MEMORIA DE GRADO

“DERECHO A LA PRIVACIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES”

MEMORISTA: PEDRO MARIANO HUICHALAF ROA

A mi madre,

por su eterna paciencia y compañía.

Capitulo I Introducción

"Vivimos en una sociedad que depende de la ciencia y la tecnología.
Prácticamente nadie sabe de ciencia y tecnología en esta sociedad"
Carl Sagan

1) Generalidades

Durante la segunda mitad del siglo pasado, la humanidad se ha visto invadida por una serie de cambios tecnológicos inexistentes hasta ese momento. La evolución de las tecnologías informáticas, la alta velocidad en las telecomunicaciones ha posibilitado un nuevo fenómeno social: las nuevas tecnologías de la información y las comunicaciones (TICs) posibilitando el afianzamiento de la sociedad de la información.

Las TICs sólo se pueden entender a partir de la convergencia de tres ámbitos: las telecomunicaciones, la informática o computación y los medios de comunicación de masas.

El surgimiento del concepto de Sociedad de la Información se remonta a los trabajos de Alain TOURAINE (1969) quien en esa fecha ya anunciaba: "La informatización de la sociedad se extenderá con independencia del régimen político y económico de cada país". Pocos podían imaginar cuánta razón tenía.

Se ha dicho por muchos autores que estamos en la "Era Digital" en la que el conocimiento se une a la tecnología para crear herramientas de trabajo en una nueva economía basada en bienes intangibles. Nos encontramos ante una nueva realidad en los procesos comunicativos. La información no tiene condición física ni material tangible.

La digitalización de la información a través de una red informática mundial ha generado un "espacio virtual" o "ciberespacio" como nuevo ámbito de comunicación,

en el cual no hay fronteras para el transporte de la información, sean estos datos, formas o sonidos, no existiendo una regulación específica ni un centro de autoridad integral.[1]

Sin embargo, por la real interacción de las TICs en la vida de las personas, en la comunidad de un sector, en la formación de criterios y nuevas ideas en un país y en el cambio y evolución en las economías, junto al fenómeno de globalización, han hecho surgir la imperiosa necesidad de una regulación jurídica que vaya más allá que una simple ordenación nacional o regional.

En lo referente específicamente al derecho a la privacidad por el uso de estas nuevas Tecnologías de la Información y las Comunicaciones, podemos indicar claramente que la definición legal de lo privado y de los recursos para protegerlo cambian también con el tiempo porque cambian las ideas y cambian las formas de organización, cambia la tecnología con la que se puede vigilar, interferir o asegurar cada ámbito. Hoy hace falta, por ejemplo, legislar con respecto a las telecomunicaciones o al uso de la informática porque hay la posibilidad técnica de proteger, compartir o difundir una masa de información que nunca antes había estado disponible de ese modo. Aspectos de la vida familiar, la sexualidad o la medicina que antes estaban sancionados, como asuntos de interés público, que correspondían incluso al derecho penal, hoy se consideran puramente privados.

El problema de la privacidad es la información: lo que otros saben o pueden saber acerca de nuestra vida. Por eso en los últimos tiempos se han presentado dificultades nuevas, en cuanto el progreso técnico ha modificado de manera radical todo lo que se refiere a la información.

Las nuevas tecnologías ofrecen recursos que hasta hace poco hubieran sido impensables para obtener información, desde el análisis de un código genético hasta la intervención de comunicaciones o el uso de cámaras ocultas; hay también recursos extraordinarios para organizar, clasificar y acumular la información y, por supuesto, hay los medios para difundir todo ello de manera masiva e instantánea. Los riesgos no se le ocultan a nadie.

Muchas instituciones públicas y privadas tienen acceso a información sobre nuestra vida. Es indispensable que la tengan. Las diferentes secretarías de estado, los bancos, los hospitales, las compañías de teléfonos, las aseguradoras, cualquier empresa o cualquier persona con la que firmamos un contrato tiene información nuestra que no

[1] DELPIAZZO Carlos E. “Derecho Informático Uruguayo”, Montevideo, 1995, pp. 54 y ss.

es del dominio público. Pero ninguna institución reúne todos esos datos: sólo bajo algunas condiciones, en determinadas circunstancias y dentro de ciertos límites pueden todas ellas compartir la información o hacerla pública. Nuestro derecho a la intimidad se define en ese terreno.

Comencemos por lo más obvio: el Estado tiene el derecho de reunir información cierta y completa sobre sus ciudadanos y es necesario que lo haga. Es necesario para que se pueda acreditar la identidad de cualquiera, es necesario para cobrar impuestos, para entregar una licencia de manejo, para garantizar el derecho de voto y para muchas otras cosas. Lo más frecuente, en casi todos los estados modernos, es que haya un documento general de identidad, que remite a una base de datos única donde se acumula toda la información personal de las instituciones públicas: estado civil, domicilio, situación fiscal, etcétera; es decir: lo más frecuente es que las dependencias del Estado compartan la información. Entre nosotros no se ha hecho todavía. Cada una de las secretarías de estado, cada oficina de licencias o pasaportes, cada autoridad tiene su propio registro, con la información que ha requerido por su cuenta. No es casualidad: la idea de que se emita un documento nacional de identidad inspira recelos y suspicacias difíciles de vencer.

Lo fundamental es la definición de los límites. Hay información que resulta indispensable para el Estado: identidad, domicilio, estado civil, declaraciones fiscales.

Hay información que no interesa al Estado, que las instituciones públicas están impedidas de solicitar o buscar: creencias religiosas, opiniones políticas, orientación sexual, contenido de la orrespondencia, comunicaciones personales. Para decirlo en una frase, el Estado tiene derecho a reunir información sobre la vida privada de sus ciudadanos, pero exclusivamente en lo indispensable para las funciones públicas. Es decir que puede pedir la información necesaria para la identificación: para el Registro Civil, para entregar pasaportes y credenciales de elector; puede pedir la información que hace falta para la acreditación pública: licencias, permisos, títulos; puede pedir información para asegurar el cumplimiento de las obligaciones fiscales y militares.

Nada de eso supone un atentado contra la intimidad. El Estado no puede requerir, en cambio, ninguna otra información, ninguna que no sea indispensable para cumplir con una función pública reconocida y legítima.

Es del todo distinto el caso de las instituciones privadas. Muchas de ellas tienen información personal de sus empleados, clientes, afiliados y socios. Necesitan tenerla. Con frecuencia, la base de esa información es un documento público para acreditar la

identidad, pero disponen también de muchos otros datos que no figuran en ningún registro público: estado de salud, historia clínica, situación crediticia, aficiones y preferencias, viajes. En general, es la información necesaria para cumplir con algún contrato, del tipo que sea: para adquirir un seguro, por ejemplo, para ingresar a un club, para solicitar un crédito o recibir tratamiento en un hospital; los particulares la entregan a la institución que sea mediante un documento privado, en garantía de confidencialidad, para los fines exclusivos de un contrato. O sea que ni se puede hacer pública ni se puede compartir con otras instituciones, públicas o privadas, salvo en circunstancias excepcionales, previstas de modo explícito por la ley.

Son conocidos los casos de compañías que venden los datos personales de sus clientes, por ejemplo, para que se usen en campañas publicitarias; también sucede que los bancos compartan información entre sí y con otras empresas. Todo ese manejo de datos es ilegal, vulnera la privacidad, a menos que haya el consentimiento expreso de los afectados. Las autoridades públicas, por su parte, pueden solicitar información a cualquier organización privada, pero sólo en los casos establecidos por la ley y, de nuevo, sólo para cumplir con una función pública. Pongamos el caso más obvio: mediante una orden judicial se puede requerir información privada, pero sólo cuando exista la sospecha fundada de que se haya cometido un delito y la información pueda servir directamente para castigarlo.

¿Cómo analizar hoy lo público y los privado bajo el imperio de las nuevas tecnologías y la globalización? La autora argentina Leonor Arfuch propone que, más que un desbalance en la relación entre los conceptos aludidos, hay una imbricación entre ellos[2]. Los medios aparecen como el soporte de visibilidad tanto de lo público como de lo privado, por lo que se constituyen en un tercer espacio en el cual las categorías clásicas se ponen en tensión. El problema radica en la propensión de los medios masivos al formato de la biografía para la divulgación de sus contenidos. La información que circula en los medios de comunicación no constituiría materia de los ámbitos público o privado, sino de uno distinto: el espacio biográfico. Ya no es público, tampoco privado: las dimensiones se interceptan, se superponen, transitan. Hay responsividad: los cambios en un espacio implican también desplazamientos significativos en su contraparte. En definitiva, lo que se verifica es una crisis de los conceptos modernos de público y privado.

[2] Leonor Arfuch. Lo Público y lo Privado en la Escena Contemporánea: Política y Subjetividad. En: Revista de Crítica Cultural, Santiago de Chile, noviembre de 2000, p. 7 y ss.

Ante esto, es evidente el hecho de que también se vuelve imposible el operar con instrumentos que suponen estas distinciones clásicas. Leyes, códigos de ética y distintas normativas que se alimentan de la pretendida distinción clara y dicotómica entre publicidad, privacidad (y también intimidad) se tornan insuficientes para dar cuenta de la realidad heterogénea de registros y circuitos en que se mueven los discursos mediáticos. Surge como un desafío la elaboración de cuerpos normativos efectivos y capaces de reglar una realidad que siempre va dos pasos delante de quienes pretenden regularla.

La situación antes descrita fue, pues, la que nos motivó a desarrollar una memoria de grado relativo a un punto tan específico, sensible y técnico como es el Derecho a la Privacidad y cómo el uso de las Tecnologías de la Información y las Comunicaciones podrían vulnerarlo.

Por muchas razones aceptamos el desafío de analizar específicamente esta area:

- Por un lado la falta de un estudio serio, completo, íntegro y global de los efectos sobre un bien jurídico tan esencial como es el derecho a la privacidad y/o a la intimidad como consecuencia de la aplicación de las TICs.
- Por otro lado la pasión que nos surge al constatar que las TICs están presente ahora, en este momento y evolucionan en forma cada vez más rápida, dejando completamente obsoleto el Derecho clásico.
- Nos motiva además (y aunque suene un contrasentido), la falta de educación en las aulas universitarias sobre el cruce existente entre las TICs y el Derecho, puesto que en la realidad vemos que este tipo de materias NO son enseñadas en la forma requerida en atención a los cambios existentes en la sociedad, su mentalidad y prácticas habituales.
- La actualización de las normas jurídicas, de la legislación y aplicación de las mismas en el ámbito social, requiere además de juristas cada vez mas tecnificados en esta area, siendo pues, nuestra idea que a través de esta memoria, aportemos con nuestra propia experiencia a la formación de operadores jurídicos válidos para el día de hoy.
- El hecho de hablar de un tema tan específico del derecho (como es el derecho a la privacidad), nos obliga satisfactoriamente a hablar de temas tan amplios como la Sociedad de la Información, el Derecho Informático, recursos como el Habeas

Data, Correo Electrónico, etc. Conceptos que cada vez son más comúnmente utilizados en el lenguaje jurídico y coloquial.

Para poder desarrollar esta gran tarea propuesta, hemos desarrollado todo un análisis de la relación existente entre el Derecho a la Privacidad y las Tecnologías de la Información desde distintas areas de estudio. Esta forma de efectuar este trabajo, nos obliga, por un lado a confrontar la realidad jurídica de Chile con la del derecho comparado, además de analizar, criticar y comentar dichas normas. Complementamos al mismo tiempo con mucha doctrina de autores nacionales como extranjeros, puesto que todos tienen una visión común en lo refererido a la Sociedad de la información.

Por tanto, la presente memoria se compone de 10 capítulos en donde hablamos sobre el tema central antes indicado.

En el Capitulo 1, comenzamos con una introducción sobre la memoria, hablando en forma muy amplia sobre la llamada Sociedad de la Información (tema que incluso podría dar pie para la confección de otra memoria). Para efectos de permitir que personas que no tengan mucho conocimiento en el vocabulario técnico de las nuevas Tecnologías, se incluyó un diccionario informático para poder entender los vocablos utilizados.

El capitulo 2 titulado Derecho a la Privacidad delimitaremos los vocablos intimidad y privacidad, con el fin de evitar una confusión que inicialmente se da al utilizar estos conceptos, para quedarnos con nuestra propia postura respecto a privacidad. Se verificará además la normativa relativa a la protección de la privacidad que actualmente existe tanto en el ámbito nacional (ya sea a través de normas de rango constitucional, legal y tratados internacionales) como internacional y que hace referencia a este punto.

El Capítulo 3 sobre el Derecho Informático, y para comenzar de lleno en la memoria, se analiza en forma precisa lo que se entiende por derecho informático. Está de más decir que este tema es muy amplio, tan amplio que se podría realizar otra memoria de grado más en torno a este tema.

Por su parte en el Capítulo 4, se desarrolla completamente la idea de protección de la privacidad por el uso de las tecnologías de la Información, desde un punto de vista civil. Se da una mirada introductoria respecto al tema, se verifica la legislación chilena, se efectúa un análisis con su respectiva crítica, analizamos jurisprudencia actual,

legislación extranjera y analizamos el fenómeno del spam, sobre todo con relación a la última modificación de la Ley de Protección al Consumidor.

El Capítulo 5 hace referencia a la protección penal de la privacidad por el uso de las tecnologías de la información a través del estudio de los llamados Delitos Informáticos y como a través de éstos se infringe la privacidad. Análisis de la ley, jurisprudencia chilena surgida en el nuevo proceso penal vigente en Chile y análisis del derecho comparado para entender la regulación externa.

Con el Capítulo 6 se comentará sobre la Intervención y rol del Estado en las TICs, y viendo específicamente la protección administrativa de la privacidad. Haremos referencia al nuevo Sistema de Registros de ADN y su relación con la privacidad y la cada vez mayor intervención estatal que existe y que vulnera gravemente el derecho a la privacidad de las personas fundándose presumiblemente en aras del bien común.

