LICENCIATURA EN GESTIÓN DE LA TECNOLOGÍA

LEGISLACIÓN APLICADA A LA TECNOLOGÍA

UNIDAD 2 – DERECHO INFORMÁTICO

a) Ramas del derecho. Relación de la informática con el derecho.

b) La informática jurídica. Historia del software en el derecho

c) Derecho Informático. Antecedentes históricos y evolución conceptual. Objeto de estudio. Características, elementos y notas distintivas. El mundo virtual y los principios jurídicos aplicables. Fuentes del derecho informático.

d) Documento electrónico y la firma digital. Concepto y nociones del documento electrónico. Caracteres: Integridad, inalterabilidad y perdurabilidad.

e) Derecho a la intimidad. Diferencia con el derecho a la privacidad. Normativa aplicable a la protección a la intimidad. Protección de los datos personales. Relación con el derecho informático.

RAMAS DEL DERECHO

El Derecho tiene múltiples ramas que han ido ganando protagonismo y autonomía a lo largo del tiempo, autonomía académica y práctica, contando con su propia normativa exclusiva, sus propios fueros (tribunales o juzgados) especializados.

El Derecho Positivo se divide en dos grandes ramas: el derecho público y el derecho privado.

Nos encontramos ante el derecho público cuando el régimen normativo prevé la intervención del Estado como poder público, es decir, actuando en la situación de supremacía que le confiere ese carácter. Se dice, en estos casos, que existe un interés estatal directamente comprometido. Son ramas a su vez del derecho público, el derecho penal, el derecho constitucional, el derecho administrativo, el derecho internacional público, el derecho procesal.

El derecho privado, en cambio, comprende las normas en que las relaciones entre las partes son reguladas sin conceder a una de ellas una supremacía como la vista anteriormente. Rige las relaciones entre particulares, tratados en un pie de igualdad.

La principal rama del derecho privado es el derecho civil, que funciona como el tronco común del cual, con el tiempo, se han separado las otras ramas que hoy integran el derecho privado, como el derecho comercial o el derecho agrario; y otras, como el derecho laboral que, en su constante evolución, se ha desprendido de su encasillamiento primario de rama del derecho privado.

RELACIÓN DE LA INFORMÁTICA CON EL DERECHO

La informática desde su nacimiento ha ido evolucionando, abarcando muchísimos aspectos de la vida humana en sociedad. Como vimos previamente, la norma siempre es posterior a la conducta humana para lograr su eficiencia en

cuanto a su cumplimiento y aplicación. Caso contrario, intentar forzar a la sociedad a adaptarse bruscamente a una conducta determinada, lleva a un tiempo de infracción sistemática.

Hoy en día la informática abarca muchos campos del derecho, puede servir en el marco del Derecho Comercial dado que podemos contratar sobre objetos relativos a la tecnología, o por vías electrónicas dependientes de la informática; en el ámbito Civil, puede verse involucrado en cuestiones relativas a la información de bases de datos de las personas, como así también por ejemplo en lo referente a los derechos de autoría y propiedad intelectual; en el campo del Derecho Laboral, puede ser objeto del inicio o extinción de la relación laboral; en el ámbito del Derecho Penal, pueden cometerse delitos cuyo tipo objetivo se configura específicamente mediante vía informática.

Es por ello que no se puede extirpar la informática de todos estos campos, para ser regulada en forma autónoma, sino que debe complementarse con el resto del plexo normativo.

LA INFORMÁTICA JURÍDICA

Se denomina Informática Jurídica a la aplicación de las tecnologías informáticas al servicio del mundo del derecho, por ejemplo, un sistema informático para la gestión de expedientes judiciales, o la administración de casos de un Estudio Jurídico; como asimismo la creación de bases de datos y búsqueda de normativas o fallos.

Una primera forma de entender la relación entre el derecho y las tecnologías de la información es interpretarla como la aplicación de instrumentos tecnológicos a las operaciones que realizan quienes actúan en el ámbito del derecho (abogados, jueces, peritos, etc.).

A esta concepción de la informática como herramienta utilizada por los "operadores del derecho" se la llama usualmente con el nombre de Informática Jurídica.

Por contraposición, se denomina Derecho Informático a la universalidad de problemas que surgen de las transformaciones que el derecho ha ido realizando como imposición de ciertas actividades novedosas que se desarrollan en el ámbito social y que requieren nuevas regulaciones o una reinterpretación de las regulaciones ya existentes a fin de dar respuestas en el sentido de la justicia.

Áreas de la Informática Jurídica:

- La Informática Jurídica de Gestión es la aplicación de la informática a las tarcas cotidianas de abogados, jueces, peritos, etc. a través del uso de computadoras y programas para realizar tareas de procesamiento de textos, de almacenamiento de datos, para efectuar comunicaciones mediante redes, etc.
- La Informática Jurídica Documental, por su parte, pretende dar solución a las dificultades en el trabajo de recuperar documentos en amplios repositorios jurídicos. Desde la invención de la escritura, tanto las leyes como las sentencias y los artículos de doctrina se expresan mediante

documentos escritos. En los últimos años, la cantidad de estos documentos jurídicos ha crecido de manera tan elevada que ha hecho imprescindible la utilización de potentes motores de búsqueda.

- La Informática jurídica Decisoria, a su vez, consiste en la aplicación al derecho de técnicas y modelos de inteligencia artificial con el objeto de lograr sistemas expertos que simulen el razonamiento jurídico. Esta disciplina sí tiene en consideración las estructuras lógicas normativas y trabaja a partir de sistemas inferenciales. La mayoría de los proyectos de Inteligencia Artificial aplicada al derecho que se han desarrollado en la Argentina y en el mundo han carecido de continuidad y hoy no existen, lamentablemente, aplicaciones ni estudios de la envergadura que se podría haber esperado.

HISTORIA DEL SOFTWARE EN EL DERECHO

Ante la llegada de la informática a nuestro mundo, con la creación de software, se suscitaron diversos inconvenientes a nivel jurídico, dado que era algo totalmente nuevo.

En el mundo, se intentó ver la forma de dar protección a los programas de algún modo, para evitar que la idea y el trabajo de uno, sea aprovechado por otros sin ninguna repercusión.

Con el desarrollo informático surge la problemática de incluir o no al software dentro de las leyes de derecho de autor. En nuestro país se regula este derecho en el año 1933 mediante ley 11.723, lo que veremos más adelante.

En los países de tradición jurídica angloamericana (common law) el derecho de autor se denomina copyright, literalmente derecho de copia, expresión que alude a la actividad de explotación de la obra por medio de su reproducción.

En tanto que en los de tradición jurídica continental europea (basada en el derecho romano) se tiene una concepción marcadamente personalista de la materia, se ha acuñado la expresión droit d'auteur (derecho de autor) que alude

al sujeto del derecho, al creador, y, en su conjunto, a las facultades que se le reconocen.

En los países de tradición jurídica latina, además de la expresión derecho de autor, también se utilizan las denominaciones propiedad literaria, artística y propiedad intelectual.

En un primer momento, los desarrolladores -ante la falta de normas específicas-, recurrieron a los tribunales exigiendo protección. Para ello, intentaron que el software sea tratado del mismo modo que las patentes de invención.

Ello nos lleva a uno de los primeros precedentes del mundo jurídico, los inventores Gary Benson y Arthur Tabbot crearon un método de conversión de decimales codificados en binario a números binarios puros, para ser utilizado en una computadora. La oficina de patentamientos de EEUU rechazó la aplicación de la patente porque se trataría de una expresión matemática pura, las cuales habían sido desestimadas previamente de ese régimen.

Es por ello que llevaron el caso hasta la instancia más alta en lo administrativo y luego a lo Judicial, llegando a la Corte Suprema de Estados Unidos de Norteamérica en 1972.

El caso Gottschalk v. Benson, la Corte denegó el patentamiento, alegando que la invención no era un “Proceso” en sí, ni estaba limitado al uso de una computadora, o máquina determinada ni para la transformación de materia prima. Se dictaminó que el proceso no era más que un algoritmo, y, por ende, no resultaba patentable.

El impacto del fallo fue contundente, confirmando que el software por sí mismo, no es comprendido en el régimen legal del patentamiento.

Pero a su vez, deja una ventana abierta, el software si puede ser patentado, solo si está destinado al control de una maquinaria para la que fue diseñado, y para la transformación de materia y/o proceso industrial. Ergo, la única ventana

posible para entrar en ese régimen se da en esos supuestos, y en forma conjunta (se patentaría teóricamente la maquinaria y el software como un todo).

Por supuesto no fue el único lugar donde esto mismo fue planteado, pero no recibió acogida favorable en este marco legal.

La cuestión ha sido recepcionada internacionalmente en el Convenio de Berna y por el otro la Convención Universal de Ginebra. El primero de 1886, con sucesivas revisiones hasta el acta de París de 1971, del que la República Argentina es parte. Se trata de una reunión de países para la protección de los autores sobre sus obras literarias y los principios de protección son el trato nacional, independencia de la protección, protección mínima (con reconocimiento de derecho patrimonial y moral, obras protegidas, plazo de protección, duración de los derechos) y ausencia de formalidades.

