Aprovecho para decir que el profesor acosador era NN”. El comentario fue recogido y viralizado por varias personas, incluida quien supuestamente fuera acosada.

El Director y el docente aludido intimaron al joven a retractarse públicamente y al pago de una compensación económica bajo amenaza de accionar civil y penalmente. Ésta se concretó cuando el docente lo querelló por injurias, figura sancionada con multa de hasta veinte mil pesos.
Y con relación al uso de las tecnologías digitales deslizo algunas reflexiones.

A) Nuevas figuras productoras de daño: Actualmente, las conductas con reproche penal (calumnias e injurias) trasmitidas por las redes sociales o las tecnologías digitales, desplazan a la comunicación tradicional, (discursos, prensa escrita o radiodifusión) rumores, críticas, comentarios, chismes y opiniones antes restringidos a circuitos limitados, hoy se difunden a una velocidad asombrosa por whatsapp, Instagram, Facebook, Tinder, Twitter o Linkedin, u otra redes, pudiendo quedar alojados para quien quiera recrearlos potenciando la memoria personal o colectiva.

La masividad de redes y tecnologías digitales trajo situaciones desconocidas obligando a buscar respuestas jurídicas, mayormente impotentes o insuficientes frente al conflicto que involucran varios derechos (comunicación, honor, imagen o privacidad entre otros). Figuras como pornovenganza, ciberbullying, stalking, sexting, grooming o phishing, -algunas incorporadas a los códigos penales o civiles- aparecen como ocasionadoras de daños, y están en pleno proceso de elaboración jurisprudencial y doctrinaria.

B) Dificultades procesales: Generalmente su aplicación trae dificultades nuevas. Y una está referida a la probanza. Imágenes, posteos, mensajes o videos dañinos que transitan por las redes muchas veces quedan circulando por poco tiempo haciendo difícil utilizarlos como medios de prueba y trabajoso para los operadores jurídicos ofrecer herramientas legales adecuadas. Las capturas de pantalla, sin certificación notarial, deben complementarse con otros medios de prueba y las compañías prestatarias de telefonía celular o internet, son muy reacias y morosas para

contestar intimaciones judiciales o no, además del plus de quienes usan perfiles falsos.

Aún así, no es imposible para los peritos informáticos individualizar celulares, computadoras o tablets, de donde vienen los mensajes dañosos.

En Europa han surgido empresas especializadas en prueba digital, que actúan como "terceros de confianza" y acreditan -con un sello de tiempo-, (timestamp) que un conjunto de datos existió en una fecha y hora concretas y que ninguno de estos datos ha sido modificado desde entonces. (ej. eGarante). Aquí todavía no se han desarrollado, pero ya hay intentos.

C) Cuestiones de competencia: La última reflexión refiere a un tema de competencia.

En el caso, el imputado se domicilia en La Plata y los twitts fueron emitidos desde su celular. Se plantea cuál es la competencia jurisdiccional: si el lugar desde donde se emitieron los mensajes lesivos o donde se producen las consecuencias dañosas.

La jurisprudencia no es categórica. Uno de los pocos antecedentes refiere a calumnias e injurias vertidas en Bahia Blanca y dirigidas a la Dirección de Cultura y Educación y al Gobernador de la Provincia, ambos con domicilio oficial en La Plata donde la competencia fue resuelta a favor del Juzgado Correccional de Bahía Blanca ("Incidente de competencia entre el Juzgado Correccional Nro. 1 –Bahía Blanca y el Juzgado Correccional Nro. 4 –La Plata" Causa Nro. 19759 Cámara de Casación Penal, Sala I, 25/08/2005). Es de suponerse que al referirse al soporte digital utilizado, la jurisprudencia no alteraría la competencia territorial.

¿Y cómo terminó la querella? Con una absolución. El Juzgado entendió que el comentario refería a un asunto de interés público por tratarse de un supuesto de violencia de género y la conducta quedaba desincriminada por la nueva redacción de las calumnias e injurias -Ley 26.551-

N.N. c/FACEBOOK s/Habeas data

Otra sentencia interesante –en justicia federal de La Plata- refiere a un habeas data contra Facebook SRL por un actor que solicitaba se eliminara una fotografía suya subida sin autorización, se suprimieran ciertas URL con declaraciones injuriantes, y comentarios y datos subidos a INSTAGRAM, además de pedir información del titular de la cuenta, el correo vinculado, número de IP y otros datos para accionar por vía civil, afirmando que las expresiones lesionaban su honor, intimidad e imagen.

El reclamo se originó por publicaciones en Facebook e Instagram de una denominada "Comisión de Género" existente en una de las Facultades de la UNLP involucrándolo en conductas machistas, de abuso psicológico y manipulación vinculadas a una relación sentimental que había mantenida con una compañera.