Por su parte el Capítulo 7, habla de la protección Laboral de la privacidad por el uso de las Tecnologías de la Información. El uso de las Tics en el trabajo, regulación de la misma, verificaremos la Legitimidad del empleador en cuanto al control de los trabajadores por el uso de las Tecnologías de la Información y si es legítimo su despido por este control. Chequearemos que nos dice la legislación nacional al respecto, cual es la doctrina emanada de las Dirección del Trabajo y que nos informa el derecho comparado

El Capítulo 8, tiene como tema central es la privacidad en Internet, la protección de los datos considerando este mundo "sin fronteras", analizaremos si es posible el anonimato en Internet o es una utopía, observaremos un caso real, práctico y cotidiano de violación de la privacidad como es el caso de las coquies y por último investigaremos sobre la ley española en lo relativo al tema, estudiando principalmente un órgano español encargado de la protección de datos.

La idea del Capítulo 9, donde concentraremos anexos de legislación chilena, está dado porque estamos seguros que en un corto tiempo más existirán modificaciones a estas leyes con las que actualmente nos basamos para efectuar todo el análisis antes expuesto, de tal forma que cuando sea leída esta memoria, se entienda acorde a la ley aplicable al momento de su redacción y no a la legislación aplicable al momento de su lectura.

Finalmente el capitulo 10, terminaremos con una reflexión personal en torno al tema y el futuro de las TICs en Chile y el mundo, desde el punto de vista de la

protección de la privacidad por el uso de las Tecnologías de la Información y las Comunicaciones.

2) Sociedad de la Información

En los últimos quince años, y especialmente en la década de los noventa, ha cobrado auge y difusión nacional y mundial el concepto de "Sociedad de la Información" (SI), sobre todo por su gran promoción en el ámbito de las políticas públicas, utilizándose de mejor o de peor manera para referirse, en general, a cualquier cuestión derivada de innovaciones tecnológicas que han devenido en un cambio en el modelo social. Frecuentemente utilizado a propósito de la irrupción de las llamadas Tecnologías de la Información y las Comunicaciones (TIC) y sus consecuencias, tal vez no se ha hecho suficientemente presente su naturaleza social y política, así como el trasfondo jurídico de una etapa en la evolución humana que posee marcadas y diferenciadoras características que la distinguen de cualquier otro estadio de la cultura.

- Sobre la Evolución Social

Como es de todos sabido, existen muchos y dispares criterios a la hora de marcar o señalar hitos en los distintos escalones de progreso del hombre. Así por ejemplo, a la distinción clásica entre historia y prehistoria definida por la invención de la escritura se suman las de carácter religioso, como la venida de Cristo para los cristianos (AC-DC) o la Hégira de Mahoma que determina el calendario de los musulmanes; otros señalan como hitos relevantes las etapas de la evolución de la especie, como la era del Cromagnon o la era del Hombre de Neardenthal, pero existen también como criterios las distinciones occidentales entre edad antigua, media y contemporánea, las referencias a personas o hechos que marcaron una época como "el siglo de Pericles", "el Renacimiento", "el Siglo de Oro español", etc.; es decir, los criterios de diferenciación irán variando de acuerdo a las distintas visiones que se empleen para analizar la historia. Ahora bien, para comprender a que nos referimos con Sociedad de la Información debemos acudir al enfoque que clasifica los modelos sociales de acuerdo a las formas de

producción, es decir, que para entender los modelos debe atenderse en definitiva a los procesos técnico económicos imperantes en cada época, lo que nos conduce necesariamente a revisar uno de los temas cúlmines de la teoría política y económica de Karl Marx, como es la concepción materialista de la historia.[3]

Así, en un muy sintético análisis de la historia de la humanidad occidental, veremos que en sus distintas etapas ha ido cambiando la base de su sistema de producción; la sociedad antigua clásica se sostiene sobre un régimen en que el poder económico reside en quién más esclavos posee, y cuando estos alcanzan la libertad, el poder pasa a quienes poseían la tierra, generándose un sistema de producción en torno a los siervos de la gleba que no poseían terrenos, lo que en general caracterizó a la Sociedad Feudal. Cuando estos escapan a las ciudades, cobra auge el intercambio de bienes, floreciendo una sociedad en que los comerciantes son los que gobiernan, como se refleja en forma directa en Venecia y Florencia e indirectamente en la compra de la Corona Imperial por Carlos V[4]. La acumulación de capitales permite enfrentar proyectos de envergadura como los llevados adelante por las Coronas de Castilla y Portugal, haciendo posible la construcción de los Estados Nacionales. Entonces el poder económico ya no reside en los dueños de la tierra, sino que se ha desplazado a los dueños del capital, quienes para acrecentarlo y gracias a los progresos del siglo de las luces, financian las industrias que producirán los bienes que la Sociedad requiere para el funcionamiento a través de las fórmulas de Ford y Taylor, es decir, de la fabricación en cadena y las cuotas de producción, utilizando gran cantidad de mano de obra no calificada, lo que en definitiva condujo a un modelo social llamado Sociedad Industrial. Y cuando la producción de bienes cede en importancia a la prestación de servicios, surge la Sociedad Postindustrial.

Y aquí llegamos al objeto de nuestro estudio: cuando se logra la automatización de los servicios respecto de un bien inmaterial e ilimitado el sistema económico vuelve a reorganizarse y, por ende, el modelo social sufre una profunda transformación: es el inicio de la Sociedad de la Información.

---

[3] "La tecnología pone al descubierto la relación activa del hombre con la naturaleza, el proceso inmediato de producción de su vida, y, a la vez, sus condiciones sociales de vida y de las representaciones espirituales que de ellas se derivan." Karl Marx, Das Kapital, tomo I.

[4] "Es notoriamente público y claro como el día que Vuestra Majestad Imperial no habría podido sin mí obtener la Corona Romana", según reza la conocida carta del banquero Jacobo Fugger alEmperador Carlos V recordándole sus obligaciones respecto del empréstito que le hiciera para obtener el voto de los Príncipes Electores alemanes.

- En torno al Concepto de Sociedad de la Información

Como cuestión previa debemos destacar suficientemente que la expresión Sociedad de la Información, tal como señala Roncagliolo[5], enraíza más bien en la tradición cultural europea y tiene implicancias y significaciones conceptuales más ricas que la information highways ("autopistas de la información") norteamericana, lo que en el fondo nos revela que Estados Unidos y Europa compiten también en los mercados o áreas de influencia cultural.

Es aquí cuando cobra gran importancia tanto América Latina como Asia, dado que los escenarios de estas incruentas luchas se plantean básicamente en estas zonas del mundo. Ejemplifica el mismo autor esta realidad (aunque sólo refiriéndose a América Latina y no extendiendo el razonamiento a Asia), con otros conceptos en pugna por supremacía, como el europeo transnacionales contra el norteamericano multinationals, telematique (Francia, 1978) versus compunications (Estados Unidos, 1977). También es el caso de teletrabajo y telecommuting ("teledesplazamiento") y otros términos que en definitiva ponen en evidencia que en general las zonas que no pertenecen al primer mundo no han desarrollado nociones y terminologías propias para los nuevos elementos y procesos tecnológicos y sociales, sino que más bien toman partido entre las opciones de las dos más importantes áreas de influencia.

Este punto es mucho más interesante de lo que pudiera parecer, pues los conceptos que adoptemos determinan la forma en que vemos el mundo, es decir, nuestra cosmovisión, y en definitiva será determinante en el proceso de toma de decisiones políticas y económicas relevantes para el mundo con consecuencias prácticas en el día a día: ¿adoptaremos el estándar de TV Digital de EE.UU. o el de la UE?, ¿el voltaje eléctrico será de 110 o de 220 voltios?, ¿estándar de televisión NTSC[6] o PAL[7]?, ¿la

[5] Rafael Roncagliolo. "¿Se Construye Ciudadanía en la Sociedad de la Información?" en Ciudadanos en la Sociedad de la Información. Pontificia Universidad Católica del Perú y The British Council Perú. Lima, 1999

[6] NTSC (National Television System Comitee). Fueel primer sistema de TV color (1953) y las principales características técnicas son: número de líneas= 525, frecuencia vertical= 60 campos/seg, frecuencia horizontal= 15759 Hz., frecuencia de portadora de sonido= portadora de video + 4,5 Mhz y frecuencia de imagen= 30 imágenes/seg. Se utiliza en EE.UU., Japón, Canadá y América Latina (con excepciones)

[7] PAL (Phase Alternation Line). Creado en 1963, sus principales características son: número de líneas= 625, frecuencia de línea= 15625 Hz., frecuencia de campo= 50 campos/segundo, modulación QAM, frecuencia de portadora de sonido= portadora de video + 5,5 Mhz. Este sistema se utiliza en Europa Occidental (excepto en Francia donde se utiliza el estándar SECAM), Medio Oriente y África

normativa nacional exigible en la protección de datos personales será compatible con la legislación norteamericana o con las Directivas europeas?, etc.

- Definiciones

Cuando se aborda el difícil tema de definir lo que es Sociedad de la Información, son recurrentes las opiniones que afirman que se trata de una sociedad en formación en que las nociones de información, comunicación y Nuevas Tecnologías se integran, aunque también es usual que se eluda conceptualizar directamente, dando una explicación en base a las características más notables e indiscutidas, pues no es menos cierto que el trasfondo del asunto es que se trata de un concepto complejo cuyo nivel de desarrollo es incipiente.

De hecho, muchas de las tentativas de conceptuar han devenido en obsolescencia, pero dentro de las que se encuentran vigentes están la de Masuda[8], quien nos dice desde una óptica humanista que se trata de una sociedad "que crece y se desarrolla alrededor de la información y aporta un florecimiento general de la creatividad intelectual humana, en lugar de un aumento del consumo material".

Bastante más descriptiva resulta la definición que da el Libro Verde sobre la Sociedad de la Información en Portugal (1997)[9], que señala que "se refiere a una forma de desarrollo económico y social en el que la adquisición, almacenamiento, procesamiento, evaluación, transmisión, distribución y diseminación de la información con vistas a la creación de conocimiento y a la satisfacción de las necesidades de las personas y de las organizaciones, juega un papel central en la actividad económica, en la creación de riqueza y en la definición de la calidad de vida y las prácticas culturales de los ciudadanos".

Podríamos dar otras muchas definiciones, pero en general son variaciones de las ya señaladas, aunque si es de interés el sello de política pública que tiene el Gobierno Vasco en su Plan para el Desarrollo de la Sociedad de la Información para el Periodo 2000 – 2003, al entenderla como "aquella comunidad que utiliza extensivamente y de forma optimizada las oportunidades que ofrecen las tecnologías de la información y las

[8] Yoneji Masuda. La Sociedad Informatizada como Sociedad Post-Industrial. Editorial Tecnos, 1994
[9] El Libro Verde fue elaborado por la Comisión de la Sociedad de la Información del Ministerio de Ciencias de Portugal y aprobado por el Consejo de Ministros de Portugal en abril de 1997

comunicaciones como medio para el desarrollo personal y profesional de sus ciudadanos miembros".

Como podemos apreciar, cada una de estas conceptualizaciones responden a cosmovisiones diferentes y explican el fenómeno desde una particular perspectiva; y cada una de ellas será más o menos aplicable dependiendo del ámbito específico al cual tratemos de aplicar el concepto.

- Características

El auge de la SI está indisolublemente ligado al florecimiento de las llamadas Nuevas Tecnologías[10] que irrumpieron con fuerza en la década de los 80 y que actúan sobre los procesos técnico-económicos, como es el caso de la nanotecnología, la robótica, la inteligencia artificial, la biotecnología, el láser, las telecomunicaciones, la informática, los superconductores, etc. y en general los avances de la técnica que rompen y cambian la forma tradicional de comprender los conceptos de tiempo y espacio.

Según Aguadero Fernández[11], quien desarrolla latamente las características que posee esta nueva sociedad en su interesante ensayo La Sociedad de la Información, aun cuando pudiera parecer que todas estas tecnologías son de muy variada naturaleza, pues proceden, se aplican y desarrollan en áreas distintas, en realidad son interdependientes, pues su núcleo fundamental es común: máquinas, programas y dispositivos que manejan, procesan y transmiten grandes volúmenes de información.

Consecuencia de lo anterior y del desarrollo de redes, es la capacidad de generar y acumular por todos los componentes del tejido social ingentes cantidades de información con facilidades de acceso en la comunicación de la misma (telemática), lo que desencadena una serie de transformaciones sociales, económicas y culturales que conducen a que la Sociedad de la Información cobre formas y características propias, marcadamente distintas de cualquier otro estadio y, desde luego, diferente a sus antecesora, la sociedad post-industrial.

[10] Lo de "Nuevas Tecnologías" tampoco ha sido una terminología pacífica en atención de que se argumenta que es connatural a la existencia humana la evolución en sus múltiples facetas, entre ellas las tecnológicas, y cada época tiene sus propias innovaciones y la velocidad de los cambios hace que lo "nuevo" de ayer, hoy se encuentre tecnológicamente desfasado

[11] Francisco Aguadero Fernández. La Sociedad de la Información. Acento Editorial, 1997.

- Reestructuración Social y Laboral

Como bien sostiene Aguader Fernández, la tecnología no determina la configuración y el desarrollo de los proceso sociales, pero incide directamente en los aspectos materiales de la realidad, con lo que transforma la estructura y organización social.

Y es así como se incorporan al modelo social nuevas capas determinantes en el progreso del mismo y que antes eran inexistentes: informáticos, biotecnólogos, genetistas, expertos en telecomunicaciones, especialistas en robótica e inteligencia artificial, etc., sumándose además una cohorte de personas y entidades que se incorpora al círculo productivo que rodea estas nuevas especialidades del conocimiento, que van desde científicos y profesores universitarios a técnicos y obreros especializados, sin olvidar a los usuarios de los servicios y tecnologías, que muchas veces ascenderán o descenderán en la estratificación laboral y social dependiendo de sus habilidades y conocimientos en las TIC.

Y este cambio por supuesto que incide en los modos de producción e incluso en la forma de comprender la ética del trabajo. Según Lipovetsky[12] la antigua fórmula "el trabajo fue su vida" ha sido reemplazada por "la vida empieza después del trabajo", con lo que se ejemplifica la profundidad del cambio de la visión, lo que nos lleva a relacionar este asunto con la automatización de los procesos, la reorganización horizontal del trabajo con reducción de puestos intermedios, el aumento de la subcontratación, la división de las grandes empresas en servicios especializados y el redescubrimiento de la importancia del ocio no sólo como actividad de esparcimiento, si no que también como área productiva.

- La Información, Núcleo del Sistema Económico.