El origen de este Convenio lo encontramos en 1878, que a instancias de la Sociéte des Gens de Lettres, se celebró París un Congreso literario internacional presidido por Victor Hugo; en su transcurso se constituyó la Asociación Literaria Internacional que, en 1884, se abrió también a los artistas e incluyó en su nombre la palabra artística y desde entonces es conocida por su sigla ALAI.

En Europa, se celebró el Convenio sobre la Patente Europea en 1973, donde definitivamente deja en claro la imposibilidad de patentar ideas, métodos, modelos de negocios, teorías, ni descubrimientos.

En su artículo 52, la Convención de Múnich dice: “Invenciones patentables...1. Las patentes europeas se concederán para cualquier invención en todos los ámbitos tecnológicos, a condición de que sea nueva, que suponga una actividad inventiva y que sea susceptible de aplicación industrial...2. No se considerarán invenciones a los efectos del párrafo 1, en particular:...a) los descubrimientos, las teorías científicas y los métodos matemáticos;...b) las creaciones estéticas;...c) los planes, principios y métodos para el ejercicio de actividades

intelectuales, en materia de juegos o en el campo de las actividades económicas, así como los programas de ordenador;...d) las presentaciones de informaciones...3. Lo dispuesto en el párrafo 2 excluye la patentabilidad de los elementos enumerados en el mismo solamente en la medida de que la solicitud de patente europea o la patente europea no se refiera más que a uno de esos elementos considerado como tal.”

EL DERECHO INFORMÁTICO

El término derecho informático se menciona por primera vez en los años ´70, en Alemania, por el profesor Steinmüller. Lloverás considera que: “El derecho informático revolucionó las ciencias jurídicas, puesto que luego de la configuración de la llamada sociedad de la información todas sus áreas de estudio se han visto afectadas. Ha cambiado estructuralmente los procesos sociales, políticos y jurídicos, no tanto ya como una nueva rama sino como una transformación.”

Guastavino enseña que: “El derecho informático es el tratamiento sistemático y normativo tendiente a regular la informática en sus múltiples aplicaciones”.

El jurista mexicano Téllez Valdés, si bien también lo define como una rama de las ciencias jurídicas, realiza una distinción que se considera fundamental, entre aquélla que contempla a la informática como instrumento (informática jurídica) y aquélla que la considera como objeto de estudio (derecho informático).

Fernandez Delpech lo define como: “El conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el derecho y la informática. La informática es una ciencia que estudia métodos, proceso y técnicas, con el fin de almacenar, procesar y transmitir informaciones y datos en formato digital”.

Podemos decir entonces que el Derecho Informático es la rama del derecho encargada del estudio de todo aquello inherente a la aplicación de tecnologías informáticas, como asimismo sus consecuencias en la sociedad. O sea, es todo aquello en el mundo del derecho, que se encarga de regular los aspectos de la informática en relación a la humanidad. Existen diversas normas que contemplan los medios digitales, electrónicos, tecnológicos, sus efectos, sus regulaciones, y demás circunstancias, las cuales iremos viendo a lo largo del programa.

También se lo nombra o reconoce como derecho telemático, de las nuevas tecnologías, de las sociedades de la información, ius-cibernética, tecnológico, del ciberespacio, de internet, etc.

El Dr. Tato (Abogado, Presidente de Mensa Argentina (Entidad de Alto IQ), Miembro Titular de la Comisión de Derecho Informático del Colegio Público de Abogados de la Capital Federal (CPACF); Director de la Sociedad Científica Argentina), define al derecho informático como el conjunto de principios y normas que regulan los efectos jurídicos nacidos de la relación de sujetos en el ámbito informático y sus derivaciones, especialmente en el área denominada tecnología de la información.

Para tal especialista, la noción de derecho informático va unida significativamente a dos conceptos vinculados: Tecnología de la información y sociedad de la información. Así entonces el primero, como concepto sociológico, define a la utilización de múltiples medios para almacenar, procesar y difundir todo tipo de información, generalmente a través de computadoras y otros dispositivos electrónicos; mientras que el segundo, es la denominación dada a la sociedad actual, que ha reemplazado a la sociedad industrial; y en la cual la creación, distribución y manipulación de la información forman parte importante de las actividades culturales y económicas, convirtiéndose sin lugar a dudas en bienes intangibles altamente valorados.

A modo sintético se puede llegar a la conclusión de que el derecho informático es una rama del derecho autónoma e incipiente del derecho, que, como conjunto de normas y principios, estudia la interrelación entre los sujetos llevadas a cabo por el uso de medios informáticos y digitales y sus consecuencias jurídicas.

Aun coincidiendo en su totalidad con las definiciones aportadas por los distintos autores resulta indispensable agregar que el derecho informático encuentra sus fuentes en el dinámico cambio propio del ámbito tecnológico, y que, la evolución de su objeto de estudio y método depende entonces, de las consecuencias del uso de las nuevas tecnologías por parte de las sociedades y sus avances.

ANTECEDENTES HISTÓRICOS Y EVOLUCIÓN CONCEPTUAL.

Como se ha desarrollado, el derecho informático es una rama incipiente en el rico universo jurídico, cuyo origen, está relacionado al mismo nacimiento de la computadora y la informática.

En Europa, entre 1960 y 1970, a nombre de derecho y cibernética, se inicial el uso de aplicaciones informáticas en ámbitos legales, tanto regulando derechos personales como en campos de investigación. El investigador célebre Mario Lasono en 1968 propone sustituir por iuscibernética el término de jurimetria, para luego acuñarse el término derecho informático como se mencionó con anterioridad en Alemania en 1970 por el profesor Steinmüller.

En el año 1996 se crea la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre comercio electrónico, uno de los mayores esfuerzos jurídicos internacionales para la regulación del incipiente comercio electrónico o e-commerce, como una propuesta a los estados parte para fortalecer la legislación sobre medios informáticos. En este documento se manifiesta la importancia y necesidad de la existencia del derecho informático en el mundo contemporáneo.

Así es como en los últimos años, cobra difusión el concepto de sociedad de la información y su promoción creciente en el ámbito público, que refiere, a la aplicación de cuestiones derivadas de innovaciones tecnológicas productoras de un cambio en el modelo económico, político, social y jurídico legal, como un ciclo de evolución humana, con características claramente diferenciadoras de cualquier otro estadio de la cultura universal.

El auge de la sociedad de la información se halla ligado al nacimiento de las Tecnologías de la Información y las Comunicaciones (TICs) que actúan sobre la mayor parte de los procesos técnico-económicos. Como consecuencia de esto y del desarrollo de redes, se produce la acumulación de cantidades de información da fácil acceso, que desencadena una serie de transformaciones culturales,

sociales y culturales que conducen a la sociedad de la información a cobrar formas y características propias.

A fines del Siglo XX, surge un medio comunicacional que une de manera innovadora a las personas de todas partes del mundo, que desafía fronteras, tiempo y espacio, libre y con una fuerte voluntad de autorregulación: El Internet, cuyo nombre proviene de la acepción traducida al español de redes interconectadas que, trata de la conexión de millones de computadoras entre sí a una red mundial y descentralizada, que provoca un sustancial cambio en la sociedad y su manera de vincularse.

Ligado a ese fenómeno aparece el de Globalización o Mundialización, que refiere a un proceso económico, tecnológico, social y cultural a escala planetaria consistente en la creciente intercomunicación e interdependencia entre los distintos países del mundo, sus mercados y culturas. Uno de sus principales efectos es la ampliación de consolidadas cadenas de distribución, poniendo al alcance de la sociedad bienes locales y extranjeros, al igual que la digitalización, reconocida como la forma de conversión de información análoga o de soporte físico aun universal estándar digital que puede ser procesado por computadoras y otros dispositivos informáticos y transmitido por innovadoras redes de comunicación.

El mundo virtual existente en internet es donde se permite la comunicación por medio de una gran red denominada World Wide Web desde lugares remotos en tiempo real entre los interlocutores, por medio de las modalidades propias a su funcionamiento.

Esto puede describirse como la creación de una página web, que contiene un nombre específico aprobado por el organismo ICANN (Internet Corporation for Assigned Names and Numbers), fundado en 1998 dependiente de normas del Estado de California en los Estados Unidos, que tiene a cargo la administración y gestión del Sistema de Registro de Nombres de Dominio.

En la República Argentina se encuentra a cargo de NIC Argentina la registración y administración de nombres de dominio.

En la red, la mayor parte de los que ingresan son en realidad proveedores de información, ya sea profesionales o no. Este servicio que brinda el acceso a Internet puede prestarse de manera gratuita u onerosa, desarrollando amplios vínculos jurídicos entre usuarios y proveedores, con las consecuencias que ello deriva.