El actor sostuvo haber reportado el reclamo en la plataforma de Facebook y utilizado los recursos de la red para denunciar que esas publicaciones le resultaban lesivas sin obtener respuesta, habiendo enviando cartas documento a la dirección de Facebook Argentina en la CABA sin que fueran recibidas por la empresa.

Incoada la acción, el Juzgado requirió el informe previsto por la ley 25.326 (respondido por la demandada) y constató por Secretaría las publicaciones aludidas. Entendió que era de aplicación la jurisprudencia de la CSJN en "Rodríguez María Belén c/Google Inc s/Daños y Perjuicios" -a partir del momento que la accionada toma conocimiento del supuesto contenido ilícito de un página web, desaparece la "ajenidad" del buscador y se puede generar una responsabilidad por culpa si no los bloquea-, e hizo lugar al habeas data contra Facebook SRL disponiendo la eliminación de los URL y ordenando informe la titularidad de las cuentas, el correo electrónico vinculado, número de IP, fecha, hora y eventualmente desde qué clase de dispositivo electrónico fueron subidos los comentarios y la fotografía.

Esta sentencia fue recurrida por Facebook sosteniendo la falta de legitimación pasiva, indicando que en el país opera Facebook Argentina S.R.L., diferenciándola de Facebook Inc, quien sí tendría facultades para cumplir la manda judicial, pero que se domicilia fuera de la Rca. Argentina

La Cámara rechazó la excepción de la supuesta desvinculación entre ambas sociedades, entendiendo que las actividades de Facebook Argentina S.R.L, -comercialización del servicio y la venta de publicidad- hacen que deba regirse por la legislación local. Y citando precedentes del Tribunal de Justicia de la Unión Europea, (sentencia Lindqvist, C101/ 01, EU:C:2003:596 y COSTEJA y AEPD Vs. Google (C131/ 12), rechazó la supuesta desvinculación entre empresas concluyendo que Facebook Argentina S.R.L. no puede eludir las mandas judiciales alegando que carece de facultades, debiendo cumplir con las resoluciones de los tribunales locales notificadas al domicilio constituido en el país.

El otro aspecto destacable de la sentencia de Cámara refiere el ámbito de la publicación difundida desde Facebook. La Comisión de Géneros se "conforma por estudiantes autoconvocadxs desde julio de 2017, en el marco de una asamblea donde se mocionó la formación de ese espacio de mujeres e identidades disidentes, para constituir un foro de discusión, y un espacio de denuncia a políticas y prácticas, colectivas o individuales, consideradas lesivas a las perspectivas de género", concluyendo que la publicación se hace cargo de un asunto de interés público.

Y lo sostiene por tres razones: a) los sujetos que intervienen; a los que define no como simples estudiantes, sino como militantes sociales de agrupaciones universitarias, con compromiso público-, b) el ámbito en que se discuten los hechos –una Facultad de una Universidad estatal- y c) la temática que involucra -comportamientos lesivos a las perspectivas de género- como cuestiones "que preocupan, importan o interesan a toda la sociedad" ("Fallos" 334:1722, considerando 14°, in re "Melo" con remisión a la Corte Suprema de los Estados Unidos en el caso 'Gertz', 418 US 323, 337), concluyendo "que las manifestaciones de una agrupación que enarbola la defensa de las mujeres e identidades disidentes, denunciando que un militante se involucra en prácticas incompatibles con dichos ideales, debe considerarse un discurso amparado constitucionalmente" Y frente a la situación de duda respecto de si un discurso en materia de género reviste carácter o no de interés público y si debe o no suprimirse, debe ser resuelta en favor de la protección constitucional de ese discurso y de su mantenimiento".Y en consecuencia revoca la sentencia de primera instancia.

En definitiva, ambas sentencias además de involucrar a las tecnologías digitales -aplicaciones como Twitter y empresa Facebook- abordan temáticas similares (violencia de género) y llegan a conclusiones parecidas (discurso de interés público protegido), Una y otra refieren al poder de viralizar la información con una extensión y rapidez desconocidas hace algunas décadas, confirmando un nuevo escenario cada vez más específico en el tema pero a la vez mas extendido por su uso, en el que lxs distintos actorxs (judiciales o no) van aportando saberes, opiniones o reflexiones en una construcción colectiva en plena elaboración.