En la Sociedad Industrial (y hasta el final de la Postindustrial) el sector económico más relevante era la producción de bienes y la prestación de servicios ligada a estos bienes. Así por ejemplo, en los inicios de los años 70` el más importante de los

[12] Gilles Lipovetsky, El Crepúsculo del Deber. La Ética Indolora de los Tiempos Democráticos. Editorial Anagrama, 1998, citado por Jesús Mercader Uguina en Derecho del Trabajo, Nuevas Tecnologías y Sociedad de la Información, Editorial LexNova, 2002

sectores económicos mundiales era la industria del petróleo, que tiene las características clásicas de los bienes del modelo social anterior: material y limitado[13].

Pero la realidad cambió radicalmente veinte años después y más aún en nuestros días; actualmente el área económica fundamental de los países desarrollados esta constituido por la información, que es inmaterial e ilimitada, y los bienes y servicios relacionados directamente con ella, siendo paradigmático, por ejemplo, la significación de Nokia para Finlandia, Ericsson para Suecia o Deutsche Telekom para Alemania.

Esto implica que la información y las comunicaciones han desplazado en importancia a las demás áreas económicas, pues es claro que quien tiene la información, la tecnología y las habilidades para aprovechar esta conjunción, podrá producir más y en condiciones de mayor ventaja competitiva[14] pues, de acuerdo a CASTELLS, estamos en "una economía en la que el incremento de productividad no depende del incremento cuantitativo de los factores de producción (capital, trabajo, recursos naturales), sino de la aplicación de conocimientos e información a la gestión, producción y distribución, tanto en los procesos como en los productos"[15].

Un aspecto práctico de lo anterior lo constituyen los diarios y revistas con consejos editoriales repartidos en distintos sectores del mundo y que imprimen simultáneamente números con contenidos comunes y otros adaptadas a la realidad local (Le Figaro, Vogue, El País, etc.), las fábricas que eliminaron las bodegas pues producen a demanda, las estrategias de captación de datos personales para marketing dirigido ("conteste esta encuesta y participará automáticamente en un sensacional concurso"), etc.

- La Globalización

Cuando este elemento comenzó a evidenciarse, se le llamó primeramente "Aldea Global" o "Sociedad Global", pero en definitiva se trata del aspecto extensivo de la Sociedad de la Información.

Para explicarlo, usualmente se le relaciona con el poder de las empresas transnacionales, lo que es un error, pues si analizamos los hechos siempre las grandes

[13] De hecho, la idea del teletrabajo es una consecuencia de la crisis del petróleo de la década del 70`, cuando los países productores miembros de la OPEP decidieron operar como cartel, planteándose en Estados Unidos la idea de que era más económico llevar el trabajo al trabajador que el trabajador al trabajo

[14] Aguadero Fernández. Op. Cit.

[15] Manuel Castells. La Era de la Información: La Sociedad Red, Vol. I. Alianza Editorial, 1997

empresas y entidades en general han tenido la capacidad de distribuir sus bienes y servicios a nivel mundial: esta es una de las características de la industrialización en general y su ejemplo más evidente es la omnipresente Coca –Cola y la industria automotriz.

No se refiere tampoco a que haya un público-masa a nivel mundial esclavo de un único sistema de ofertas, sino que más bien al fenómeno contrario: todos somos potenciales medios de comunicación y de producción (oferta) y también consumidores (demanda), y esta característica nos permite generar y destinar productos e información a públicos cada vez más fragmentados, rompiendo los esquemas o modos de hacer tradicionales, lo que se refleja en que las radiodifusoras y la televisión se ven impelidos a iniciar un proceso de personalización del mensaje enfocando su oferta de programación a los gustos de grupos etarios o de intereses específicos. Al respecto, cabe hacer mención que existe un periódico en Chile llamado "Condor"[16], publicado en papel y disponible en Internet que no está dirigido al gran público, si no que satisface los requerimientos de quienes estando en Chile, hablan alemán y tienen la necesidad de leer e informarse en el idioma de Schiller de lo que ocurre tanto en el país como a orillas del Rhein. ¿Y cómo se financia esta idea si aparentemente existen tantas restricciones como barreras idiomáticas y culturales, costos de publicidad a gran escala, capacidad de distribución limitada y un presupuesto restringido?: procesando la información que les permite llegar a las personas específicas que están interesadas en la iniciativa.

Desde el punto de vista del abastecimiento, la globalización también rompe los cadenas de distribución más consolidadas al poner al alcance de los "usuarios" (otro concepto estrechamente vinculado a las TIC y que en ciertos aspectos se confunde con el de "Ciudadano") no sólo los bienes que se ofrecen localmente, sino cualquiera que desee, pues los tiempos y distancias no son relevantes.

Pero no todo el proceso de globalización puede mirarse tan positivamente, pues el hecho de acceder con facilidad a la información mundial que transita por redes trazadas sin fronteras geográficas también va cambiando los intereses y actitudes de los observadores al introducir nuevos elementos a su entorno y experiencia personal, abandonando muchas veces sus patrones culturales, pues ¿para que va a seguir esforzándose un habitante del Amazonas en cazar animales para alimentarse y vestirse, si por televisión muestran que basta con ir al supermercado?, ¿para que los franceses

[16] Condor Online en http://www.condor.cl/

van a comprar frutillas de su región si se han informado que en España las hay más grandes y sabrosas? y ¿para qué vas a tratar de conservar tu lengua, si sabes que la mayoría habla una distinta?.

Ante esta realidad surgen los movimientos antiglobalización, que no son más (ni nada menos) que "la reacción de las identidades particulares que manifiestan la necesidad de autoafirmación individual y colectiva para preservar su entorno más cercano e inmediato"[17], como la religión, lengua, cultura, tradiciones, etc.

Sin embargo, para el profesor HELD tanto los adherentes como detractores acérrimos de la globalización serían representantes de una posición extrema y poco razonable pues, según su concepción, es tan probable la aparición de una cultura global como que las identidades culturales nacionales permanezcan absolutamente inalteradas en medio de su inmersión en estructuras de comunicaciones, concluyendo que "el resultado es incierto; y, por el mismo motivo, también es incierta la futura posición cultural del Estado-nación en esta red cada vez más compleja"[18].

- Fortalecimiento de Redes de Asociación y Cooperación.

El nuevo orden tecnológico permite la interrelación de distintos tejidos y sensibilidades a nivel mundial, dado que el entramado de relaciones posibilita la fluidez de la información independientemente del lugar y tiempo de distancia, permitiendo el establecimiento de esfuerzos con miras a objetivos y fines comunes, lo que se expresa en la renovación de las formas de asociación.

Por ello, no es extraño que grandes corporaciones se asocien a otras entidades más pequeñas con miras a compartir información vital para el desarrollo de ambas o de un relacionado como, por ejemplo, la asociación que existe en Chile entre compañías de teléfonos para los efectos de compartir listados on line de clientes morosos.

Así, las empresas en general cambian sus estrategias de autosuficiencia por otra de intercambio e integración vertical procurándose flujos de información, las Organizaciones No Gubernamentales (ONG) en vez de expandirse y replicar su estructura en otros países para ampliar su ámbito de influencia, se asocian a otras ONG locales para procurarse información estratégica y aumentar su presencia nacional e internacional, llevando adelante proyectos conjuntos sin los costos que tendrían en otras

[17] Aguadero Fernández, Op. Cit.
[18] David Held. Modelos de Democracia. Alianza Editorial, 2001.

circunstancias históricas; a su vez, los Gobiernos intentan satisfacer las demandas de la población a través de la integración funcional de sus sistemas de bases de datos y la concentración de funciones en sistemas de ventanilla única.

En resumen, gracias a las TIC cada entidad y persona de la Sociedad de la Información actúa como nodo, captando información y distribuyéndola a sus asociados.

- Digitalización y Convergencia

En el mundo actual todos los esfuerzos se centran en la digitalización, es decir, en conversión de la información física (papel, pintura, fotografía, etc.) o analógica (audio, vídeo) a un estándar universal susceptible de procesamiento por computadores y transmisión por redes, es decir, en traducir información como textos, imágenes, sonidos, programas de radio y televisión, etc. a un lenguaje binario, constituido sólo por los dígitos cero y uno (0 y 1) y susceptibles de procesamiento por máquinas de cálculo[19].

Con la digitalización, se puede transmitir la información y el conocimiento en un formato que pueden manejar las computadoras y los equipos de telecomunicación, lo que explica también el acercamiento de la televisión y los medios en general a los sectores de la informática y las telecomunicaciones.

Las tecnologías digitales suponen una gran flexibilidad de los soportes y gran capacidad de interconexión, diversidad de usos y de enormes capacidades de conservación de la información audiovisual y la apertura a un potencial de desarrollo multimedia que facilita una aceleración del proceso de convergencia de los medios, lo que es claro, según Muñoz Machado[20], si consideramos que el próximo gran acontecimiento mundial del proceso de digitalización será el forzoso cambio o conversión de los actuales televisores analógicos a aparatos digitales, lo que iniciará el reinado del audiovisual digital antes de diez años.

La convergencia es un proceso indisolublemente ligado a la digitalización, definido por la Unión Europea en el Libro Verde sobre la Convergencia de los Sectores de Telecomunicaciones, Medios de Comunicación y Tecnologías de la Información y

[19] Por ejemplo, la letra "a" para un computador es una forma convencional de la secuencia "01100001" mientras que la "A" es "01000001". E incluso el número "1" que ves en la pantalla, en realidad es una forma visual de la secuencia binaria "00110001".
[20] Santiago Muñoz Machado. La Regulación de la Red. Poder y Derecho en Internet. Taurus, 2000.

sobre sus Consecuencias para la Reglamentación[21], como la "capacidad de diferentesplataformas de red de transportar tipos de servicios esencialmente similares", esto es, la aproximación de dispositivos de consumo, tales como el teléfono, la televisión y el computador a través de un lenguaje único, lo que en definitiva conlleva toda la problemática jurídica de la desaparición de las hasta ahora inequívocas distinciones que separaban a los servicios de telecomunicaciones, los medios de comunicación y las tecnologías de la información. Por ejemplo: las radios que transmiten por Internet ¿deben cumplir la normativa de las concesiones de servicio público de telecomunicaciones propia de las radiodifusoras?. Si quieren darme conexión a Internet a través del sistema eléctrico ¿estamos ante un proveedor de energía eléctrica o de acceso a Internet?[22].

Otra cara de la convergencia radica en que la aparición de la tecnología digital ha obligado a una reordenación mundial del espacio radioeléctrico, pues las frecuencias digitales ocupan mucho menos espacio que los canales o frecuencias analógicas, multiplicando enormemente la capacidad de tránsito de contenidos como también la cantidad de operadores del mercado, dando como resultado que la capacidad de transmisión terrestre y vía satélite supera, por primera vez, la capacidad de producción de la industria de contenidos[23].

- Alfabetización Digital

En la Sociedad de la Información no basta saber leer y escribir, sino que es un imperativo social el conocimiento y dominio de la nuevas formas de alfabetización más acordes con los complejos entornos informacionales, lo que se evalúa a través de una serie de indicadores internacionales que miden, comparan y proyectan la penetración y uso efectivos de las TICS, incluyendo su influencia sobre factores educacionales, de democratización, desarrollo económico, etc., pues el sistema global funciona sólo en la

[21] Comisión Europea. Libro Verde sobre la Convergencia de los Sectores de Telecomunicaciones, Medios de Comunicación y Tecnologías de la Información y sobre sus Consecuencias para la Reglamentación. 3 de diciembre de 1997

[22] Nos referimos a una empresa de la transnacional Enersis que solicitó y obtuvo el año 2002 una autorización para instalar, operar y explotar experimentalmente lo que denominó “Proyecto Piloto Tecnológico de PLC” (Powerline Communications), para prestar servicio de acceso a Internet banda ancha y de telefonía local, lo que les permitirá desarrollar un modelo de negocios de Carrier de Carriers e incluso prestar servicios de telecomunicaciones a través de una filial independiente, de acuerdo a la resolución 683 de la Comisión Resolutiva, de 8 de abril del 2003.

[23] Muñoz Machado, Op. Cit.

medida que la sociedad sea multifocal, es decir, que todas las personas tengan acceso a la red para convertirse en focos de opinión e influencia.

Los promotores de la SI postulan que ésta incluso da mejores posibilidades de integración e igualdad de oportunidades a los discapacitados respecto de cualquier otra etapa en la historia del hombre.

Lo ideal para el modelo es que todos estén alfabetizadas digitalmente, es decir, que las personas comunes tengan conocimientos en el uso de tecnologías, como computación, telefonía móvil, cajeros electrónicos, operación de lavadoras automáticas, Internet, etc.

Desafortunadamente este aspecto también ha generado externalidades negativas, pues el desconocimiento de ciertas herramientas de desarrollo por las personas han hecho surgir nuevas formas de discriminación en que se distingue respecto de quienes están alfabetizados digitalmente y quienes no, alzándose barreras en el acceso al mercado del trabajo, lo que ha llevado a preguntarse si esta nueva sociedad es realmente más justa que las anteriores[24].

- Difuminación de Límites y Fronteras

"Internet desconoce los equilibrios de Westfalia", nos dice Muñoz Machado. Y esta característica del centro y símbolo de la Sociedad de la Información se extiende a toda ella, imprimiéndole su carácter.

Los sistemas de comunicación y el trazado de redes no responden a la nomenclatura territorial y política del Estado. Son abiertos y accesibles, posibilitando la transmisión de flujos de información y la intercomunicación directa e inmediata de todo el planeta con entornos físicos y virtuales, destacando que estos últimos están sujetos a normativas no heterónomas que determinan incluso las condiciones de entrada, salida y permanencia.

A lo anterior debemos sumar que los cambios políticos, sociales, económicos y culturales conducen a una etapa o proceso de desdibujamiento de los sistemas tradicionales de control, lo que se ve agravado por el surgimiento de formas de organización en constante mutación que toman decisiones relevantes a nivel global al margen del poder político.

[24] Para un estudio detallado, véase de la Comisión Europea, Libro Verde. Vivir y Trabajar en la Sociedad de la Información. Prioridad para las Personas. 22 de julio de 1996

Por ejemplo, la autoridad que asigna nombres de dominio para todo Chile ¿es un organismo del Estado?. No. ¿Dependen sus funciones de alguna organización gubernamental nacional o supranacional?. No. NIC Chile[25] actúa por delegación de ICANN[26], sucesor de IANA[27] y ninguna de estas entidades corresponde claramente a Gobierno alguno: es una organización sustentada por los propios usuarios de Internet a través de reuniones generales, elecciones en línea a nivel mundial y acuerdos sobre estándares técnicos[28].