En lo que respecta a Facebook, consiste en un sitio web, en sus orígenes destinados a relaciones virtuales y vínculos sociales entre estudiantes de la Universidad de Harvard, que en la actualidad se ha extendido a nivel mundial a todo tipo de individuos, empresas y organismos públicos y privados de cualquier tipo, en donde sólo se pide como requisito el ingreso de un usuario, contraseña y dirección de correo electrónico para abrir una cuenta en esta red social. A estas aplicaciones informáticas se las denomina redes sociales por su amplia capacidad de unir a un impensado número de personas que interactúan a lo largo y ancho del mundo virtual desde cualquier punto aleatorio del planeta.

Esta red social, al igual que Twitter, Instagram y un sinnúmero de aplicaciones más, que operadas en el sistema de un dispositivo tecnológico permiten la interrelación de los sujetos, generando nuevos conflictos y responsabilidades derivadas en materia civil y penal, como el ciberbullyng, el acoso en la web (ciberacoso o grooming) abordados por el derecho penal conforme su normativa vigente, se analizara en las siguientes unidades.

OBJETO DE ESTUDIO.

De manera simple y didáctica el Dr. Guastavino, considera que el objeto de estudio del derecho informático son los denominados hechos informáticos, es decir, aquellos actos jurídicos llevados a cabo o ejecutados mediante todo tipo de dispositivos informáticos.

Luego, para otros autores, como el Dr. Tato, el derecho informático si bien tiene un objeto de estudio propio, no lo es de manera exclusiva. Esto se debe a que muchos de los aspectos que abarca son abordados por el derecho penal, civil y comercial, por la falta de legislación específica que contemple los caracteres que la sociedad de la información implica. Es decir que, la falta de plena autonomía en su objeto obedece más a la ausencia de legislación específica que a la falta de autonomía per se.

El estudio de esta nueva clase de conflictos debe abordarse desde una perspectiva multidisciplinaria adoleciendo las áreas tradicionales del derecho de serias limitaciones respecto de la extensión de los casos, evidenciándose la falta de una legislación específica que contemple sus particularidades, por esto es que varios países han estado en los últimos años, legislando sobre ello.

Se considera notable y ampliamente superadora la visión aportada por Tato, ya que, si bien el derecho informático tiene un objeto propio, en los términos de Guastavino, este no se agota en los hechos informáticos. Ello porque el derecho forma parte de un todo homogéneo y cada una de sus partes o subdivisiones aportan distintas soluciones a los más diversos conflictos judiciales. Sin embargo, se destaca la necesidad de que leyes especiales y particulares, que, si serán objeto específico del derecho informático, brinden las soluciones concretas a las que las demás ramas jurídicas no logran abordar.

CARACTERÍSTICAS, ELEMENTOS Y NOTAS DISTINTIVAS.

En términos generales, se expuso que el derecho informático supone un conjunto de normas que regulan los actos jurídicos generados a partir del uso de la computadora y toda clase de herramientas informáticas; y por ser una rama del derecho joven, novedosa y esencialmente dinámica, su regulación y fuentes normativas se encuentran dispersas en diversas legislaciones.

La mayoría de la doctrina actual, incluyendo a Zamora, acepta su existencia,

como nueva rama autónoma del derecho y no discute su relevancia, planteando también una división entre el derecho informático puro (cuyos elementos no tienen paralelo con otra rama del derecho y requiere del elemento tecnológico-informático) y el derecho informático impuro (cuyos elementos tienen puntos de contacto con otras ramas del derecho y le son aplicables sus normativas),

Para finalizar, ha de tenerse en cuenta el traspaso de los límites que separan a los países y sus fronteras por parte de los usos de estas herramientas informáticas novedosas que permiten una intercomunicación en tiempo real y de manera instantánea.

Por este motivo, el derecho informático debe concebirse como un derecho de carácter supranacional, para así lograr soluciones concretas y efectivas de acuerdo a su capacidad de hacer frente a los conflictos que se sucedan a nivel mundial.

EL MUNDO VIRTUAL Y LOS PRINCIPIOS JURÍDICOS APLICABLES.

Existe un mundo digital, un nuevo modo de pensar, una nueva realidad, que sigue paradigmas digitales. Ejemplo de ello es la regulación de Internet y la tecnología digital por el derecho requiriendo la aplicación de principios generales, por su flexibilidad, aptos para resolver conflictos, legislar o sustanciar acciones judiciales.

La doctrina mayoritaria y fallos judiciales de diversos magistrados a nivel mundial consideran de manera muy acertada que ciertos principios generales del derecho resultan aplicables al mundo virtual, en virtud de la indubitable ausencia de una regulación específica en la materia, a saber:

- Principio de libertad de expresión en Internet. Es uno de los más importantes, referido al espacio público y privado, a la eventual responsabilidad de proveedores de información, intermediarios y en general, la libertad de publicar cualquier contenido en la web. Esto

significa que cualquier persona tiene el derecho de hacer público y acceder a cualquier tipo de información por los medios de conexión con la red, con los límites de razonabilidad que la ley impone al ejercicio de todos los derechos y libertades personales.

- Libertad de Comercio. La normativa nacional e internacional propicia la noción de libertad de mercado y convención de los particulares, lo que implica la autorregulación de las partes, con mínima intervención estatal limitada al control de funcionamiento, aplicable al comercio, negocios y contratos electrónicos.
- Principio de No Discriminación del Medio Digital. Se refiere a la postura neutral que debe adoptar el estado, en un contexto de libertad de las formas, así como la tendencia a la digitalización de sus procesos, comprometiéndose a no dictar normas que limiten la participación ciudadana por el hecho de cumplimentar el formalismo escrito, afianzando la libertad de las partes e incentivándolas a la adopción de procedimientos de registro, verificación de autoría, de firmas digitales, eliminándose obstáculos basados en requerimientos excesivos de un formalismo ritual ineficiente.
- Principio Protectorio. Establece la protección de la parte más débil de la relación jurídica en cuestión, fomentando el dictado de normas amplias que equiparen las diferencias que existen entre los sujetos, ya sea de índole económica o cognoscitiva, que se acentúa en el mundo informático o economía digital.
- Derecho de Intimidad. Es el opuesto o limitación del principio de libertad de expresión y comercio, razonablemente merituados a la luz de la Constitución Nacional y los Tratados Internacionales, que se relacionan con la preservación de toda persona de sufrir injurias, ataques al derecho de su privacidad o la de su familia, su domicilio o su correspondencia.
- Libertad de Información y Autodeterminación. Se vincula a la privacidad, refiriéndose al registro de datos personales, individualizaciones, categorización de los sujetos y la facultad de cada individuo de disponer

y rectificar datos referentes a su vida privada, como también, su derecho de acceso a todas las bases de datos que los contengan.

- Carácter Internacional. Habiéndose señalado que el Internet es una tecnología masiva mundial, todas las normas receptan el principio de que sus disposiciones deben ser interpretadas conforme los preceptos internacionales vigentes.

FUENTES DEL DERECHO INFORMÁTICO.

El derecho informático es esencialmente multidisciplinar e interdisciplinar dada la diversidad de sus fuentes. De allí que también resulte metodológicamente flexible por su particular y dinámico objeto de estudio que son los hechos informáticos.

Así ha de nutrirse de diversas fuentes: Tratados internacionales en materia de derechos humanos, de carácter comercial, penal o de propiedad intelectual; leyes especiales de derecho público y privado, la costumbre, la doctrina y jurisprudencia.

De esta manera, se ha gestado una especial asignatura del derecho que no solo toma principios generales del derecho civil, sino también comparte normas de protección del consumidor, del derecho comercial y penal.

Además, involucra derechos y garantías constitucionales como la privacidad, la intimidad, el honor de las personas, el derecho a la libertad de expresión y de ejercer toda industria lícita, siendo esta interdisciplinariedad un rasgo característico que la define y caracteriza como tal.

DOCUMENTO ELECTRÓNICO Y LA FIRMA DIGITAL.

El documento electrónico aparece entre las múltiples y variadas aplicaciones o herramientas que la informática ofrece a las personas. Su regulación por parte del derecho resulta, en consecuencia, de una necesidad propia de nuestros tiempos.

Basanta explica: “La utilización de la informática se evidencia tanto en el ámbito privado como público y de la justicia; los particulares, se comunican cada vez más por correo electrónico y los estados aprovechan estas nuevas redes para facilitar el acceso de los ciudadanos a la realización de todo tipo de tramitación de impuestos y documentos por medios digitales. El impacto que éste produce en nuestras vidas y en definitiva en las relaciones jurídicas, nos enfrenta a la necesidad de revisar nuestra legislación, más concretamente nuestro código civil y dictar las normas complementarias necesarias, para dar una respuesta eficaz ante los cambios introducidos por estas nuevas tecnologías. Se hace necesario así analizar conceptos tales como: documento electrónico, la firma digital y hacer especial referencia a la validez probatoria de los mismos.”

En primer lugar, corresponde describir la forma que hace a la existencia de un documento, para luego, particularizar en el documento electrónico.