EL "STALKING". ¿UNA SIMPLE MOLESTIA, UNA CONTRAVENCIÓN O UN DELITO? CUESTIONES PENALES DINÁMICAS DE LA FIGURA

LEONARDO MONTI [1]

EDGARDO VILLORDO [2]

[1] Abog. docente adscripto en Derecho Procesal Penal en la Univ. Nac. de Córdoba y en la Univ Cat. de Córdoba

[2] Abog. Mg. en Desarrollo Humano y en Gobierno y Economía Política Especialista en DDHH y Abog. Digital por la UNAM

Desde hace algunos años y hasta la actualidad se habla cada vez con mayor frecuencia de los denominados ciberdelitos o cibercriminalidad; conceptos estos que sin dudas habrían dejado sin palabras y más aun sin respuestas a los redactores del código penal de 1921. Ahora bien, han pasado más de 90 años de aquella gesta jurídica y si bien es mucho lo que se ha avanzado en el tema no es menos cierto que es mucho el camino que queda por recorrer y si se me permite la expresión, mucha tela por cortar.

Es acertado sostener que el legislador no puede prever situaciones que ocurrirán varias décadas después de la sanción de la norma jurídico penal pero no podemos soslayar que vivimos en una era en la que los avances tecnológicos (sobre todo en lo que se refiere a informática y tecnología digital) va mucho más delante de lo que el legislador en su mente puede imaginar.

A toda esta situación podemos agregar un condimento adicional, el derecho no crea la realidad, ésta es preexistente, aquel solo se encarga de tomar algunos aspectos de ella y convertirlos en una norma jurídica de alcance general.
Pues bien aquí empiezan a florecer algunos conflictos respecto de determinadas conductas que se repiten con bastante frecuencia en la sociedad actual y que pareciera no haber acuerdo respecto de su regulación o ubicación dentro de un cuerpo normativo (entiéndase código de convivencia ciudadana o código penal).

Algunos conceptos previos:
¿De qué hablamos cuando nos referimos a cibercrimen?

Una aproximación interesante nos brinda el manual de recursos de justicia criminal del departamento de justicia de Estados Unidos de Norteamérica donde, en líneas generales, nos dice que se trata de actos ilegales de cualquier tipo en los cuales el conocimiento de la tecnología computacional constituye un factor determinante para que la realización de esos actos sea exitosa,
Es decir, queda claro que quien realiza este tipo de actividades debe tener conocimientos mínimos o muy elevados de informática, según sea el caso, para poder llevar adelante su plan delictivo; y que para lograrlo no se vale de cualquier instrumento sino de dispositivos informáticos, servicios o aplicaciones de internet.

El STALKING

Se trata de un término anglosajón que se traduce como acoso, hostigamiento, acecho, al sujeto activo se lo denomina STALKER.

Se trata ni más ni menos que del popularmente conocido acoso cibernético.

Los primeros en regular esta conducta fueron los estadounidenses en la década el 90, más precisamente en la legislación represiva del estado de California, siendo actualmente un delito federal.
En otro continente y en otro sistema jurídico como es el español, la figura fue introducida en el año 2015 y se establece un sistema de prosecu-

ción de la acción similar al de los delitos de acción pública dependiente de instancia privada (al menos en la figura básica) que rige en nuestro ordenamiento: a instancia de parte o de su representante legal.

Las conductas típicas son básicamente: vigilar, perseguir, buscar la cercanía física, usar indebidamente los datos personales de la víctima, atentar contra su libertad o patrimonio, etc. Todo ello tiene que ser realizado de manera insistente y reiterada y sin estar legítimamente autorizado, el STALKER, a realizar dichas conductas que, además, deben modificar gravemente el desarrollo de la vida cotidiana del sujeto pasivo de la acción.

Las penas conminadas para estas acciones son de prisión (que serían excarcelables en nuestro sistema) o multa, en tanto que cuando la víctima sea una persona que se encuentra en situación de vulnerabilidad por su edad, enfermedad o entre otros casos, la figura se agrava y se aplica pena de prisión de seis meses a dos años.

¿Y por casa cómo andamos?
En nuestro país el STALKING no está tipificado, al menos como delito penal (si hay proyectos).
Lo cierto es que una figura similar a la descripta en el derecho comparado se encuentra receptada en el código de convivencia ciudadana de Córdoba, pero con la particularidad que no es especifica en el sentido de los medios que se pueden utilizar para llevar a cabo la conducta típica.

No obstante ello, la doctrina dominante entiende que la figura tipificada en el código de convivencia provincial puede llevarse a cabo utilizando cualquier medio por lo cual quedarían incluidos los dispositivos informáticos entre los medios comisivos.

El bien jurídico protegido es aquí la libertad de autodeterminación de las personas.

Prescribe el citado código de convivencia:
Artículo 65.- Hostigamiento. Maltrato. Intimidación. Serán sancionados con hasta diez (10) días de trabajo comunitario, multa de hasta veinte Unidades de Multa (20 UM) o arresto de hasta treinta (30) días los que intimiden, hostiguen o maltraten física, psíquica o económicamente a otro, siempre que el hecho no constituya delito.