En la SI también existe una crisis de los sistemas tradicionales de control respecto del cumplimiento de aspectos legales que antes eran de sencilla constatación y fiscalización, como la circulación de contenidos nocivos o ilícitos, la copia de software, el pago de impuestos por productos intangibles que circulan por redes, censura de contenidos y, en general, de controversias de Derecho Internacional Privado respecto del tránsito de información por distintos estados nacionales.

- Desmaterialización del Dinero

En la actualidad, y a diferencia de cualquier otro momento de la humanidad, la importancia y volumen del dinero "constante y sonante" es secundario respecto de las transacciones electrónicas a través de sistemas de información.

Los primeros y grandes pasos en esta línea los dieron las tarjetas de crédito y débito, pero actualmente son muy relevantes los flujos de capitales a través de bolsas electrónicas, las transferencias electrónicas bancarias e incluso las compras de bienes y servicios a través de aparatos de telefonía móvil; en definitiva esto ha conducido a la dinamización de las economías a nivel local y global y lleva a concluir que en el nuevo esquema social el volumen en transacciones con dinero físico es tan relevante como lo que podríamos llamar dinero electrónico o digital.

- Terciarización de la Producción y Auge de los Servicios de la Sociedad de la Información

[25] NIC Chile en http://www.nic.cl
[26] Internet Corporation for Assigned Names and Numbers, en http://www.icann.org.
[27] Internet Assigned Numbers Authority, en http://www.iana.org/
[28] Para mayor información sobre esta forma de organización, véase el sitio de Internet Society en http://www.isoc.org .

Más del 50 % de los trabajadores de las sociedades más avanzadas trabajan en el sector terciario de la producción y de ellos, la mayoría trabaja en productos y servicios vinculados a la información, constituyéndose en el área económica más fuerte y dinámica de todas.

Como es evidente, la diferencia con la sociedad post-industrial radica no sólo en que la prestación de servicios crece mucho en relación a la producción de bienes, sino que se trata, en definitiva, de bienes y servicios vinculados a la información.

- Búsqueda de Libertad y Crisis de la Democracia Representativa

Este es uno de los aspectos más polémicos y discutidos de la SI, pues está referido a la transformación de la vida personal, social y política de los ciudadanos-usuarios, quienes han cambiado la forma de mirarse a si mismos, la manera de relacionarse con los demás y los esquemas de participación democrática.

Para ilustrar el inicio de este proceso pensemos en la radio y la televisión convencional de los años 80` ¿qué es lo que había?. Había un número limitado de emisores que entregaban una programación definida por ellos mismos que, con mayores o menores variaciones, eran muy semejantes entre sí, lo que en definitiva no era relevante porque tenían el monopolio de lo que el público escuchaba y veía. Con la invención del personal stereo o walkman se rompe el monopolio de las radios y con la oferta televisiva ocurre algo semejante tras la aparición de los equipos de vídeo para hogares.

¿Qué tienen en común ambos proceso?. Evidentemente el poder de decisión que pasa de los operadores a los ciudadanos-usuarios, quien deciden no sólo sobre los contenidos, sino que también sobre la oportunidad y forma de los mismos.

Este no es un hecho aislado, pues a nivel social se inicia un camino paralelo, ya que el desarrollo de las líneas de comunicación e Internet provocan la reafirmación del ciudadano-usuario opinante, preocupado personalmente de su entorno, quien a través de las tecnologías viaja, investiga, interviene y quiere decidir sobre los temas que le atañen, dado que ya no confía en la capacidad de la democracia representativa para solucionar problemas sociales, lo que en definitiva conduce al resurgimiento de la democracia directa y a la consiguiente recuperación de la soberanía por los ciudadanos-usuarios.

Y este interés por participar directamente en los procesos de decisión, individualista en la forma, se potencia al relacionarse y coincidir con el de los demás

integrantes del ciberespacio, con quienes ha ido construyendo un complejo de relaciones, unidas o no a proyectos comunes, en el que están contestes en no aceptar restricciones a su libertad de ningún tipo por parte de los poderes públicos o privados convencionales, constituyéndose en un poder legitimado.

Como consecuencia de lo anterior y dada su incapacidad actual de controlar la vida individual y social del ciudadano, el poder del Estado tradicional retrocede, pero busca fórmulas que legitimen la democracia representativa[29] y la base que la apoya, que son los partidos políticos, los que han sufrido grave detrimento por este nuevo condicionamiento a la delegación de la soberanía a los gobernantes. Pero esta tendencia de fortalecimiento de la democracia directa, nos advierte Muñoz Machado, en cualquier caso tiene un carácter marcadamente ateniense, pues el acceso a las redes mundiales de comunicaciones aún es privilegio de las clases sociales más acomodadas.

Y estos "atenienses" o nuevas generaciones de ciudadanos-usuarios tienen modelos de comportamiento que los hacen ser identificados, según Louis Rossetto de Wired, como "imparciales, libertarios, tolerantes por naturaleza, políticamente incorrectos, escépticos respecto de los medios establecidos; se sienten menos amenazados por el gobierno en la medida en que lo consideran anticuado e inoperante", cuestiones en las que coincide Katz[30] quien reafirma lo anterior señalando que se trata de "libertarios, materialistas, tolerantes, racionales, adeptos a la tecnología, desvinculados de organizaciones políticas…"[31].

En relación a este tema, el Consejo de Estado francés elaboró en 1998 el informe Internet y las Redes Digitales, que dice "Internet y las redes digitales son, ante todo un nuevo espacio de expresión humana, un espacio internacional que trasciende las fronteras, un espacio descentralizado que ningún operador ni ningún estado puede dominar por entero, un espacio heterogéneo donde cada uno puede actuar, expresarse y trabajar, un espacio apasionado por la libertad"[32].

- Crítica al Concepto de Sociedad de la Información

[29] Un ejemplo claro de lo anterior son las iniciativas que miran el voto electrónico como una forma de contrarrestar el escaso interés de la ciudadanía por participar en elecciones políticas, legitimando los resultados obtenidos.
[30] Jon Katz. Revista Wired, "Birth of a Digital Nation"
[31] Ambos autores son citados en el ya mencionado La Regulación de la Red…
[32] Tomado de Muñoz Machado, Op. Cit.

Como ya hemos dicho, generalmente al dar una noción conceptual de Sociedad de la Información son recurrentes las respuestas que se trata de una sociedad en formación definida por los conceptos de información, comunicación y Nuevas Tecnologías.

Sin embargo, ese estadio aún no existe, por lo que definir un concepto de sociedad a partir de una realidad que aún no existe, pero que se espera que exista, sería según Torres[33], un procedimiento puramente tautológico producto de una confusión metodológica que lleva a resultados imprecisos y ambiguos, por lo que más bien deberíamos decir que estamos ante una pre-noción.

Pero la crítica más dura es de orden social y proviene de las Naciones Unidas, cuyo Secretario General en el Informe del Milenio preparado para la Asamblea General titulado Nosotros los pueblos: la función de las Naciones Unidas en el siglo XXI[34] dice: "Supongamos, por un momento, que el mundo es realmente una "aldea planetaria", tomándonos en serio la metáfora a que a menudo se recurre para describir la interdependencia mundial. Digamos que esa aldea tiene 1.000 habitantes, con todas las características de la raza humana de hoy día distribuidas en exactamente las mismas proporciones. ¿Qué aspecto tendría? ¿Cuáles consideraríamos que son sus principales problemas? Unos 150 de los habitantes viven en una zona próspera de la aldea y aproximadamente otros 780 en barrios más pobres. Unos 70 viven en un barrio que está en transición. Los ingresos medios por persona son de 6.000 dólares al año y hay más familias de ingresos medios de las que había antes. Pero el 86% de toda la riqueza está en manos de sólo 200 personas, mientras que casi la mitad de los aldeanos se esfuerzan por sobrevivir con menos de 2 dólares al día.

El número de hombres es superior al de mujeres por un pequeño margen, pero las mujeres constituyen la mayoría de los que viven en la pobreza. Ha aumentado la alfabetización entre los adultos, pero unos 220 aldeanos, las dos terceras partes de ellos mujeres, son analfabetos. De los 390 habitantes de menos de 20 años, las tres cuartas partes viven en los barrios más pobres y muchos buscan desesperadamente puestos de trabajo que no existen. Menos de 60 personas poseen una computadora y sólo 24 tienen

[33] Asdrad Torres. ¿Qué es la Sociedad de la Información?, en Ciudadanos en la Sociedad de la Información, publicada por el Fondo Editorial de la Pontificia Universidad Católica del Perú y The British Council Perú, 1999.
[34] Kofi Annan. Nosotros los pueblos: la función de las Naciones Unidas en el siglo XXI. 3 de abril del 2000

acceso a la Internet. Más de la mitad no han hecho ni recibido nunca una llamada telefónica".

Al parecer, y de acuerdo al análisis estadístico que subyace al informe del Secretario General, en realidad tendríamos que concluir o que la Sociedad de la Información está muy lejos de ser alcanzada o que sólo es aplicable a los países más desarrollados del mundo occidental.

Finalmente algunos autores de visiones más optimistas previenen que la SI nunca existirá, pues antes de que consolide sus características ya estará mutando hacia la Sociedad del Conocimiento, es decir, vamos hacia aquel estadio del desarrollo humano en que los nodos (personas y entidades) dejarán de emitir y recibir sólo información, sino que comenzarán a generar conocimiento, actuando de forma semejante a las redes neuronales de nuestro cerebro.

Cualquiera que sea el caso, aún hay demasiado camino por recorrer. Tal vez la SI llegará a todos en América Latina, pero las señales nos indican que es previsible que sea con mucho tiempo de diferencia y en condiciones de grave desigualdad: en Chile, si bien el 20,5% de los hogares dispone de computador, lo que representa una de las más altas cifras regionales, en realidad el 2,1% de ese número corresponde al 20% de los hogares más pobres del país[35] y el acceso a Internet que puedan tener, ni siquiera cuenta para efectos estadísticos.

3) Conceptos básicos a considerar.

A continuación, y de una forma de auxiliar a aquellas personas que no tengan un dominio del vocabulario tan técnico que se utiliza comúnmente cuando hacemos referencia sobre las Tecnologías de la Información y las Comunicaciones, se describe un pequeño diccionario con conceptos básicos a considerar, para una comprensión mas completa e íntegra.

Estos conceptos se ordenan en forma alfabética y algunos hacen referencia a vocablos que tienen el mismo significado.

[35] De acuerdo al Instituto Nacional de Estadísticas (http://www.ine.cl) , en base al último Censo Nacional puede afirmarse que al año 2002 el 51,5% de los hogares cuenta con teléfono de red fija y el 51% de ellos tiene al menos un teléfono celular. Asimismo, el 20,5% de los hogares dispone de computador y el 10,2% de ellos presenta conexión a Internet.

A

Accesibilidad

Conjunto de técnicas y herramientas cuyo propósito es facilitar al mayor número posible de personas el pleno aprovechamiento de las tecnologías de la información y de la comunicación, especialmente (pero no únicamente) a aquellos individuos que sufren de limitaciones físicas y/o cognitivas. En cada vez más ordenamientos jurídicos, la aplicación de las referidas técnicas es impuesta como obligatoria, sobre todo con relación al acceso a los servicios y a la información pública.

Adware

Subespecie del software freeware, caracterizado por el despliegue de anuncios publicitarios al usuario, a través de los cuales se subvencionan los costos de desarrollo y distribución. Puede o no estar relacionado con el spyware.

ASP

Acrónimo de "application service provider". Contrato de arrendamiento de software en línea, por medio del cual el arrendatario accede por medios telemáticos al servidor de su proveedor ASP y, desde allí, ejecuta aplicaciones y procesa datos, a cambio del pago de una tarifa prefijada por unidad de tiempo.

Autodeterminación informativa

Derecho fundamental, derivado del derecho general a la privacidad, que se concreta en la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente -pero no exclusivamente- los almacenados mediante medios informáticos.

Autoridad certificante

Ver entidad certificante.

B

Base de datos

Una compilación sistemática y estructurada de datos relacionados entre sí, generalmente creada y gestionada por medios informáticos. No se debe confundir una "base de datos"

con el "software administrador de base de datos", por medio del cual se gestiona a aquélla.

Beta (software)

Calificativo que se otorga a un software que se encuentra aun en la etapa de depuración y pruebas previa al lanzamiento o liberación oficial. Un software beta es usualmente distribuido para que los usuarios puedan colaborar con la detección y corrección de sus posibles defectos, así como para generar observaciones y comentarios que puedan contribuir a mejorar la versión definitiva.

Bomba lógica

Código ejecutable insertado clandestinamente en un sistema informático, con el propósito de "detonar" (provocando alguna consecuencia, normalmente perjudicial), al cabo de cierto lapso de tiempo o del acaecimiento de alguna condición prefijada.

C

Caballo de Troya

software introducido en un sistema informático por medio del engaño (por ejemplo, indicando al destinatario que se trata de un nuevo juego, o bajo el disfraz de un utilitario) y que, una vez allí, está programado para realizar alguna función perjudicial.

Certificado digital

Mecanismo informático por medio del cual se garantiza técnicamente la autenticidad e integridad de un documento, mensaje electrónico o archivo digital asociado con una firma electrónica.

Cesión de derechos (de software)

Convenio por medio del cual el autor o titular de los derechos de autor sobre una aplicación de software transfiere a un tercero o terceros los derechos patrimoniales de la obra. Empleada más frecuentemente en el desarrollo a la medida que respecto del software comercial, la cesión es una alternativa al licenciamiento.

Ciberhostigamiento

El envío no solicitado a otra persona de amenazas, propuestas indecorosas, gráficos u otros elementos ofensivos o intimidantes, por medios telemáticos (típicamente, mediante correo electrónico, mensajería instantánea o por medio de salas de "chat").

Ciberocupación

Acción y efecto de registrar un nombre de dominio, a sabiendas de que otro ostenta mejor título a él, con el propósito de extorsionarlo para que se lo compre o bien simplemente para desviar el tráfico web hacia un sitio competidor o de cualquier otra índole.

Ciberprecarismo

Ver ciberocupación.