Echandía, desde un aspecto procesal explica que “el documento es toda cosa objeto de representación, es decir todo aquello que sirve de prueba histórica indirectamente de cualquier hecho.”

Por su parte, Lorenzetti, afirma que “el documento consta de dos elementos: La capacidad de incorporar y trasmitir una declaración de voluntad, y el soporte, es decir una cosa, corporal como el papel, o incorporal o electrónico o digital, en relación al universo virtual.”

Llambías, sostiene que “la forma de un documento jurídico es la medida, el modo en que el sujeto se relaciona con el objeto, es decir, es la exteriorización de la voluntad del sujeto relacionado al fin jurídico.”

En otras palabras, la forma es lo que otorga visibilidad a la manifestación de voluntad del autor del documento. En ciertos casos, se debe cumplir con los requisitos establecidos por ley para que el acto tenga validez. Se trata del principio de legalidad de las formas, que consiste en la necesidad de una forma esencial o solemne para el nacimiento efectivo de derechos y obligaciones.

Salvat agrega que la prueba, es la demostración de la verdad de un hecho por alguno de los medios que la ley establece, del que depende la existencia o no de un derecho. Mientras la forma, al ser esencial, debe existir al tiempo de ser celebrado el acto, la prueba podrá existir en ese momento o a posteriori.

Así, un acto jurídico puede existir dada su forma, aunque, puede no ser probado.

CONCEPTO Y NOCIONES DEL DOCUMENTO ELECTRÓNICO.

Lloverás considera que el documento electrónico, pertenece al género del documento en sentido estricto, puesto que éste no exige el escrito como forma ni el papel como soporte para existir ni para el reconocimiento de su valor probatorio.

Sin embargo, tanto en la República Argentina como en el derecho comparado no existe acuerdo acerca del valor probatorio, concepto ni denominación de este tipo de documentos.

Así, existen discrepancias en la doctrina especializada en la noción de documento electrónico. A modo de síntesis, se expone a continuación las principales tres posiciones al respecto:

- Según Giannantonio, debe entenderse por documento electrónico: “Información dentro de soporte electrónico o magnético, es decir que este documento es aquél que luego de ingresar información a una CPU termina conservado en su memoria o en un soporte magnético. El documento en

estos casos es accesible al conocimiento humano o de las personas con la ayuda de un sistema informatizado como una computadora"

- Un segundo grupo de juristas considera que el documento electrónico es aquel producido por todo elemento informático o tecnológico. La información que contiene el documento puede ser conocida de manera directa por el hombre sin necesidad de la computadora. Se trata, de documentos emitidos a través de algún dispositivo de salida, sobre soporte papel, una imagen en el monitor o visor óptico, entre otros. Lo esencial en esta concepción es que la información que contiene puede ser leída y es perceptible por el hombre sin necesidad de intervención de la computadora.
- Por último, una tercera posición, considera al documento electrónico como el continente de un acto jurídico alojado en la memoria de la computadora y producidos por este sistema informático a través de distintos dispositivos de salida de información. Esta postura lo entiende tanto como el contenido en soporte magnético que registran hechos o negocios jurídicos, como los documentos que se encuentren sobre soportes tradicionales, pero cuyo origen sea la memoria ya se trate de un documento impreso, del lector óptico o de una imagen en el monitor. Este grupo de juristas entiende que al igual que en los instrumentos públicos podemos distinguir entre documento original, que es el registrado en la memoria y las diferentes copias que pueden obtenerse a través de los periféricos de salida.

Ahora bien, el documento electrónico, como cualquier documento, y a la luz de la doctrina referida también posee dos elementos: Una declaración de voluntad que es incorporada y transmitida; y un soporte electrónico, constituido por bits.

Por ello, mucho antes ya de la vigencia del Nuevo Código Civil y Comercial se admiten dentro del género del documento, y como estos, se distinguen entre los que llevan firma y los no firmados, denominados ahora instrumentos particulares no firmados. La noción de documento escrito con la firma de su autor como único

medio de atribución de la declaración de voluntad, fue ampliado paulatinamente, admitiéndose progresivamente otros modos de instrumentación de los hechos y actos jurídicos en numerosas variantes novedosas como el estampillado, los códigos, el membrete y la firma mecanografiada, que fueron considerados como suficientes para cumplimentar el requisito de la firma en supuestos especiales.

Ahora bien, uno de los puntos más controversiales a la hora de hablar de los documentos electrónicos, su conservación, pues puede desaparecer en un instante y ofrecería, para ciertos juristas, menos seguridades que el escrito. Ello se relaciona de manera íntima con su valor probatorio, aunque no se observan obstáculos para que el juez, dentro de sus facultades, admita estos documentos, subsiste en gran parte de la población mundial reticente a los cambios, la incertidumbre sobre la seguridad de este tipo de instrumentos.

Hay que destacar que, si bien el Nuevo Código Civil y Comercial Unificado los ha incluido en su innovador articulado, para analizar su admisibilidad, el Artículo 288, en su segunda parte, prescribe para los instrumentos obtenidos por medios electrónicos, el requisito de la firma, satisfactorio con la utilización de una firma digital, elemento asegurador, de manera indubitable de la autoría e integridad del instrumento.

Así entonces la norma establece utilización de una firma digital como presupuesto de satisfacción del requisito de la firma de los instrumentos obtenidos por medios electrónicos, con el fin de asegurar indubitablemente su autoría e integridad.

Si bien el artículo no indica ninguna especificación en cuanto a la modalidad de materialización de dicha firma, se considera que, tratándose de una norma general, debe observarse en concordancia con la normativa establecida por la Ley de Firma Digital.

CARACTERES: INTEGRIDAD, INALTERABILIDAD Y PERDURABILIDAD DE LA INFORMACIÓN.

Como se expuso con anterioridad, la cuestión principal que sucinta el análisis del documento electrónico y la información que contiene es la posibilidad de otorgar garantías y seguridades per se que lo hagan gozar a del valor probatorio que requiera la evidencia digital en un proceso judicial.

Según Giannantonio, “La clave para la aceptación de nuevos métodos tecnológicos como soporte de documentos radica en la confiabilidad de los procedimientos con que se realizan. Por ello es conveniente analizar los conceptos de integridad, alterabilidad y perdurabilidad de la información, que son caracteres del documento electrónico, y además considerar cómo estos términos se relacionan con la firma digital, el archivo de la información y las distintas formas de almacenamiento.”

Al respecto enseña Giannantonio que un documento electrónico que merezca considerarse como tal y resultar confiable ha de reunir tres caracteres:

- Integridad: Significa que la información no ha sido modificada o que no carece de ninguna de sus partes. La integridad es imprescindible para otorgar efectos jurídicos a la información firmada, en forma independiente de su almacenamiento.
- Inalterabilidad: Puede extraerse información de ellos, pero no pueden ser modificados. Por tanto, el documento electrónico es seguro si es difícil de alterar. Considerando que la información puede ser alterada, concluimos en que la inalterabilidad no se refiere a la información sino al almacenamiento. La firma digital detecta si se ha producido alguna alteración, pero no la puede impedir. La inalterabilidad del medio de almacenamiento no garantiza la integridad de la información.
- Perdurabilidad: Se refiere a la calidad del lugar de almacenamiento para permanecer en el tiempo, si la información es archivada adecuadamente.

DERECHO A LA INTIMIDAD.

El Diccionario de la lengua española (DRAE) define la intimidad como la “zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia” y la privacidad como el “ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión”.

La intimidad tiene un alcance más restringido, hace referencia a la zona íntima y reservada: el domicilio, las creencias religiosas, las afinidades políticas, las preferencias sexuales, etc. Su protección legal se canaliza a través de los tres primeros párrafos del artículo 18 de la Constitución y de las normas que los desarrollan en aspectos tales como el derecho al honor, a la intimidad personal y la propia imagen, la inviolabilidad de las comunicaciones, etc.

La privacidad tiene un sentido más amplio y de mayor alcance que la intimidad. Se refiere a aspectos de la persona que de forma aislada pueden no tener excesiva relevancia (hobbies, gustos musicales, libros preferidos, películas más vistas, etc.) pero que tomados en su conjunto arrojan un perfil completo del individuo en cuanto a gustos, aficiones, preocupaciones o necesidades, que, sin lugar a dudas, también merecen protección. En este punto los medios de comunicación, la tecnología y la informática permiten cruzar datos y mantenerlos en el tiempo, por lo que se hace necesaria una limitación y reglamentación de su uso.

A ello da respuesta la legislación en materia de tratamiento de la información personal y la protección de datos.

NORMATIVA APLICABLE A LA PROTECCIÓN A LA INTIMIDAD.

En la normativa encontramos distintos referentes, comenzando desde la Constitución Nacional que dice: “Artículo 18.- (...) El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados (...)” “Artículo 19.- Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y

exentas de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.”

Aquí ya nos hace mención la carta magna sobre datos, circunstancias y actos denominados “Privados” brindándoles protección, impidiendo siempre que no afecten a terceros, o al orden y/o moral pública, la intervención del aparato estatal.