Artículo 66.- Agravante. El máximo de las sanciones previstas en el artículo 65 de este Código se duplicarán cuando: a) El autor o instigador sea la persona sostén de familia; b) La víctima sea persona menor de dieciocho (18) años de edad, mayor de setenta (70) o con necesidades especiales; c) Se cometa por razones de género, o d) El hecho se produjere con el concurso de dos (2) o más personas.

CUESTIONES PENALES DINÁMICAS CON EL DERECHO INFORMÁTICO:
Si bien, el presente artículo a claras luces es analizado como una simple molestia, su dinámica a lo largo del tiempo, entendiendo esto como la persistencia, sin el accionar de las autoridades, ha sido una cuestión que no es menor mencionar. Las derivaciones peligrosas a las que está expuesta la víctima debido al uso de las tecnologías informáticas, tanto redes sociales e internet, muchas veces mutan o se agravan, y el acoso al sujeto pasivo se torna, no ya en una simple molestia sino más bien en un delito de difícil resolución.

En este caso, mencionamos que la Provincia de Córdoba, lo tiene incorporado normativamente como una contravención, lo cual constituye un buen inicio como política de seguridad informática y criminal. Empero, si bien este tipo de comportamiento tiene implicancias directas con cuestiones técnicas informáticas, que por cuestiones de extensión del presente artículo solo haremos mención sucintamente; así tenemos la violencia de género, previsto en la ley 26485 y los tipos penales, que se pueden ver inmiscuidos como violencia; por otro lado, la protección de datos personales previsto en la Ley 25326.

Incluso la conducta desplegada, puede volverse más compleja, volviéndose un tema de carácter internacional, cuando el sujeto activo de la

conducta disvaliosa aquí llamada por medio de un anglicismo STALKING, se encuentra fuera del país, como suele suceder en muchos de estos casos, teniendo que implementarse desde el inicio una estructura de abordaje compleja similar a los tipos penales, entrando ya en vigencia para este tipo de ciber delitos el Convenio de Budapest, y los instrumentos de DDHH, correspondientes; sumado a las otras figuras penales potenciales que pueden interactuar, con esta simple conducta. En este sentido es claro que pueden verse comprometidas, en el caso de pluralidad de sujetos, distintas jurisdicciones nacionales e incluso internacionales.

La conducta desplegada como venimos mencionando más arriba puede comprometer; múltiples bienes jurídicos, por lo que puede pasar de una simple molestia y convertirse en una cuestión pluriofensiva de distintos bienes jurídicos, que exige un accionar eficaz y efectivo por parte de las fuerzas de seguridad preventiva. Ello coloca ya este tipo de accionar, no dentro en la norma contravencional inicialmente mencionada; sino más bien en los tipos penales, que pueden ir desde lesiones a la salud, de la psicología de la víctima por su edad, apariencia, raza, ideología política; utilización dañosa de imágenes personales de la víctima o su entorno familiar, calumnias e injurias tanto a la víctima como a su entorno familiar, o personas allegadas.

Como se puede ver, el derecho informático, el cual se encuentra cada vez más inserto en nuestras vidas, y su abordaje, exige por sobre todas las cosas, educación. No decimos nada nuevo menciono, si ponemos de manifiesto que las conductas disvaliosas informáticas, son cada vez más propensas a cometerse desde el ámbito internacional por medio de personas en distintas partes del mundo.

Por otro lado la cuestión de los menores en la red, es un tema que debemos regular debidamente para que quienes usen las redes sociales, estén debidamente capacitadas para usarlas, tengan una edad que les permita comprender el daño que se puede hacer con una viralización de imágenes, videos o frases desafortunadas de personas adultas o niños, o de personas discapacitadas o de personas de cierta edad quienes pueden ser más vulnerables, y exigen una revisión de la posibilidad de publicación por parte de dichas personas, bajo la exclusiva responsabilidad de quien lo hace, o su tutor, o progenitor, debemos empezar a anular en mi humilde criterio la posibilidad de las formas culposas o mejor aún incluirlas en estas cuestiones informáticas.

Que además de la educación como elemento preventivo para su tratamiento, exigen otro abordaje más dinámico por parte del Estado en estas cuestiones para su correcta regulación. Sobre todo, lo que tiene que ver, con cuestiones de niñas niños y adolescente, “porno venganza”, y otras situaciones de violencia en la red; ni que hablar de la cifra negra en los delitos informáticos, todo en un contexto donde, conceptos como intimidad y privacidad tiene una mutabilidad dinámica que excede el presente artículo; que son una materia aparte de la cual, en entregas futuras, tendremos el gusto de analizar con mi colega DR. LEONARDO MONTI, con el cual tengo el honor de articular estas palabras.