Ciberterrorismo

La planeación y ejecución de actos de terrorismo por medios informáticos, especialmente telemáticos (por ejemplo, provocando la interrupción o mal funcionamiento de los servicios públicos).

Cifrado

Ver encriptación.

Cláusula de tiempo máximo de respuesta

Disposición propia de los contratos de servicios de mantenimiento correctivo de hardware o de software, por medio de la cual el proveedor se compromete a atender un requerimiento de auxilio dentro de un tiempo máximo fijado, vencido el cual se incurrirá en alguna clase de sanción, probablemente pecuniaria.

Click-wrap

Modalidad de licenciamiento de software en el que los términos de la licencia son presentados al usuario en pantalla y éste los acepta o rechaza por medio de la selección de un control (por ejemplo, un botón de comando).

Código abierto, código cerrado

Expresiones que denotan el hecho de que el titular de los derechos de una aplicación informática facilite o no, respectivamente, el acceso a su código fuente a terceros. El código abierto es característico del software libre, mientras que el código cerrado lo es del software propietario.

Código fuente

Expresión del contenido de una aplicación informática por medio de un lenguaje de programación, legible e inteligible por quienes estén versados en él (por ejemplo, C++, Java o Perl). Antes de que el código fuente pueda ser ejecutado por el computador, debe ser interpretado o compilado para traducirlo a código objeto. El código fuente debe considerarse un elemento integral del software, para efectos de su tutela jurídica.

Código objeto

Expresión del contenido de una aplicación informática por medio del lenguaje binario de unos y ceros (lenguaje de máquina), que es el único que la computadora puede ejecutar. Usualmente, se obtiene el código objeto como resultado de someter el código fuente a un proceso de compilación.

Comercio electrónico

Toda forma de transacción comercial o intercambio de información relativa a una transacción comercial, que se inicia y perfecciona utilizando tecnología telemática. Se diferencia al comercio electrónico directo (que, por referirse a bienes o servicios digitales, se concierta y ejecuta completamente por vía informática) del indirecto (referido a bienes o servicios físicos que aun cuando permitan una celebración por medios tecnológicos, requieren del medio físico tradicional para su cumplimiento). También se suele categorizar en comercio electrónico de empresa a empresa (B2B), de empresa a consumidor (B2C), de consumidor a consumidor (C2C) o entre empresa y Estado (B2G).

Contratos informáticos

En sentido amplio u objetivo, son todos los convenios cuyo objeto sea un bien o servicio informático, independientemente de la vía por la que se celebren. En sentido restringido o formal, son aquellos contratos cuyo perfeccionamiento se da por vía informática, indiferentemente de cual sea su objeto. A estos últimos se les conoce también, propiamente, como contratos electrónicos.

Contratos electrónicos
Ver contratos informáticos.

Contratos web
Denominación colectiva para los contratos alusivos a cualquiera de las etapas de diseño, construcción, publicación y mantenimiento de un sitio web, incluyendo el hospedaje y registro de nombres de dominio.

Cookie
Tecnología creada por la empresa Netscape con el fin de simular una persistencia en las conexiones sin estado de la WWW. Consisten en pequeños archivos de texto que un programa navegador es capaz de crear y después de recuperar, a petición de un servidor remoto. Pueden ser locales o remotas, según que existan en función de las necesidades del servidor web que las crea o de terceros.

Correo basura
Ver spam.

Cracker
Persona que, con buenos o malos propósitos (lo más usual es lo segundo), se dedica a quebrantar los mecanismos de seguridad de un sistema informático, con el fin de penetrar en él de modo no autorizado.

Criptografía
Ver encriptación.

D

Datos personales

La información que unívocamente distingue a un individuo de otro. Incluye no solo a las llamadas "calidades generales" (como el nombre o el domicilio) sino, muy especialmente, a los datos sensibles (como el origen étnico o racial, la filiación religiosa o ideológica y las preferencias sexuales). Su difusión o manipulación no autorizada compromete el derecho fundamental a la autodeterminación informativa.

Delitos informáticos

Toda conducta típica, antijurídica y culpable que sea vea facilitada o convertida en más dañosa o más lucrativa a causa de la vulnerabilidad creada por el uso creciente de los sistemas informáticos. En la delincuencia informática, el computador puede fungir como objetivo de la acción dañosa (como, por ejemplo, en el sabotaje informático) o bien como mero instrumento para su comisión (como, por ejemplo, en el fraude informático).

Denegación de servicios

Delito informático en el que se recurre a determinadas técnicas informáticas (como por ejemplo al envío masivo de correo electrónico) para provocar una degradación en el rendimiento de un sistema remoto y, eventualmente, su caída, con la consiguiente imposibilidad para sus usuarios legítimos de acceder a él normalmente. Es frecuente encontrar referencias a esta figura con el acrónimo DoS (del inglés "denial of service").

Denegación distribuida de servicios

DDoS ("distributed denial of service"). Modalidad del delito de denegación de servicios, en la que el ataque contra el servidor remoto no proviene de una única fuente sino de múltiples, que actúan coordinadamente y, por ende, con un efecto aun más poderoso. Suele ser el resultado de convertir a esos múltiples sistemas atacantes en partícipes involuntarios ("zombies"), mediante la previa introducción en ellos de un software malicioso diseñado al efecto.

Derecho informático

Disciplina social que procura analizar y proponer respuestas jurídicas a los problemas jurídicos creados por el desarrollo y crecimiento de la informática moderna.

Desarrollo a la medida de software

La creación de aplicaciones de software diseñadas para llenar las necesidades específicas de una persona u organización. De relevancia jurídica cuando es el resultado de un convenio, fruto del cual podría o no derivar la cesión de los derechos patrimoniales del autor o proveedor. El software desarrollado a la medida es lo opuesto al software estándar.

DNS

Ver nombre de dominio.

Documento electrónico

Toda representación de hechos, actos o transacciones jurídicas, producida y conservada electrónicamente.

E

E-comercio

Ver comercio electrónico.

E-gobierno

Ver gobierno digital.

E-sufragio

Ver voto electrónico.

Encriptación

Procedimiento por medio del cual se convierte un texto, mensaje, archivo, documento, etc., de su formato normal a otro normalmente ilegible o ininteligible para quien no posea la clave necesaria para revertir el proceso. Puede ser simétrica o asimétrica, según se emplee la misma clave, o bien dos claves diferentes pero matemáticamente relacionadas entre sí, para encriptar y desencriptar, respectivamente.

Enlace profundo

El establecimiento de un enlace de hipertexto desde un sitio web determinado a una página secundaria de otro, en vez de hacerlo a la página principal o inicial. La práctica es particularmente objetable, por violatoria de la propiedad intelectual, cuando se realiza

por medio de marcos ("frames"), de manera que la página del sitio enlazado parezca formar parte del enlazante.

Entidad certificante

La persona jurídica, pública o privada, nacional o extranjera, que emite certificados digitales para respaldar un procedimiento de firma electrónica de documentos, mensajes o archivos digitales.

Expediente electrónico

Mecanismo informático por medio del cual se emula electrónicamente el expediente físico tradicional de un procedimiento administrativo o judicial. Así como el expediente tradicional consta de documentos físicos, el electrónico está compuesto por registros y documentos electrónicos, gestionados por medio de una aplicación especializada, normalmente de base de datos.

F

Filtrado

Técnica informática por medio de la cual se puede regular el acceso a los contenidos en Internet, bloqueando aquellos que se consideren indebidos o indeseables. Puede realizarse tanto a nivel de servidor (por ejemplo, por medio de un servidor proxy) como de usuario final (mediante un software instalado al efecto en la computadora de éste).

Firma electrónica

Conjunto de datos adjunto o lógicamente asociado a un mensaje, documento electrónico o archivo digital, cuya finalidad sea comprobar su integridad y permitir la identificación unívoca del autor.

Firma digital

Modalidad de firma electrónica desarrollada a partir de una infraestructura de clave pública (PKI) y privada; es decir, de la tecnología de criptografía asimétrica.

Firmware

software que se almacena y ejecuta desde la memoria de solo-lectura (ROM) del computador. Su grado de fijación al equipo puede ser absoluto, como en el caso de los

programas implantados vía circuitos trazados, o relativo, como en el caso de los ROM reprogramables (EPROM). Para efectos jurídicos y por su propia naturaleza, el firmware se considera accesorio del hardware y, por ende, sigue su misma suerte.

Fraude informático

Delito informático que, en sentido amplio, alude a cualquier cambio no autorizado y malicioso de datos o informaciones contenidos en la computadora, en cualquier fase de su procesamiento (entrada, procesamiento o salida), ya sea que medie o no el ánimo de lucro o un perjuicio a terceros. En sentido estricto, solo cuando se dan esos últimos elementos. Se denomina fraude fiscal informático cuando el sujeto pasivo es la Administración fiscal.

Freeware

software cuyo licenciamiento al usuario final se caracteriza por la ausencia de contraprestación; es decir, por su gratuidad. En esa característica no necesariamente va implícita una renuncia a los restantes derechos patrimoniales del autor de la obra, de modo que no se debe confundir freeware con software de dominio público.

G

Gobierno digital o electrónico

Modelo de interacción entre gobernantes y gobernados, que se basa en la idea de emplear medios informáticos no sólo para permitir a los segundos una mejor y más intensa comunicación con los primeros a todo nivel, sino además para permitir la prestación directa de servicios y el sometimiento de toda clase de gestiones a los despachos administrativos, obteniendo por la misma vía la resolución correspondiente.

Gusano

software malicioso, perteneciente a la categoría general de los virus informáticos. Su única o principal funcionalidad consiste en replicarse numerosas veces, ya sea en una sola computadora o a través de redes informáticas. Aun cuando no contenga una carga dañina específica, un gusano puede replicarse tantas veces como para finalmente provocar la caída del sistema o red, o por lo menos, ocasionar un rendimiento degradado.

H

Habeas data

Recurso de amparo especializado, cuyo propósito es la tutela del derecho fundamental de autodeterminación informativa. Por medio de él se pretende lograr acceso a la información personal que obre en un banco de datos público o privado; y eventualmente su actualización, rectificación, supresión, inclusión, adecuación al fin o confidencialidad.

Hacker

Originalmente, un "hacker" era una persona de gran talento e ingenio en el área de la programación; capaz de resolver problemas que escapaban al promedio de los mortales. En la actualidad, el término por lo general posee una connotación negativa, aludiendo a aquellas personas que ponen su talento al servicio de la comisión de actos dañinos o destructivos en el ciberespacio.

hardware

Todos los componentes físicos, tangibles, de un sistema informático. Incluye no solo a la unidad central de proceso (CPU, por sus siglas en inglés), sino también a todos los llamados equipos periféricos (teclado, pantalla, etc.)

Hospedaje web

Contrato de servicios telemáticos, cuya prestación esencial consiste en arrendar espacio en disco en un servidor conectado a Internet para la publicación de un sitio web.

Hosting

Ver Hospedaje web

I

ICANN

Acrónimo de Internet Corporation for Assigned Names and Numbers, asociación sin fines de lucro establecida en el estado de California, Estados Unidos, y que por convenio con el Departamento de Comercio de los Estados Unidos, tiene la misión de dictar políticas y supervisar el funcionamiento global del sistema de nombres de dominio (DNS) de Internet.

Informática jurídica

Disciplina tecnológica que tiene por objeto el estudio e implementación de medios por los cuales la informática pueda hacer más eficiente, ágil y productivo el ejercicio del Derecho en general. Es decir, en la informática jurídica se ve a la computación como herramienta o instrumento del Derecho. Se suele dividir en informática jurídica de gestión e informática jurídica documental. La primera, a su vez, se acostumbra desagregar en informática jurídica operacional, registral y decisional.

Ingeniería reversa

El proceso de extraer el código fuente de una aplicación a partir del código objeto. También llamada descompilación.

Inteligencia artificial

Conjunto de técnicas e investigaciones relacionadas con la posibilidad de que una máquina pueda simular los procesos de razonamiento que caracterizan al cerebro humano.

Intrusión

Delito informático conocido también como "penetración no autorizada de sistemas". La comete quien ingresa en un sistema informático al que no tiene autorización para acceder, posiblemente mediante la violación o previa desactivación de sus mecanismos de autenticación y seguridad.

ISP

Acrónimo de Internet service provider o proveedor de servicios de Internet. Persona física o jurídica que vende servicios de conectividad a la red, ya sea por vía conmutada o dedicada. Es frecuente que el servicio incluya facilidades adicionales, tales como la asignación de uno o más casilleros de correo electrónico.

L

Leasing

En general, contrato por medio del cual una persona física o jurídica (locador) se obliga a entregar el uso y goce de un bien a otra (locataria), quien se obliga a su vez a pagar un alquiler por él, por el término del contrato, al finalizar el cual el locatario

puede optar entre solicitar la prórroga del contrato, devolver el bien o adquirirlo. En el mundo de la informática, resulta de gran conveniencia como alternativa a la compraventa de hardware, en la medida en que ayuda a minimizar los problemas de la obsolescencia tecnológica.

Licenciamiento de software

Contrato por medio del cual el titular de los derechos de autor puede sustituir la enajenación total o parcial de sus derechos patrimoniales respecto de un software, por la simple concesión a terceros de una licencia o autorización de uso de la aplicación, que como regla (es decir, siempre que la propia licencia no indique otra cosa) se considerará como no exclusiva e intransferible. Puede constar por escrito, ya sea en un soporte físico o de modo electrónico, distinguiéndose en particular las modalidades comunmente denominadas shrink-wrap y click-wrap.

M

Mantenimiento

Denominación genérica de un conjunto de servicios técnicos orientados a garantizar el buen funcionamiento de un hardware, de un software o de otros bienes o servicios informáticos (como, por ejemplo, un sitio web), y que se puede acordar tanto como componente accesorio de un contrato de alcance más general o bien por sí solo, como contrato autónomo. En el caso del hardware, se distingue el mantenimiento preventivo del correctivo, mientras que respecto del software o de los sitios web, se habla además del mantenimiento evolutivo, orientado a la actualización.

Monitoreo electrónico

La aplicación de métodos electrónicos e informáticos, por medio de hardware o software, con la finalidad de vigilar la conducta de otra persona o personas. Por ejemplo, la utilización de software de monitoreo para supervisar el uso que los menores de edad en el hogar, o los empleados en el centro de trabajo, dan a los recursos tecnológicos.