En el CCyCN encontramos otras disposiciones al respecto:

“ARTICULO 52.- Afectaciones a la dignidad. La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal, puede reclamar la prevención y reparación de los daños sufridos, conforme a lo dispuesto en el Libro Tercero, Título V, Capítulo 1.” Aquí está protegiendo la lesión a la intimidad personal o familiar, o el menoscabo de su dignidad, utilizando en modo amplio el término “intimidad” siendo éste abarcativo de la privacidad por el contexto de la redacción de la norma.

“ARTICULO 53.- Derecho a la imagen. Para captar o reproducir la imagen o la voz de una persona, de cualquier modo, que se haga, es necesario su consentimiento, excepto en los siguientes casos: a) que la persona participe en actos públicos; b) que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario; c) que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general. En caso de personas fallecidas pueden prestar el consentimiento sus herederos o el designado por el causante en una disposición de última voluntad. Si hay desacuerdo entre herederos de un mismo grado, resuelve el juez. Pasados veinte años desde la muerte, la reproducción no ofensiva es libre.” En este artículo la ley prevé un resguardo incluso de la utilización de la imagen de una persona sin su consentimiento, con algunas excepciones.

“ARTICULO 55.- Disposición de derechos personalísimos. El consentimiento para la disposición de los derechos personalísimos es admitido si no es contrario a la ley, la moral o las buenas costumbres. Este consentimiento no se presume, es de interpretación restrictiva, y libremente revocable.” Aquí nos dice la norma que podemos ceder, comercializar, o sea disponer de nuestros derechos personalísimos, como podrían ser datos íntimos o privados en favor de otros, pero siempre y cuando no sea contra la ley, moral o buenas costumbres. También aclara que no se puede dar por supuesto el consentimiento, sino que, por el contrario, tiene que ser expreso y claro al brindarse, debiéndose en caso de duda entenderse que la persona NO prestó su consentimiento, pudiéndose revocar en todo momento.

En cuanto al Código Penal, podemos mencionar la existencia de dos tipos penales que se relacionan con estos derechos. La violación de domicilio (arts. 151 y ss.) y violación de secretos (arts. 153 a 157).

La Ley de Entidades Financieras 21.526 establece que las mismas no podrán revelar las operaciones que realicen, ni las informaciones que reciban de sus clientes (art. 39).

La jurisprudencia en nuestro país creó todo un precedente sobre este tema en particular. En principio se estableció que el derecho a la privacidad e intimidad, con fundamento en el artículo 19 de la Constitución Nacional, en relación directa con la libertad individual, protege jurídicamente un ámbito de autonomía individual constituido por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, 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 los extraños significan un peligro real o potencial a la intimidad (CSJN, 15-4-93, E. D. 152-569).

Cabe tener presente que hoy en día la información es una propiedad que se compra y se vende, pero ante los traficantes de la intimidad, el derecho protege también la vida privada, el debido proceso libre de todo prejuicio sensacionalista,

el derecho al silencio, a no exhibirse, a hacer el bien sin divulgarse nuestros datos, a mantener bajo resguardo los aspectos más delicados de la intimidad fuera de toda curiosidad, indagación o burla.

PROTECCIÓN DE LOS DATOS PERSONALES. RELACIÓN CON EL DERECHO INFORMÁTICO.

La principal estrella de las normas relativas a la privacidad e intimidad, podríamos decir que es la Ley 25326 de Protección de Datos Personales, la que en su ARTICULO 1° expresa:

"(Objeto). La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas."

Este artículo nos habla de los datos "personales" y de dónde podrían estar incluidos, mencionando en forma genérica "otros medios técnicos" por si a futuro se incorporan nuevas tecnologías que escaparían del alcance de la norma de no dejarlo abierto, el propósito es defender el honor y la "intimidad" de las personas. Cita aquí al artículo 43 tercer párrafo de la Constitución Nacional, que dice: "Artículo 43.- (...) Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el

secreto de las fuentes de información periodística. (...)" Ello en relación al acceso a la información que figura sobre las personas en éstas "bases de datos".

Finalmente expresa que esta protección rige sobre empresas o personas de "existencia ideal", y ratifica la protección a la libertad de expresión defendiendo las fuentes periodísticas. Dentro de las definiciones que da la ley en su artículo 2, interesan más que nada las siguientes:

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

En su artículo 3 esta ley menciona que las bases de datos deben ser lícitas e inscriptas, y no pueden tener una finalidad contraria a la Ley o Moral Pública. Luego de ello, el artículo 4 nos dice que los datos deben ser verídicos -debiendo ser corregidos de ser incorrectos-, y adecuados al propósito de la base de datos (no excesivos).

La recolección de datos obviamente debe ser de modo lícito y no mediante engaños, lo recolectado no puede ser utilizado para otro fin distinto al que le dio origen. Deben ser almacenados para que el titular de los datos pueda consultarlos. Y deben ser destruidos al dejar de ser necesarios.

El artículo 5° de la Ley 25326 de Protección de Datos Personales habla sobre el Consentimiento y expresa:

"1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones deberá figurar en forma expresa y destacada, previa notificación al requerido de

datos, de la información descrita en el artículo 6° de la presente ley. 2. No será necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526."

Aquí en el inciso 1 expresa que el titular de los datos debe dar un consentimiento libre expreso e informado, por escrito (u otro medio, dando pie a nuevas tecnologías), el cual debe figurar expresamente y notificarse al interesado la información del artículo siguiente:

"ARTICULO 6° — (Información). Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos."

La cantidad de información que debe dar quien recopila los datos al titular de los mismos es enorme y detallada, pero como esto es una normativa local, muchas veces las empresas tecnológicas internacionales lo omiten pese a que operan en nuestro país, sea por desconocimiento, o por negligencia.

Nos indica también cuándo NO se necesita el consentimiento y enumera:

- Fuentes de acceso libre y público.
- Cuando sean para el ejercicio del poder del Estado, o por obligación legal.
- Datos muy elementales como nombre, apellido, DNI, domicilio, fecha de nacimiento, CUIL/CUIT y ocupación.
- Datos que se obtienen por un contrato, por motivos científicos o profesionales del titular de los mismos, y sean necesarios para desarrollarlos y cumplirlos.
- Operaciones bancarias e información de sus clientes para casos en que lo requiera el Banco Central, o entidades recaudadoras de impuestos.

En relación a los “datos sensibles” (cuya definición vimos antes) la Ley exige aún más precaución:

“ARTICULO 7° — (Categoría de datos). 1. Ninguna persona puede ser obligada a proporcionar datos sensibles. 2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. 3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros. 4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.”

Nótese que restringe la obligación a brindarlos, cuando muchas veces algunos sistemas tecnológicos actuales nos lo demandan básicamente para continuar su utilización. Tampoco podrían colectarlos salvo razones de “interés general” y autorizadas por ley.

Esta ley también prohíbe un archivo de datos sensibles que puedan ser revelados, salvo el registro de fieles de las religiones, agrupaciones políticas y sindicales. Los datos de antecedentes penales/contravencionales solo se pueden tratar por autoridades públicas.

Luego el art. 8 aclara que los establecimientos médicos SI pueden guardar registro de sus pacientes y sus patologías, algo lógico, pero por si existe alguien que considere que está en violación de la ley al hacerlo, se deja expresa constancia de ello.

El art. 9 nos habla de la responsabilidad del que genera la base de datos y los usuarios de la misma (quienes acceden a dicha base de datos). Éstos tienen que garantizar la seguridad y confidencialidad de la información. Queda prohibido mantener estas bases de datos sin sistemas de seguridad. Obviamente de fallar esto, deberán responder mínimamente en forma pecuniaria.

El art. 10 indica que quienes participaron en la generación de la base de datos, deben mantener secreto de todo aquello que conocieron, aún después de terminar su trabajo. Se puede terminar con el secreto si existe un peligro para la seguridad o salud pública, y mediante la resolución judicial que lo autorice.

El art. 11 nos indica que para entregar o transferir (ceder) la información, esto debe realizarse previo consentimiento del titular de los datos, a quien se le debe explicar a quién se le ceden y con qué fin. Este consentimiento se puede revocar.

También establece excepciones a este requisito cuando:

- Lo diga la ley
- No necesite consentimiento para su recolección (ver art. 5 inc. 2).
- Entre órganos del estado.
- Datos de salud, cuando haya riesgo epidemiológico, preservando la identidad de los pacientes.
- Cuando no se pueda asociar el dato al titular del mismo (datos anónimos).

Aclara que quien recibe estos datos también se vuelve responsable del mismo modo que quien los recabó originariamente. A nivel internacional no se permite transferir datos, siempre que no garanticen seguridad y protección.

Esto no rige para los casos de:

- Colaboración judicial internacional (un prófugo en el extranjero, por ejemplo).
- Datos médicos
- Se realiza por un tratado internacional.
- Transferencias bancarias.
- Lucha contra el crimen organizado, terrorismo, narcotráfico.