N

Neutralidad tecnológica

Propiedad de un sistema de información en virtud de la cual el acceso al sistema o a los datos contenidos en él no está condicionado al empleo de determinadas plataformas tecnológicas. La neutralidad tecnológica se logra, esencialmente, mediante el apego a estándares abiertos, tales como los fijados por la International Standards Organization (ISO) o por el World Wide Web Consortium (W3C) para la web.

Nombre de dominio

Etiqueta alfanumérica asociada a una dirección IP que, a su vez, identifica unívocamente a un servidor en Internet. La traducción de una etiqueta (tal como hess-cr.com) a un número IP (tal como 207.44.228.73) y viceversa, es efectuada conforme al sistema de nombres de dominio (DNS, por sus siglas en inglés), por medio de múltiples servidores de nombres distribuidos en la red. Los nombres de dominio se dividen en genéricos o gTLDs ("generic top-level domains" como .com, .org, .net) y de código nacional o ccTLDs ("country-code top-level domain" como .cl, .fr, .mx).

O

OMPI

Organización Mundial de la Propiedad Intelectual. Organización internacional cuyo objetivo es velar por la protección de los derechos de los creadores y los titulares de propiedad intelectual a nivel mundial.

Opt-in, opt-out

Literalmente, "optar dentro, optar fuera". La expresión alude a aquellas bases de datos o registros empleados esencialmente para que las personas puedan especificar si desean o no recibir ofertas comerciales por teléfono o correo electrónico; permitir o no que sus datos personales sean recopilados y utilizados por empresas de mercadeo; etc.

P

Patentamiento de software

Régimen legal de tutela jurídica del software existente en aquellos ordenamientos que no han optado por hacerlo a través del derecho autoral, o que lo hacen alternativa o complementariamente. La obtención de una patente respecto de una aplicación informática está sujeta a los mismos tres criterios que tradicionalmente aplican a cualquier otra clase de invención, a saber: uso práctico, novedad y carácter inventivo.

Procedimiento electrónico

Alude a la posibilidad de sustanciar trámites procesales, en sede administrativa o judicial, por medios electrónicos. Esto normalmente involucra admitir y regular la validez legal de los documentos electrónicos, el registro electrónico de gestiones y el expediente electrónico, así como de algunos elementos complementarios, tales como la firma electrónica.

R

Registro electrónico de gestiones

Alude a la posibilidad de someter documentos electrónicos a las dependencias públicas, por vías telemáticas. Entre sus ventajas se cuenta que elimina la necesidad de traslado físico del gestionante hasta la oficina pública en cuestión, ahorrando tiempo y dinero; los despachos se descongestionan, reduciendo filas en ventanillas; la información se captura electrónicamente, minimizando errores y la necesidad de digitar nuevamente los datos; existe la opción de remitir los documentos fuera de horas de oficina; y se prescinde del papel, beneficiando al ambiente.

S

Sabotaje informático

Delito informático tipificado como el acto de borrar, suprimir o modificar sin autorización funciones o datos de un sistema informático con intención de obstaculizar su funcionamiento normal. Resulta especialmente aplicable a quien, deliberadamente, introduzca un virus informático en dichos sistemas.

Servidor proxy

Hardware o software que actúa como un intermediario entre un usuario de una red local y la Internet, con el fin de implementar políticas de seguridad, control administrativo y servicios de caché. Un servidor proxy intercepta una petición de acceso a un recurso en Internet (por ejemplo, una página web) y la valida contra sus políticas de filtrado. Si no las cumple (típicamente porque cierta clase de contenidos -como la pornografía, los juegos o las descargas de música- han sido restringidos), devuelve un mensaje al usuario en el sentido de que el acceso ha sido denegado. Caso contrario, el proxy revisa su caché de archivos y páginas previamente accedidos y, si lo encuentra, lo

transmite al usuario sin necesidad de descargarlo de Internet, lo cual acelera sustancialmente la navegación. En caso de no tenerlo disponible, obtiene el archivo o la página, actualiza el caché local y acto seguido transmite el resultado al usuario.

Desde el punto de vista jurídico y dependiendo de cómo se les utilice, los servidores proxy pueden plantear eventuales problemas en los campos del filtrado de contenidos y la vigilancia electrónica de los usuarios.

Shareware

Por "shareware" no se entiende en rigor una clase de software, sino a una modalidad de licenciamiento que se caracteriza por permitir el examen del producto hasta el acaecimiento de una condición preestablecida, en cuyo momento el usuario debe decidir si desea conservarlo o no. Caso afirmativo, deberá satisfacer una contraprestación estipulada en el contrato por el licenciante.

Shrink-wrap

Manifestación del contrato de licencia, típica del software comercial, en la que el clausulado viene estampado, bien en la caja de distribución del producto o –más frecuentemente aun– en un documento que se agrega al contenido, ya sea al inicio del manual del usuario o en hoja aparte. Se le denomina de esta manera por asociación con el plástico adhesivo mediante el cual se sella el paquete y cuyo rasgado es interpretado como una aceptación tácita de los términos de la licencia.

Sistema experto

Aplicación informática que procura capturar conocimiento y luego utilizarlo para emular el mecanismo de raciocinio de un experto humano, para la resolución de problemas concretos. Esto se logra automatizando su procedimiento de toma de decisiones. Es decir, los creadores de sistemas de este tipo analizan no sólo lo que un experto sabe, sino además la manera en que resuelve problemas, con el fin de tratar de replicar ese proceso artificialmente. Un sistema experto consta fundamentalmente de una base de conocimiento, un motor de inferencia y una interface de diálogo con el usuario.

Software

Todos los componentes lógicos de un sistema informático, que incluyen tanto a las aplicaciones como a los datos sobre los cuales operan. Desde una óptica técnica, se subdivide en software de sistema y software de aplicación. Las posibles subdivisiones de interés jurídico dependen del criterio de clasificación empleado, a saber: a) según el grado de estandarización: software estándar o hecho a la medida; b) según el grado de vinculación del software al hardware: firmware o software autónomo; c) según la presencia o ausencia de contraprestación y sus modalidades: software comercial, shareware o freeware; y, d) según la modalidad de licenciamiento: software propietario, libre o de dominio público.

Software malicioso

Software que ha sido deliberadamente diseñado para producir un resultado defectuoso o dañoso para el usuario. Incluye tanto la categoría genérica de los virus informáticos, como la del llamado spyware.

Spam

Se denomina "spam" al correo electrónico masivo, no solicitado, de carácter comercial. "Spamming" es la acción y efecto de enviar spam. Finalmente, "spammer" es la persona o empresa que se dedica a enviar spam.

En la problemática del spam encontramos un conflicto de intereses jurídicos, que involucra la libertad de expresión comercial o publicitaria, de una parte, versus el derecho a la información (en sentido inverso o negativo) y a la privacidad, de otra.

Algunos términos relacionados incluyen "spim" (envío de comerciales no solicitados por medio de un servicio de mensajería instantánea) y "spit" (envío de comerciales no solicitados por medio de un servicio de telefonía de Internet).

Spyware

Categoría de software malicioso, similar pero separada de la de los caballos de Troya, cuya funcionalidad consiste en recopilar información subrepticiamente sobre el usuario o usuarios de un sistema informático, o bien supervisar sus patrones de conducta en línea, con el fin de reportar los resultados de vuelta a su creador. El propósito más común de estos datos es el de crear perfiles de consumo para efectos de telemercadeo.

T

Teletrabajo

Modalidad de la relación laboral, en virtud de la que los servicios del empleado son prestados esencialmente de manera remota, haciendo uso de herramientas telemáticas. Todos los elementos usuales de un contrato de trabajo (subordinación, remuneración, etc.) se encuentran presentes en la relación, excepto el de la supervisión presencial por parte del empleador. Se le conoce en la jerga angloparlante como telecommuting.

Tesauro jurídico

Herramienta de la informática jurídica, cuyo propósito es minimizar los problemas de polivalencia y sinonimia que caracterizan al lenguaje jurídico y que pueden afectar negativamente la búsqueda libre de contenidos, ya fuere en una base de datos, la Internet, etc. Por medio del tesauro jurídico, la búsqueda de un determinado concepto producirá no solo los resultados que le corresponden de modo exacto, sino además los asociados a los conceptos que hayan sido especificados como equivalentes en la herramienta.

TICs

Abreviatura de la frase Tecnologías de la Información y las Comunicaciones.

Tutela jurídica del software

Mecanismo o mecanismos jurídicos por medio de los cuales se procura brindar protección al software en tanto creación intelectual que es. Estos pueden incluir, de acuerdo con el ordenamiento jurídico de que se trate: a) las patentes de invención; b) el derecho autoral (derechos de autor); o, c) sistemas sui generis.

U

UDRP

Acrónimo de "Uniform Domain Name Dispute Resolution Policy" ("Política Uniforme para la Resolución de Disputas por Nombres de Dominio"). Conjunto de reglas adoptado desde 1999 por la ICANN para procurar la solución extrajudicial (arbitral) de diferendos relativos a nombres de dominio en la red, particularmente debido al crecimiento del fenómeno conocido como ciberocupación.

V

Virus informático

En sentido amplio, cualquier software que se diseña y difunde con propósitos maliciosos, incluyendo los virus propiamente dichos, asi como los gusanos, caballos de Troya y bombas lógicas. En sentido estricto, un virus se caracteriza por la presencia usual de tres elementos distintivos: una carga ("payload"), un mecanismo de replicación y un mecanismo de elusión. La carga es la acción generalmente dañina o destructiva, que el virus está diseñado para ejecutar. El mecanismo de replicación permite que el virus se disemine, "infectando" a otras aplicaciones o computadoras. El mecanismo de elusión procura lograr que el virus pueda actuar sin ser detectado. En 1949, John von Neumann fue el primero en teorizar acerca de un software auto replicante.

Voto electrónico

En general, un mecanismo por el cual se busca sustituir el sufragio mediante papeletas o boletas tradicionales de papel, con medios electrónicos e informatizados. En principio, el voto electrónico reportaría una importante seria de ventajas (mayor rapidez en el cómputo, menor gasto electoral, posibilidad de votar en forma remota, etc.). Sin embargo, algunos críticos han señalado también que adolece de importantes debilidades (confusión de los electores, opciones de fraude, etc.)

W

Web bug

Una imagen GIF que se hace virtualmente invisible por medio de fijar su tamaño en 1 x 1 pixel y cuyo propósito es registrar, por medio de su software asociado, el hecho de que una persona haya leído el mensaje o visualizado la página web que la contiene. En otras palabras, constituye una modalidad de spyware.

Capitulo II Derecho a la Privacidad

"Los ordenadores son como los dioses del Antiguo Testamento, repletos de reglas y faltos de piedad"
Joseph Campbell

1) Concepto.

Cuando analizamos el título de esta memoria y que reza "DERECHO A LA PRIVACIDAD Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES", vemos que la primera referencia que hacemos al mundo jurídico dice relación con la privacidad.

Para poder realizar un análisis exhaustivo de la relación existente entre derecho y Tecnologías de la información y las comunicaciones, debemos reparar en la palabra "privacidad" y sus verdaderos alcances, diferenciándolo de "intimidad", puesto que la regla general es hacer sinónimos ambos conceptos sin hacer una diferenciación entre su uso, tanto por parte de la doctrina como por los legisladores.

La principal dificultad radica en la confusión que las leyes, los códigos de ética y los manuales de estilo hacen de los términos privacidad e intimidad, a los que tratan como sinónimos. Si a eso le sumamos el desarrollo de los medios de comunicación no sólo en términos tecnológicos, sino también en términos de lenguaje, de dinámica, en definitiva en todo lo que involucra un cierto acervo mediático, nos percatamos que los conceptos en uso ya no alcanzan para dar cuenta de la realidad. Y menos aún para normarla.

Ante tal escenario, difícilmente podemos hacer algo más que intentar una descripción inequívoca de qué es lo público, lo íntimo y lo privado, y dar un contexto a

la forma en que éstos se articulan en el quehacer periodístico del mundo contemporáneo.

- Intimidad y Privacidad son sinónimos:

A la hora de hablar del Dº a la privacidad varios autores consideran que ambas palabras tienen un significado común y no es necesario analizarlas y establecer diferencia alguna.

1. Situación en Chile

Así por ejemplo, en nuestro país el profesor Renato Jijena lo define en un principio como "el bien jurídico intimidad" [36] y literalmente señala "Personalmente consideramos como sinónimos una serie de términos que manejan los autores: intimidad, privacidad, privacy, vida privada, esfera íntima y esfera privada." [37]

Por otro lado se menciona «la doctrina de los autores ha definido a los antecedentes y hechos de la vida privada, cuya reserva y custodia se busca, como intimidad y, a ésta, como el derecho personalísimo que protege la reserva espiritual de la vida privada del hombre, asegurando el libre desenvolvimiento de éste en lo personal, en sus expresiones y en sus afectos" [38] y contrariamente con nuestro pensamiento que mas adelante desarrollaremos, se indica que "una diferenciación carece de efectos jurídicos en nuestro ordenamiento, y es así que la Constitución Política de 1980 —como ya lo veremos— utiliza la voz «vida privada» como sinónimo de la noción de «intimidad».")[39]

Conteste a lo anterior, el actual Ministro de la Corte de Apelaciones de Talca Eduardo Meins Olivares indica que "la doctrina alude indistintamente a la intimidad, a la vida privada o a la privacidad." Y que "entendemos como sinónimos, para todos los efectos, las voces intimidad y vida privada, a pesar que algunos distinguen entre ambos conceptos"[40]. Siguiendo claramente su postura y conforme al cargo de ministro que ocupa, nos señala que como primera cosa, debemos tener presente que frente a un caso concreto en que se plantee la violación a la vida privada o intimidad, es el tribunal

[36] Jijena Leiva, Renato Javier, Chile, la protección penal de la intimidad y el delito informático, Santiago, Ed. Jurídica de Chile, 1992
[37] Ibid, pág, 23
[38] MUÑOZ NAVARRO (n. 24) ver libro dº penal
[39] Ibid, pág. 25
[40] Meins Olivares, Eduardo, Derecho a la intimidad y a la Honra en Chile, Revista Ius ex Praxis, año 6 N° 1, 2000

respectivo a quien compete decidir si la faceta de la vida de la persona que se estime afectada queda o no comprendida dentro del ámbito del derecho a la intimidad.