A partir del artículo 13 nos indica derechos del titular de los datos. Se puede pedir ver los datos propios sin costo alguno. El encargado de la base de datos tiene 10 días para mostrarlo, caso contrario queda abierta la acción legal de “Habeas Data” o de protección de datos personales.

Se puede pedir al menos cada 6 meses, y pueden hacerlo los sucesores de una persona fallecida.

Debe ser clara la información. Puede pedirse su rectificación (corrección), actualización, o supresión cuando corresponda. Se debe realizar en 5 días, sino se da lugar a la acción de “Habeas Data”.

Existen excepciones por cuestiones de orden público. Posteriormente nos indica la ley cómo se deben registrar las bases de datos y sus titulares.

BASES DE DATOS ESPECIALES

Se aborda el tema de la información con fines de obtención de créditos:

“ARTICULO 26. — (Prestación de servicios de información crediticia). 1. En la prestación de servicios de información crediticia sólo pueden tratarse datos

personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. 2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés. 3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión. 4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho. 5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.”

Solo pueden formarse con datos patrimoniales de los titulares, de fuentes accesibles al público, o facilitadas por el interesado, mediante consentimiento. También puede tener datos de acreedores.

Estos datos se registran UNICAMENTE por los últimos 5 años, y si el deudor cumplió con su obligación solo puede quedarse registrado ese dato por 2 años.

Aclara que estos datos en particular se pueden ceder sin comunicarse al titular, siempre que sean para actividades de crédito/comerciales. El artículo 27 nos habla de los datos con fines de publicidad, y aclara que éstos si son públicos se pueden recabar, para establecer perfiles para publicidad o promocional, o ver hábitos de consumo. Si no son datos públicos el interesado debe prestar su consentimiento. El titular puede acceder a sus datos, y puede pedir que se lo excluya del banco de datos en cualquier momento.

También excluye de estos requisitos a encuestas de opinión, estadísticas, científicas, siempre que sean anónimas o se disocien los titulares de los datos. Sanciones

Finalmente habla de las consecuencias, más allá de los daños y perjuicios, y sanción administrativa por parte del organismo de control, se le aplica al responsable de cualquier infracción una multa de hasta $ 100.000. Incorpora asimismo una figura al Código Penal, en su artículo 117 bis, que penaliza la carga o transmisión de información de bases de datos falsa, agravándose la pena por ocasionar perjuicio a alguien, o por ser un funcionario público quien comete el delito. Incorpora también el art. 157 bis. del Código Penal, que sanciona a quien accede a una base de datos violando su seguridad, asimismo a quien revele la información de la base de datos confidencial cuando debía guardar secreto por ley. Se agrava si se trata de un funcionario público.

ACCIÓN DE PROTECCIÓN DE DATOS PERSONALES “HABEAS DATA”

Ya en el art. 43 de la Constitución Nacional nos dice:

“...Toda persona podrá interponer esta acción (AMPARO) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística…”

Bajo este principio Constitucional, la Ley se adecúa y reglamenta la Acción de “Habeas Data”.

A partir del art. 33 la Ley nos indica cuándo se puede utilizar esta acción judicial para la protección de los datos personales. Y nos indica en qué casos procede:

- Para ver nuestra información que esté cargada en bases de datos.

- Para corregir, actualizar o suprimir datos incorrectos.
- O cuando haya datos prohibidos por ley.

Tramita como una acción de amparo común, aplicando en forma supletoria las normas del procedimiento Civil y Comercial de la Nación. La parte requerida no puede alegar confidencialidad de los datos, salvo para proteger fuentes periodísticas. Los plazos procesales son muy breves dada la importancia del resguardo de los datos de las personas.

USO DE LAS REDES SOCIALES EN EL DERECHO LABORAL

En ciertas ocasiones las redes sociales son utilizadas para obtener información de aspirantes a puestos de trabajo. Se verifican los contactos que tiene o los grupos de los que forma parte el aspirante o candidato.

Esta investigación o recolección de datos, puede ser contraria a algunas normas que protegen la intimidad y privacidad del trabajador. También se puede utilizar esta información con fines discriminatorios.

La normativa nacional nada ha dicho en forma específica sobre estos temas. Sin embargo, es posible aplicar la ley de Protección de Datos Personales, para el caso que éstos han sido recolectados y/o tratados fuera de los límites legales.

En cuanto a la discriminación, la Ley sería aplicable una vez que se inició la relación laboral, y no durante el proceso de selección, pero pese a ello puede encuadrarse esta actividad en el art. 1º de la ley antidiscriminación Nº 23592, el cual dispone que:

"...quien arbitrariamente impida, obstruya, restrinja o de algún modo menoscabe el pleno ejercicio sobre bases igualitarias de los derechos y garantías fundamentales reconocidos en la Constitución nacional, será obligado, a pedido del damnificado, a dejar sin efecto el acto discriminatorio o cesar en su realización y a reparar el daño moral y material ocasionados. A los efectos del presente artículo se considerarán particularmente los actos u omisiones discriminatorios determinados por motivos tales como raza, religión,

nacionalidad, ideología, opinión política o gremial, sexo, posición económica, condición social o caracteres físicos".

También resultaría aplicable la Recomendación General Nº6 "Contra la discriminación en la oferta de empleos" del Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI).

EL USO DE LAS REDES SOCIALES COMO HERRAMIENTA DE TRABAJO FACULTADES DE CONTROL DEL EMPLEADOR

Debe advertirse que, de la utilización de redes sociales -como así de toda otra herramienta informática de comunicación en el trabajo- a instancias del empleador, emerge una indudable facultad de control en favor de éste, debido a que existen diversos intereses que la justifican, a saber:

- Propiedad sobre los medios de producción: el empleador como propietario de las herramientas de trabajo tiene derecho a controlar los bienes de la empresa que dirige. Sostiene al respecto Hocsman que el empleador es titular de los medios de producción, y tanto la computadora, el software como el resto de los elementos que permiten las comunicaciones electrónicas entran en esa categoría. Así, el trabajador dispondría de tales herramientas sólo a efectos de la actividad laboral, y por lo tanto el control sobre ellas se vería justificado.
- Rendimiento del trabajador: la utilización de redes sociales durante el tiempo de trabajo y fuera del uso sugerido por el empleador constituye una forma de esparcimiento que puede insumir tiempo de efectiva prestación de labor del trabajador. Ello, llevado a gran escala, puede generar detrimentos económicos en la empresa, motivados por la pérdida de productividad de los dependientes. El control por parte del empleador adquiere importancia, entonces, a los fines de preservar un ambiente de trabajo eficiente.
- Información confidencial: debe permitirse al empleador el monitoreo de las herramientas informáticas pues siempre existe la posibilidad de que

por medio de las comunicaciones electrónicas pueda facilitarse información confidencial y secretos comerciales de su empresa.

- Seguridad Informática: en la utilización de redes sociales -como en todo servicio de Internet está siempre latente la posibilidad de comprometer la seguridad informática de la empresa a partir de ataques externos, y, por tanto, derivar en la pérdida de información confidencial o relevante para la empresa. - Imagen o reputación: todo aquello que la persona sube en su perfil social, en tanto sea accesible de manera pública, puede repercutir negativa e indirectamente en la reputación de la empresa, violando así el legítimo interés del empleador de resguardar el buen nombre e imagen de su firma. En este sentido se ha dicho que "la ruptura de la escisión entre lo profesional y lo privado conlleva a que actos en principio relativos a la esfera de libertad individual del empleado, como la decisión de colgar fotos, publicar videos, comentar ideas, pensamientos, experiencias, opiniones o críticas puedan tener relevancia no sólo sobre el actor sino también, dependiendo del contenido de las mismas, sobre la imagen y reputación de la empresa, de los otros empleados o de los clientes".
- Responsabilidades legales: el empleador tiene una responsabilidad refleja o indirecta por el hecho de un dependiente, y por tal motivo debe fiscalizar el uso de las redes sociales para evitar conductas de parte del trabajador que puedan afectar cualquiera de los intereses empresariales señalados. En suma, vislumbramos motivos suficientes -muchos de ellos amparados y limitados por normas diversas, como luego veremos- para permitir al empleador el monitoreo o control del uso de las herramientas informáticas de comunicación vía Internet, esto es, correo electrónico, servicios de mensajería instantánea y redes sociales.

CONTROL SOBRE LAS OPINIONES, IMAGEN Y DATOS PERSONALES DEL TRABAJADOR

Un punto controvertido que surge de modo particular en el ámbito de las redes sociales, a diferencia de la problemática de la inspección del correo electrónico, es aquel vinculado con la posibilidad de controlar las opiniones, la imagen y los datos personales que el trabajador publica en sus perfiles. Veremos a continuación estos supuestos:

- Opiniones: es habitual que en las redes sociales, en esa dinámica de permanente interacción que plantean sus funciones y/o aplicaciones, los trabajadores hagan comentarios que puedan afectar intereses del empleador, como ser opiniones contrarias a la persona del principal, de sus superiores o de sus compañeros de trabajo, al lugar o ambiente de trabajo, a los procedimientos utilizados para producir o comercializar bienes o prestar servicios, a la calidad del producto o servicio que ofrece la empresa, etc.
- Imagen: en el ámbito de las comunidades virtuales, es frecuente que una persona publique una fotografía, o simplemente la comparta de manera privada con ciertos contactos, y ésta inmediatamente comience a distribuirse por toda la comunidad de usuarios, llegando a contactos o publicaciones no deseadas por el usuario, o simplemente que su imagen sea publicada sin su autorización (es usual que además de la publicación se identifique a una persona por medio de una "etiqueta", que permite redireccionar a su perfil, sin requerir su consentimiento). Ya remarcamos que, dependiendo del contenido de la foto, video o material que involucre la imagen del trabajador, en muchas ocasiones, puede repercutir en la imagen de la empresa.
- Datos personales: el auge de la utilización de los servicios de redes sociales ha propiciado un nivel de circulación de datos personales que no registra precedentes, no sólo por la enorme cantidad de ellos que fluyen sin control alguno por la red, sino principalmente por el hecho de ser accesibles en forma abierta y global. Entre esos datos, se suelen incluir

como información disponible públicamente el puesto de trabajo que se ocupa, la empresa para la que se presta servicio, los contactos profesionales, y, eventualmente, algún otro tipo de información, e inclusive fotografías, videos, enlaces, y/u otro material adicional o de referencia que hacen a la organización empresarial.

La situación es de difícil solución y podría admitir matices, pues como señalamos con anterioridad, en las redes sociales se desdibujan los límites entre lo profesional y lo personal, entre lo público y lo privado. Existen intereses del empleador que pueden verse afectados, como el derecho a la imagen y reputación de su empresa y el derecho a evitar la publicación de información confidencial, y que, en principio, habilitarían cuanto menos una regulación a nivel de reglamentos de empresa.

Sin embargo, creemos que, por la calidad de los bienes jurídicos en juego - datos personales, libertad de expresión y derecho a la imagen- que se contraponen a aquellos legítimos intereses, en ningún caso -se trate de la utilización de redes sociales a instancias del empleador o se trate de un perfil creado espontáneamente por el trabajador- es admisible prohibición alguna por parte del empleador.

LÍMITES: LIBERTAD DE EXPRESIÓN E INTIMIDAD DEL TRABAJADOR

Veamos ahora cuáles son los límites al derecho a controlar las herramientas informáticas de comunicación vía Internet provistas por el empleador:

a) Derecho a la intimidad: a primera vista, la interferencia más importante se da a nivel de la privacidad del trabajador.

Se plantea así una tensión entre dos derechos constitucionales en juego: el derecho a la intimidad del trabajador y el derecho a la libertad de empresa y de propiedad del empleador. Entendemos que la amplitud del concepto de derecho a la intimidad comprende a la inviolabilidad y privacidad de las comunicaciones,

a la protección de datos personales, al derecho a la imagen, y a cualquier otra injerencia arbitraria sobre la vida íntima del trabajador.

Tal como sostuvimos con anterioridad, el problema del monitoreo de las comunicaciones y la inviolabilidad de la correspondencia del trabajador -en el caso, el derecho a mantener en reserva el contenido de todo aquello que se transmite vía Internet-, es idéntico cuando hablamos de correo electrónico que cuando hablamos de redes sociales.

Sobre aquél, ha sostenido Hocsman que, tanto en el derecho comparado como en la mayoría de los autores de la doctrina nacional se plantea el tema en términos de una disyuntiva, vale decir, que la cuestión debiera ser regulado o bien a favor del empleador, permitiendo en todo caso la vigilancia y acceso a los contenidos de las comunicaciones en el ámbito laboral, o bien en favor del trabajador, prohibiéndose para todos los casos la intromisión en su correspondencia electrónica, pues se afectaría su derecho a la intimidad.

Creemos, no obstante, que la cuestión admite matices, y no debiera ser planteada a modo de antítesis; por el contrario, pensamos que se trata de dos derechos absolutamente compatibles.

Coincidimos con Fernández Delpech en que "se mezclan dos temas que tienen que tener dos soluciones normativas diferentes: la garantía de la confidencialidad del trabajador, y las facultades del empleador con relación a las políticas de uso del correo electrónico y de Internet en el lugar de trabajo".

De esta forma, entendemos que debe distinguirse la posibilidad de establecer políticas de uso de las herramientas de trabajo del acceso a dichos contenidos.

La primera está relacionada con la sugerencia de buenas prácticas, a los fines de resguardar los distintos intereses que dijimos justifican el control del empleador, y, eventualmente, también está vinculada con su facultad disciplinaria. Por otro lado, la confidencialidad del trabajador se refiere a la

garantía de inviolabilidad de las comunicaciones que se cursan por vía electrónica.

Ahora bien, en lo que respecta al control sobre los datos personales y la imagen del trabajador, tema que por cierto se plantea de modo peculiar en las redes sociales, hemos dicho que el empleador no posee potestades de control o reglamentarias sobre dichos contenidos, pues, de permitirse, se estaría avanzando peligrosamente sobre la intimidad del trabajador.

No se trata aquí solamente de la dispensa o renuncia del secreto de las comunicaciones laborales, sino que, además, se encuentran en juego otros derechos: el de autodeterminación informativa y el de disponer de la propia imagen.

Se tratan aquí dos facultades personalísimas que siempre permanecerán en cabeza de su titular de modo irrenunciable. Si bien es cierto que puede consentirse el tratamiento de datos personales, incluso de datos sensibles, o autorizarse el uso de la propia imagen, ello, en modo alguno, significa cederlos a punto tal de ser reemplazados o sustituidos en su ejercicio, cuestión que efectivamente se daría si se permitiese al empleador imponer pautas acerca de qué datos o imágenes publicar, dejar de publicar, o a cuáles de ellas tendrá acceso.

Asimismo, creemos que todo control sobre los datos personales y la imagen no tienen vinculación alguna con el contrato de trabajo o con las prestaciones laborales.

Sea la utilización de redes sociales a instancias del empleador o no, en ambos casos, la conclusión no varía. Si es un perfil estrictamente personal, no hay nada que legitime avanzar sobre su contenido; ahora, si se trata de un perfil "profesional", y se considera una herramienta de trabajo, el mentado derecho de propiedad que corresponde al empleador debe ceder frente a otro derecho de mayor jerarquía, el derecho a la intimidad.

Ello, sin embargo, no obsta a que la utilización de las redes sociales como forma de esparcimiento pueda dar lugar a sanciones disciplinarias por no cumplir adecuadamente con el trabajo durante la jornada laboral.

b) Derecho a la libertad de expresión: también este derecho del trabajador puede colisionar contra aquellos intereses del empleador que justifican el contralor de las herramientas informáticas. Como dijimos, las redes sociales permiten a los usuarios efectuar comentarios y emitir opiniones en pequeños espacios virtuales que hacen las veces de blogs o bitácoras personales -los cuales, en su versión tradicional, han caído en desuso ante la gran versatilidad de las aplicaciones sociales contenidas en una plataforma de red social-, y así afectar legítimos intereses del empleador. Nuevamente aquí debemos concluir como aplicable la misma solución que para los casos anteriores donde se afectan los datos personales y la imagen.

Es decir, prevalecerá el derecho a la libre expresión del trabajador, y, por tanto, no podrá regularse, ni controlar ni acceder a todo aquello que el trabajador libremente opina, sube, comparte y hace en su red social privadamente. Sin embargo, debemos agregar en este punto que, en caso de que efectivamente se utilicen perfiles públicos en las redes sociales para emitir comentarios que afecten intereses de la empresa del empleador (ver. calumnias e injurias dirigidas al jefe o a los compañeros de trabajo), desde luego que surge una responsabilidad ulterior (penal y civil, pero también laboral, pues puede dar lugar a una sanción o a un despido justificado) que debe ser afrontada por el trabajador.

REGULACIÓN EN LA LEGISLACIÓN ARGENTINA

En la República Argentina no existe disposición normativa alguna que regule expresamente las facultades del empleador relativas al monitoreo de las redes sociales, el correo electrónico y demás herramientas informáticas en el ámbito laboral.

No obstante, es menester recordar que la Ley de Contrato de Trabajo 20744 rige las relaciones entre empleadores y trabajadores desde el punto de vista contractual individual, y que, si bien carece de una previsión que se refiera específicamente al supuesto en análisis, creemos que son aplicables sus principios generales.

Como punto de partida, debe tenerse en cuenta que en toda relación laboral debe regir el principio de buena fe recíproca (art. 63 L.C.T.), el cual se extiende no sólo a las conductas a las que las partes expresamente se obligaron en el contrato de trabajo, sino a todos aquellos comportamientos que sean consecuencia del mismo, apreciados con criterio de colaboración y solidaridad (art. 62 L.C.T.). Asimismo, entre las facultades específicas del empleador se encuentran la organización económica y técnica de la empresa como también su dirección (art. 64 y 65 L.C.T.), mientras que entre las obligaciones del trabajador se halla el deber de fidelidad, por el cual debe guardar reserva o secreto de las informaciones a las que tenga acceso (art. 85 L.C.T.).