Otro autor de renombre como es Eduardo Novoa, no le da ningún tratamiento especial para diferenciar ambos conceptos, sobre todo cuando hace referencia a la libertad de expresión, pues hace equivalentes el derecho a la vida privada y la intimidad.[41]

Continuando con esta idea de igualdad en los conceptos, don Humberto Nogueira Alcalá, cuando hace referencia al proyecto de ley referida a la protección del honor y la intimidad de las personas (actualmente este proyecto se encuentra aprobado en la Cámara de Diputados y enviado al Senado con fecha 9 de diciembre de 2003, en actual trámite en la Comisión de Constitución, Legislación y Justicia del Senado de la República), menciona que "en el ámbito de privacidad e intimidad los terceros sólo pueden penetrar con el consentimiento de la persona afectada, poseyendo, asimismo, la persona la facultad de control de dichos actos, como asimismo, de los datos referentes a su vida privada e intimidad"[42]. En esta frase no efectúa ninguna diferenciación. Sin embargo, el proyecto de ley a la que se refiere claramente habla solo de honor e intimidad y no de privacidad.

Esta igualdad de conceptos no es privativa de los autores sino también de los tribunales de justicia. Así por ejemplo se ha establecido que las clínicas u hospitales no pueden grabar, filmar y exhibir operaciones realizadas en pacientes sin su expreso consentimiento, ya que ello viola el derecho al respeto y protección de su intimidad. Corte de Apelaciones de Santiago, Rol N° 2563-92 P., confirmado por la Corte Suprema Rol N° 20.142 del dieciséis de diciembre de 1992). A nuestro entender se estaría dando un correcto uso de intimidad. Paralelamente la Corte de Apelaciones de Santiago, en fallo de Recurso de Protección, de 08 de septiembre de 1997 confirmado por la Corte Suprema, contenido en la Revista Gaceta Jurídica, Nº 209, pág.49, frente al recurso de protección deducido por Francisca Milena Andrea Rischmaui Grinblatt, en contra del "Consorcio Periodístico de Chile S.A. Copesa", señala que dado que éste cometió un acto arbitrario e ilegal que perturba su legítimo derecho al respeto y protección de su vida privada, y que consiste en la publicación en el Diario "La Cuarta"

[41] Novoa Monreal, Eduardo, Derecho a la vida privada y libertad de información : un conflicto de derechos, 2ª.ed. México : Siglo Veintiuno, 1981

[42] NOGUEIRA ALCALA, Humberto. Pautas para Superar las Tensiones entre los Derechos a la Libertad de Opinión e Información y los Derechos a la Honra y la Vida Privada. *Rev. derecho (Valdivia)*, dic. 2004, vol.17, p.139-160

de 31 de julio de 1997, de una fotografía suya, en traje de baño, en una playa, sucedida de la leyenda "la esbelta y atractiva lola sueña con que llegue luego el verano para retornar a las cálidas arenas", todo ello sin su autorización y sin que ello obedeciera a ninguna información o noticia que lo hiciera pertinente, señaló : "Que, aunque como manifiesta el recurrido no puede efectivamente afirmarse que con la sola publicación de la fotografía en referencia -seguida de la ya expresada leyenda-, se haya afectado la "honra" de la recurrente, no es menos cierto que, al haberse procedido a ello sin su consentimiento previo, se ha perturbado sin embargo el derecho que al "respeto y protección" de su "vida privada y pública" le asegura la Constitución. En este caso existiría un error al confundir vida privada (o privacidad) con intimidad.

2. Situación extranjera.

A nivel internacional, Pablo Dermizaky Peredo, catedrático boliviano nos habla del derecho a la intimidad en la legislación boliviana sin hacer distinción alguna con el derecho a la privacidad, asimilándolos completamente en un solo concepto.[43]

Lo mismo ocurre con la definición de derecho a la privacidad dada por el Colombiano Ernesto Villanueva y que reza “Es el derecho fundamental de la personalidad consistente en la facultad que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público”[44] puesto que hace referencia a un elemento de la personalidad que se encuentra a nuestro entender, solo en el derecho a la intimidad mas no en la del derecho a la privacidad, por las razones que mas adelante indicaremos.

- Intimidad y Privacidad son conceptos distintos:

Recientemente se ha comenzado a distinguir entre estos dos conceptos, señalando diferencias que aunque mínimas, a nuestro entender, establecen pautas de aplicación distintas, en lo referente a protección legal, respecto por un lado al derecho a la intimidad y derecho a la pivacidad.

[43] Dermizaky Peredo, Pablo, EL DERECHO A LA INTIMIDAD, Revista Ius ex Praxis, año 6 N° 1, 2000.
[44] Villanueva, Ernesto. *“Derecho de la información”*. CIESPAL, Quito, 2003, p. 233.

En la legislación Española, por ejemplo y refiriéndose específicamente al derecho fundamental a la protección de datos de carácter personal, la Ley Orgánica 17/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal dispone en su artículo 1 que la ley tiene por objeto:

"Garantizar y proteger los derechos y libertades fundamentales en lo concerniente al tratamiento [automatizado o no] de los datos personales y especialmente el derecho al honor e intimidad personal y familiar de las personas físicas". Esta ley fue la que derogó a su vez la Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal texto legal en cuya Exposición de Motivos se afirmaba "que ***se habla de la privacidad y no de la intimidad: aquélla es más amplia que ésta***, pues mientras la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona; la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí [por la posibilidad actualmente que ofrecen las nuevas tecnologías], arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".

En consecuencia, la Exposición de Motivos concebía interés social susceptible de protección por ella a la privacidad, concepto distinto y mucho más amplio que el de la intimidad. Asi, podemos concluir que el derecho a la protección de datos (es decir, derecho a la privacidad) es mucho más amplio que el derecho a la intimidad. En efecto, mientras el derecho a la intimidad sólo comprende dentro de su ámbito, los datos de la vida íntima, el objeto derecho a la protección de datos abarca no sólo a los llamados datos íntimos de la persona, sino también a cualquier otro tipo de dato personal, sea o no íntimo, esto es, sea público privado, cuyo conocimiento o empleo por terceros puede afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual (pues para ello está la protección dispensada por el artículo 18.1 C.E.), sino los datos de carácter personal.

Por otro lado, José García Falconí, jurista ecuatoriano nos comenta dice a la hora de establecer diferencias entre privacidad e intimidad que "la privacidad es mas amplia que la intimidad. La intimidad protege la esfera en que e desarrollan las facetas mas singularmente reservadas de la vida de la persona, como el domicilio, las

comunicaciones. etc., en cambio la Privacidad constituye un conjunto mas amplio, mas global de facetas de su personalidad que este tiene derecho a mantener en reserva"[45]

Los tratadistas alemanes[46], han distinguido la *Intimsphäre,* o esfera de lo secreto, y cuya violación se produce por el conocimiento de los hechos o noticias que deben permanecer ignorados; la *Privatsphäre,* protectora del ámbito familiar y personal – y la individualsphäre, correspondiente al ámbito personal del individuo, a su yo interno. (honra, propia imagen, nombre).

En Chile, esta diferencia de tratamiento entre derecho a la intimidad y la privacidad se ve reflejada especialmente cuando se contrapone con el derecho a la información.

Así, por ejemplo lo señala Miguel González Pino, profesor de Derecho y Ética de la Información en la Universidad Diego Portales, en su artículo titulado "La vida privada y la ética informativa" al señalar que "todo hombre que está inserto y que se conduce normalmente en la sociedad está íntegramente cubierto por tres dimensiones: la esfera pública, la esfera privada y la intimidad."[47]

Conforme a lo anterior, El Código de Ética del Colegio de Periodistas de Chile esboza una suerte de diferencia al establecer en su artículo 26 y que dice: "El periodista debe mantener un incuestionable respeto a la dignidad y vida privada de las personas, evitando dejarse tentar por las posibilidades de invasión de la intimidad que ofrecen las nuevas tecnologías." Esta misma idea es aplicada por el Consejo de Ética quien en la sentencia nº 55 señala que "La intrusión forzada o clandestina en dichas áreas, y/o su difusión periodística, violan el derecho a la intimidad o vida privada de las personas, sea que se irrumpa físicamente en tales recintos; o que se empleen medios técnicos para observar, escuchar, fotografiar, grabar o captar de cualquier manera palabras o imágenes que están protegidas por el derecho a la vida privada; o que se usen al efecto testimonios de terceros.", considerando como íntimo por naturaleza a situaciones como una conversación telefónica y"en consecuencia inviolable, a menos que los que intervienen en ella consientan en que se haga pública". (Sentencia N° 8)

- Nuestra propia postura:

[45] García Falcón, José; http://www.dlh.lahora.com.ec/paginas/judicial/paginas/D.Constitucional.69.html
[46] H. Hubmann. Das Persönlichkeitsrecht. Böhlau, Köln, 2 edición, 1967. Cit. por Perez Luño, ob. Cit. pág. 328
[47] Para poder leer este artículo, se puede visitar la página oficial de la Asociación Nacional de la Prensa (http://www.anp.cl) e ir a la sección aspectos legales.

Para nuestro entender el concepto de intimidad y privacidad si son distintos y se les debe dar un tratamiento distinto. Advertimos de antemano que en muchas situaciones, es muy difícil entender cuando nos referimos a intimidad y cuando a privacidad.

La principal dificultad radica en la confusión que las leyes, los códigos de ética y la doctrina (como lo hemos demostrado con anterioridad) hacen de los términos privacidad e intimidad, a los que tratan como sinónimos. Si a eso le sumamos el desarrollo de los medios de comunicación (materia principal de esta memoria) no sólo en términos tecnológicos, sino también en términos de lenguaje, de dinámica, en definitiva en todo lo que involucra un cierto acervo mediático, nos percatamos que los conceptos en uso ya no alcanzan para dar cuenta de la realidad y menos aún para normarla sin dificultad, en principio.

Analizando las lenguas de diversos países, observamos que en todas existen palabras distintas para expresar intimidad y privacidad, excepto la lengua inglesa que, a pesar de tenerlas, se ha decantado por privacidad.

En alemán: *Intimität* y *Privat Leben*

En francés: *Intimité y vie privée*

En italiano: *Intimitá y riservatezza*

En inglés: *Intimity y privacy*

En español: Intimidad y privacidad.

En la lengua inglesa, la palabra *intimity* se suele emplear para denominar las relaciones sexuales ilícitas, por lo que se ha evitado utilizarla para el objeto a que nos referimos aquí, quedando sólo la palabra *privacy* para designar tanto la intimidad como la vida privada.

Por lo mismo, y de modo de justificar nuestra postura, tenemos que diferenciar ambos conceptos, tratando de señalar los límites y alcances de sus propias definiciones.

2) Derecho a la Privacidad v/s Derecho a la Intimidad

- ¿Qué es lo íntimo?

Para el Diccionario de la Real Academia, intimidad es "la zona espiritual intima y reservada de una persona o un grupo, especialmente de una familia".
Como puede apreciarse, tal definición gira en torno a la idea de secreto, a la confidencialidad de una persona o de un grupo, especialmente de carácter familiar.

El adjetivo *íntimo* viene del latín *íntimus, -a, -um*, que es el superlativo de *interior* 'interior'. En latín, el adjetivo *íntimus* significa 'recóndito, que está en el fondo de algo, situado en lo más interno'.

Según el origen de la palabra, se refiere a lo que se guarda en el interior, lo más próximo, que no se comparte con nadie o casi nadie. De hecho, la expresión suele servir como adjetivo, se usa para distinguir una conducta, una situación, un lugar, que se caracteriza por esa cercanía o esa particular discreción. Así se habla de los pensamientos íntimos, también de amigos íntimos, relaciones íntimas, incluso lugares íntimos, donde uno puede estar separado de los demás.

Tentativamente, se podría definir diciendo que es íntimo lo que se hace rigurosamente fuera de la mirada de otros, que sólo se manifiesta voluntariamente, a unos cuantos.

El concepto jurídico de intimidad ha ido evolucionando a lo largo del tiempo, su origen puede ser situado a finales del siglo pasado. Será un asunto aparentemente irrelevante el que permitirá definir por primera vez las características técnico jurídicas de la noción *de privacy.* En concreto, Samuel D. Warren, casado con la hija del Senador Bayard, se dedicó a conducir una vida tildada de dispendiosa y desordenada en la época. Asi, D. Warren y Louis D. Brandeis ansiosos por evitar intromisiones en la esfera privada de aquel, por parte de la prensa, realizaron un estudio que culminó en su monografía "The *Right to* Privacy"(1890), donde "privacy" aparece configurada como el derecho a la soledad, la garantía frente a cualquier invasión privada y domestica.

Mucho tiempo ha pasado desde entonces, las condiciones políticas, sociales, económicas *y* tecnológicas han cambiado *y* junto a alias han hecho su aparición nuevas amenazas para la esfera privada del individuo, que han originado la transformación del concepto de intimidad. Hay que esperar a los años sesenta para asistir a un cambio radical en la sensibilidad social respecto a la intimidad. Este cambio se debe, en gran medida, a la conciencia de que la informática abarca territorios cada vez mas amplios, a través de una perfeccionada red que permite una fluida y rápida transmisión de datos. La rapidez de elaboración, la capacidad de selección así como la facultad de agregar y disgregar información del ordenador es tal que el ciudadano se alarma: la enorme

cantidad de datos memorizados permitiría, a quien ostentase el poder, controlar a fondo cada actividad.

De todos modos, la acepción mas arraigada de intimidad es la que la considera como la garantía de que nadie pueda sufrir intrusiones o investigaciones no deseadas sobre su vida privada y que tales investigaciones no puedan ser divulgadas. Así entendida, la intimidad serviría para preservar "el ámbito personal" donde cada uno, alejado del mundo exterior, "encuentra las posibilidades de desarrollo y fomento de la personalidad[48].

El derecho a la intimidad ha sido considerado por la teoría jurídica tradicional, junto con el honor y la propia imagen, como manifestaciones de los derechos de la personalidad y, en el sistema actual de derechos fundamentales, como expresiones del valor de la dignidad humana. Esta última constituye uno de los pilares sobre los que se construye el sistema de garantías constitucionales de los derechos y libertades, de modo tal que los derechos fundamentales se erigen en instrumento para la plena realización de la dignidad humana, cuyo fin ultimo es el libre desarrollo de la personalidad.