Finalmente, también resultan de aplicación las disposiciones relativas a controles que el empleador puede efectuar sobre el trabajador, que, si bien no aluden al caso de las comunicaciones electrónicas, sí se refiere a la salvaguarda de los bienes y herramientas de trabajo de propiedad de la empresa (arts. 70, 71 y 72 L.C.T.).

En base a este conjunto de normas, surge con claridad que el empleador tiene un derecho de propiedad sobre los medios de trabajo; las comunicaciones en Internet como herramientas para el cumplimiento de la prestación a la que se comprometió el trabajador, forma parte del concepto de medios de trabajo. Ahora bien, ese derecho de propiedad también implica la facultad de establecer sistemas de control que tengan por objeto salvaguardar los bienes de la empresa, siempre y cuando se respete la dignidad y privacidad del trabajador y se pongan en conocimiento de la autoridad de aplicación, de la organización sindical que represente a los trabajadores, y del propio trabajador. A

su vez, esa potestad de fiscalización del empleador está supeditada a que su ejercicio no resulte violatorio de los derechos del trabajador. Llevado al caso en particular, es correcto afirmar que la facultad de establecer controles sobe los e-mails y demás herramientas de comunicación es legítima en tanto no se afecte la intimidad y libertad de expresión del trabajador.

En relación a lo expuesto, se evidencia que el empleador efectivamente podrá establecer políticas de uso de las herramientas informáticas que provea al trabajador, y también imponer sanciones en base a sus facultades disciplinarias que surgen de los arts. 67 y 68 L.C.T.

Su interés se justifica en su eventual responsabilidad por los hechos de sus dependientes, en que no haya divulgación de información confidencial comercial y/o industrial (el empleador en este caso estará amparado por la ley 24766), y en que no se viole su derecho a exigir lealtad y reserva (arts. 85 y 88 L.C.T.).

Por su parte, encontramos límites al control del empleador, ya no sólo en las propias facultades que confiere la L.C.T., sino principalmente en otras normas tuitivas de la intimidad de cualquier persona, se encuentre o no en relación de dependencia. Debemos citar aquí las previsiones de la Ley de Protección de Datos Personales 25326 en materia de recolección de datos durante la relación laboral, el art. 31 de la ley 11723 relativo al derecho a la imagen del trabajador.

En cuanto a las normas que protegen la libertad de expresión, sería aplicable la ley 26032, que establece que la búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de Internet, se consideran comprendidas dentro de la garantía constitucional que ampara la libertad de expresión (arts. 14 y 75 inc. 22 CN.). De este modo, el trabajador, como todo usuario de Internet, tiene derecho a expresar con toda libertad y sin censura previa sus opiniones en todo tipo de temas: políticos, religiosos, económicos, sociales, culturales, etc., con la única condición de que, si afecta derechos de terceros, tendrá responsabilidad ulterior.

REGULACIÓN A TRAVÉS DE LOS REGLAMENTOS DE EMPRESA

Sosteníamos con anterioridad que es posible compatibilizar los intereses de empleadores y de trabajadores, sin necesariamente contraponer definitivamente las posibles soluciones jurídicas que buscan zanjar el problema del control laboral de las comunicaciones electrónicas. Dijimos también que tanto el derecho de propiedad del empleador y el derecho a la intimidad del trabajador son derechos que permiten ser regulados a través de una política de uso de las herramientas informáticas, la cual debe estar contemplada en un instrumento normativo convencional general: los reglamentos de empresa.

Hoy en día, se estila en la práctica prever reglas de juego claras pero lo suficientemente flexibles y que no vulneren los derechos del trabajador en materia de utilización de Internet, de correo electrónico, y, cada vez más, en materia de redes sociales. Desde luego que tales lineamientos tienen que ser debidamente informados por el empleador y firmados por el trabajador, dando así conformidad a lo que ha leído, o al menos que conoce su existencia. En base a lo expuesto, a continuación, veremos cuáles son las cláusulas que habitualmente se incluyen y cuáles deberían incluirse en un instrumento que regule el uso de las herramientas informáticas de comunicación en general, y de redes sociales en particular:

- Deben especificarse qué herramientas de hardware y software se ponen a disposición del trabajador. En el caso del hardware, deberá hacerse referencia a qué tipo de computadora -PC, notebook, teléfono inteligente, tableta, etc.- y qué dispositivos de entrada y de salida se proveen; en el caso del software, cuáles son los programas operativos y de aplicaciones instalados, y si está permitido o prohibido instalar nuevos programas, actualizaciones y/o complementos o aplicaciones. En su caso, también podrá el empleador reservarse la facultad de instalar programas que impidan el acceso a otros, o, en el caso de Internet, de instalar filtros a ciertas páginas de ocio, entre las que podrán incluirse las redes sociales, ya sea alguna en particular o bien todas.

- Debe hacerse mención de si el uso de programas o sitios web que brindan servicios de mensajería instantánea, correo electrónico, y en general el envío y recepción de mensajes por Internet -u otra red de computación abierta o cerrada- está permitido o no. De estar prohibido, creemos que tal interdicción sólo debe extenderse al lugar y horario de trabajo. Asimismo, debe preverse una excepción cuando el trabajador deba recurrir a estos medios a los fines de realizar comunicaciones urgentes. De admitirse, deben fijarse pautas en cuanto a las condiciones, frecuencia y oportunidad de uso, limitándolas siempre también al ámbito de trabajo. Creemos que resulta útil distinguir entre cuentas laborales o personales, aunque, como vimos, en las redes sociales, al ser plataformas con multiplicidad de funciones, se confunden las fronteras entre lo laboral y lo íntimo.
- El control del contenido de las comunicaciones deberá hacerse por muestreo entre todos los trabajadores y debe ser periódico, excluyendo así todo seguimiento particularizado a un trabajador. Tal acceso debe estar restringido a las cuentas de correo o de redes sociales provistas a instancias del empleador; de tratarse de cuentas personales, en principio, el empleador no tendrá acceso a ellas si no es con el consentimiento expreso del trabajador, quien puede renunciar a su derecho a la confidencialidad.
- Si hay algo que no esté expresamente previsto en este punto, entendemos que el trabajador tiene una expectativa de privacidad que no puede ser vulnerada, por lo cual, el principio de monitoreo admite una importante excepción que surge de la primacía del derecho a la intimidad. En este sentido, creemos que, ante la falta de estipulación entre las partes, es ilícito bajo el prisma de la legislación nacional que el empleador pueda acceder a los contenidos de las comunicaciones personales y laborales del empleado, pues, las comunicaciones por Internet son asimiladas a la correspondencia epistolar en cuanto a su protección constitucional. La única forma para acceder a ellas sería con autorización judicial fundada en ley.

- El empleador, a los fines de garantizar la fidelidad de una eventual prueba informática en juicio, debe procurar que cada computadora o cada cuenta sea accesible sólo por un trabajador, brindando, por ejemplo, una contraseña de ingreso.
- El empleador no debe dar tratamiento a los datos personales -mucho menos aquellos sensibles- de los trabajadores que hubiesen sido obtenidos de un monitoreo del contenido. En todo caso, si el empleador cumpliera con la ley 25326, en particular, con la obligación de registrar sus bases de datos, deberá indicarse al trabajador en cada caso que sus datos serán incluidos en un banco de datos y los fines de dicha recolección, siempre y cuando medie previo consentimiento, y se otorgue la posibilidad de acceder, rectificar, actualizar, suprimir o someter a confidencialidad dichos datos. Cabe aclarar que el principio general que debe mantenerse es que los datos del trabajador obtenidos en esas condiciones no pueden ser utilizados por el empleador.
- El empleador no puede establecer qué datos deben colocarse o no en un perfil de una red social que sea personal del trabajador, sea que se trate de un perfil público o de un perfil privado. Los datos siempre son de propiedad del trabajador, y lo único que excepcionalmente podría autorizarse es un tratamiento en una base de datos del empleador.
- Tampoco podrá limitarse la libertad de expresión del trabajador cuando realiza comentarios u opiniones sobre su ámbito de trabajo. Aquí quizás debiera distinguirse entre el perfil público y privado del trabajador, a los fines de sugerir en el primer caso evitar realizar comentarios que afecten los intereses de la empresa.
- El empleador podrá prohibir la divulgación de informaciones confidenciales de la empresa, procurando hacer saber al trabajador en cada caso qué informaciones deben mantenerse en reserva.
- Por último, puede el empleador, en el ejercicio de sus facultades disciplinarias, establecer sanciones, en tanto sean proporcionadas a la falta o al incumplimiento demostrado por el trabajador, con el alcance de los arts. 67 y 68 L.C.T.