La intimidad se vincula a la esencia de las personas. Su difusión es una tarea que sólo la propia persona puede realizar por la naturaleza de este ámbito de la personalidad. Involucra los sentimientos, pensamientos, sensaciones y reflexiones propias de un individuo en su estado de máxima introspección. Esto se ve reflejado en las características que tendría la intimidad según Norberto González Gaitano.

1) Sólo las personas físicas gozan de intimidad; las personas jurídicas y las instituciones, no. Cuando se habla, por ejemplo, de las “intimidades de un partido”, el término se emplea en sentido figurado. Su significado real reside en la propia persona, es el corazón de su personalidad.

2) La intimidad requiere el consentimiento para participar de ella sin que se destruya. Requiere siempre del consentimiento libre del sujeto para hacer partícipe a otros. Conocer y difundir la intimidad de una persona contra su voluntad comporta automáticamente su destrucción.

3) La intimidad implica el respeto a la libertad de las personas, pues su existencia, conocimiento y difusión ocurre sólo por donación, la cual es siempre libre y voluntaria, como en el caso de la amistad y el amor.

[48] Bajo Fernandez, M., "Protection del honor e intimidad" en AA VV.Comentario a las leyes penales, Madrid**,** 1982, Ed. Edersa, p. 101.

4) La intimidad tiene un valor absoluto, incuestionable e inviolable, lo que se refleja en ciertos derechos como la libertad de pensamiento o doctrinas como la objeción de conciencia que no pueden ser objeto de mandatos judiciales.[49]

- ¿Qué es lo privado?

El término *privacidad*[50] es uno de los más difundidos por los medios de comunicación, así como uno de los más discutidos por los especialistas en temas normativos de la lengua.

En general, los libros de estilo y otras obras jurídicas rechazan la palabra, por considerarla un barbarismo o un anglicismo innecesario fácilmente sustituible por *intimidad* tal como lo habíamos señalado anteriormente. Por su parte, solo recién en la edición de su diccionario normativo, publicada en el año 2001, la Real Academia Española[51] ha admitido la palabra *privacidad*, con el significado de "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".

Morfológicamente, *privacidad* es un calco del inglés *privacy* y del francés *privacité*. Es posible que el término en español no sea un ejemplo de «pureza» morfológica, pero se encuentra dentro de los límites del sistema de la lengua, es decir, dentro de las posibilidades expresivas que ofrece el sistema.

Aunque la ley chilena no define qué significa vida privada o familiar, sí trata de delimitar sus alcances, para impedir el uso abusivo de estos términos en desmedro de la libertad informativa. Para ello efectúa en primer lugar una precisión, respecto de circunstancias que claramente pertenecen al ámbito privado. En el artículo 30 de la Ley Nº 19.733, a propósito del delito de injuria se señala: "Se considerarán como pertinentes a la esfera privada de las personas los hechos relativos a su vida sexual, conyugal, familiar o doméstica, salvo que ellos fueren constitutivos de delito."

El concepto de vida privada es un concepto variable en el tiempo. El ámbito de la vida privada es aquel donde el individuo actúa como parte de una pequeña unidad (familia, círculo de amigos), que reclama y esté preparada, como dice Westin, para

[49] González Gaitano, Norberto. El deber de respeto de la intimidad en la información periodística. En: Agejas, José Ángel. "*Ética de la comunicación y de la información"*. Editorial Ariel, Barcelona, 2002, p. 163.

[50] En algunos países hispanoamericanos, como México, se emplea preferentemente el término *privacía*
[51] Real Academia Española, *Diccionario de la lengua española* , Madrid, Espasa, 2001

ejercer una segregación corporativa, permitiendo alcanzar relaciones francas, relajadas y cerradas entre dos o mas personas.

Lo privado es un ámbito no público, el cual se excluye del conocimiento público, en el que se practica un determinado tipo de relaciones interpersonales, entre ellas debe incluirse cierto tipo de relaciones profesionales, como por ejemplo, las que tiene el medico con su paciente o el abogado y su patrocinado, las que estén estrechamente vinculadas con la privacidad.

La vida privada en un círculo o ámbito mas profundo lleva al concepto de intimidad. La intimidad es el ámbito reservado del individuo que no desea ser develado al conocimiento y acción de los demás, el cual aparece como necesario para mantener un mínimo de calidad de vida humana. El derecho a la intimidad es la facultad de la persona para evitar las injerencias de terceros en el ámbito de su privacidad, salvo la autorización de tal develamiento de la intimidad por el propio afectado. El derecho a la privacidad comprende el derecho de la intimidad que tiene un carácter más estricto y dimensión individual que abarca como aspectos básicos la concepción religiosa e ideológica, la vida sexual, el estado de la salud, la intimidad corporal o pudor, entre otros.

Así precisando en el ámbito constitucional positivo chileno, el articulo 19 N° 4, asegura tres dimensiones del derecho: a) el derecho al respeto de la vida privada de las personas; b) el derecho al respeto de la vida publica de las personas; y c) el derecho al respeto de la honra de la persona y de su familia.

El respeto implica la obligación de terceras personas, sean naturales o jurídicas, públicas o privadas, en orden a no interferir en el ámbito del valor y conducta protegido jurídicamente, el cual recibe la protección del Estado a través del conjunto de garantías que brinda a tales bienes jurídicos *y a* sus titulares para defenderlos *y* exigir que ellos sean respetados.

Este respeto y protección debe desarrollarse en relación con la "vida privada" de la persona y la "vida publica" de ella.

El concepto de vida privada no fue precisado por el constituyente, es un concepto jurídico constitucional indeterminado, cuya delimitación y configuración quedó entregado a la doctrina y jurisprudencia, sin perjuicio de las configuraciones que haga el legislador.

Sin perjuicio de las reflexiones ya hechas en esta materia, consideramos adecuada la conceptualización de vida privada que nos entrega Espin Templado, para el cual vida

privada "es el conjunto de circunstancias y datos relativos a la vida de una persona que quedan fuera del conocimiento de los demás, salvo que medie un expreso deseo de comunicarlo o de ponerlo de manifiesto por parte de la persona afectada y al margen, naturalmente, de las personas que comparten con ellos aspectos más o menos amplios de su vida[52]

3) Situación Jurídica del derecho a la privacidad en la Legislación Nacional

Para analizar este punto y considerando lo expuesto, sobre todo lo relativo a la confusión de significados entre intimidad y privacidad, debemos observar las normas relativas a este "derecho a estar solo", desde la óptica de las normas constitucionales, normas legales y referencia a tratados internacionales.

- **NORMAS CONSTITUCIONALES**

La norma básica en materia de privacidad se encuentra en el artículo 19 de la Constitución Política de la República de 1980, que establece:
"La Constitución asegura a todas las personas:
N° 4: El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia;

En su inciso segundo dispone que la infracción a este precepto, cometida a través de un medio de comunicación social, y que consistiere en la imputación de un hecho o acto falso, o que cause injustificadamente daño o descrédito a una persona o a su familia, será constitutiva de delito y tendrá la sanción que determine la ley.

Con todo, agrega la disposición, el medio de comunicación social podrá excepcionarse probando ante el tribunal correspondiente la verdad de la imputación, a menos que ella constituya por sí misma el delito de injuria a particulares. Además, concluye, los propietarios, editores, directores y administradores del medio de comunicación social respectivo serán solidariamente responsables de las indemnizaciones que procedan.

[52] Espin Templado, Eduardo, "Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio", *Revista del Centro de Estudios Constituconal* , Madrid, Espana, 1991, p. 45.

N° 5: La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse, en los casos y formas determinados por la ley".

Un punto debatido en la Comisión que elaboró estas disposiciones fue la de precisar el alcance del concepto "hogar", que no sólo debía comprender la morada de la persona, sino también la oficina o el lugar donde ejerce la persona su trabajo o cualquier otra actividad. La idea que se persigue es garantizar que la persona sea respetada en sus actividades básicas y donde está iniciando su acción exterior o desarrollando sus actividades más personales.

En cuanto a la inviolabilidad que se pretendía consagrar, ésta debía comprender todo lugar privado, con especial énfasis en el hogar y sus extensiones naturales, a fin de preservarlos de toda invasión externa. Se pretendió establecer, entonces, una inviolabilidad más amplia, que cubriera todo recinto respecto del cual recayera el derecho de propiedad.

Se acordó en definitiva que el término "hogar" comprende la casa-habitación, la oficina, y todo lugar cerrado, sea de propiedad o de quien lo ocupa y posee, aunque no haya actividad vital actual en él. Y lo que se ampara bajo la inviolabilidad del hogar es cualquier recinto, lugar o espacio, aunque dentro de él no se desarrolle una expresión de privacidad.

Otra garantía importante y vinculada con la vida privada de las personas es la relativa al secreto de la correspondencia y de las comunicaciones. Se optó por la expresión comunicaciones privadas que cubriría todo acto comunicacional que no fuera público. Lo que se pretendía, a fin de cuentas, era que la Constitución protegiera la vida privada y la honra de las personas y familias, y del mismo modo, el hogar y las comunicaciones personales entre los individuos, aunque estos dos ámbitos se refieren a garantías diferentes, que debían quedar comprendidas en normas diversas.

La primera se relaciona con protecciones de orden material (hogar y correspondencia), y la segunda garantizaba valores de orden moral o espiritual (privacidad y honra).

La jurisprudencia de los tribunales superiores de justicia ha asegurado y protegido el derecho a la inviolabilidad del hogar y de toda forma de comunicación privada en distintos ámbitos o facetas del derecho. En efecto, la Corte Suprema de Justicia ha determinado la estricta reserva que deben guardar los bancos de los

instrumentos en que consten "la existencia del contrato de cuenta corriente, los depósitos, giros y demás operaciones que le son propias, las que deben asimilarse a la garantía de inviolabilidad contemplada en el N° 5 del articulo 19 de la Constitución Política y cuyo "registro" solo se permite en los casos y formas determinados por la ley" (Rol N° 13.087 de fecha 19 de enero de 1988).

Por otro lado, la citación por el Servicio de Impuestos Internos al gerente de una institución bancaria para que concurra al Departamento de Investigación Tributaria con la fotocopia y documentación correspondiente a la cuenta de ahorro del recurrente, perturba la garantía constitucional de la inviolabilidad de las comunicaciones y documentos privados (Corte Suprema, fallo del 5 de octubre de 1981, Revista Fallos del Mes n° 275, p. 419).

Esta garantía establecida en el nº 5 debe contrastarse con aquella que es propia del derecho a la información, establecida en el artículo 19 N° 12:

La libertad de emitir opinión y la de informar, sin censura previa, en cualquier forma y por cualquier medio, sin perjuicio de responder de los delitos y abusos que se cometan en el ejercicio de estas libertades, en conformidad a la ley, la que deberá ser de quórum calificado.

También debe considerarse como una protección, entre otros derechos, a la vida privada, la norma que consagra el derecho a rectificación, en el mismo artículo 19 N° 12:

Toda persona natural o jurídica ofendida o injustamente aludida por algún medio de comunicación social, tiene derecho a que su declaración o rectificación sea gratuitamente difundida, en las condiciones que la ley determine, por el medio de comunicación social en que esa información hubiera sido emitida.

- **NORMAS LEGALES**

Dentro de la legislación nacional encontramos numerosas normas referidas a la protección de la privacidad, en diversos cuerpos normativos, ya sea dentro de códigos, regulación a través de leyes especiales hasta en decretos.

Para dar algunos ejemplos de regulación, verificaremos el ámbito de aplicación de las referidas normas, a saber:

- A fin de hacer efectivo el precepto constitucional sobre la privacidad del domicilio y a la protección de las comunicaciones:

El Código Penal sanciona las conductas que atentan contra dicha garantía en los siguientes artículos:

Artículo 144: El que entrare en morada ajena contra la voluntad de su morador, será castigado con reclusión menor en su grado mínimo o multa de seis a diez unidades tributarias mensuales.
Si el hecho se ejecutare con violencia o intimidación, el tribunal podrá aplicar la reclusión menor hasta en su grado medio y elevar la multa hasta quince unidades tributarias mensuales.

Artículo 145: La disposición del artículo anterior no es aplicable al que entra en la morada ajena para evitar un mal grave a sí mismo, a los moradores o a un tercero, ni al que lo hace para prestar algún auxilio a la humanidad o a la justicia.

Tampoco tiene aplicación respecto de los cafés, tabernas, posadas y demás casas públicas, mientras estuvieren abiertos y no se usare de violencia inmotivada.

Artículo 155: El empleado público que abusando de su oficio, allanare un templo o la casa de cualquiera persona, o hiciere registro en sus papeles, a no ser en los casos y forma en que prescriben las leyes, será castigado con la pena de reclusión menor en sus grados mínimo a medio o con la suspensión en cualquiera de sus grados.
Violación de correspondencia y comunicaciones privadas

Artículo 146: El que abriere o registrare la correspondencia o los papeles de otro sin su voluntad, sufrirá la pena de reclusión menor en su grado medio si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en su grado mínimo.

Artículo 156: Los empleados en el servicio de correos y telégrafos u otros que valiéndose de su autoridad interceptaren o abrieren la correspondencia o facilitaren a terceros su apertura o supresión, sufrirán la pena de reclusión menor en su grado

mínimo y, si se aprovecharen de los secretos que contienen o los divulgaren, las penas serán reclusión menor en cualquiera de sus grados y multa de 11 a 20 Unidades Tributarias Mensuales.

Artículo 337: El empleado de una oficina telegráfica que divulgare el contenido de un mensaje sin autorización expresa de la persona que lo dirige o a quien es dirigido, incurrirá en una multa de seis a diez Unidades Tributarias Mensuales, y deberá indemnizar los perjuicios provenientes de la divulgación.
Las mismas penas se impondrán al empleado que, por descuido culpable, no transmitiere fielmente un mensaje telegráfico y, si en la transmisión infiel hubiere mala fe, se estará a lo dispuesto en el artículo 195.

El artículo 161-A del Código Penal, agregado por la ley N° 19.423 de noviembre de 1995, por otro lado señala:

Se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500 Unidades Tributarias Mensuales al que, en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado, sustraiga, fotografíe, fotocopie o reproduzca documentos o instrumentos de carácter privado, o capte, grabe, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público.

Igual pena se aplicará a quien difunda las conversaciones, comunicaciones, documentos, instrumentos, imágenes y hechos a que se refiere el inciso anterior.

En caso de ser una misma la persona que los haya obtenido y divulgado, se aplicarán a ésta las penas de reclusión menor en su grado máximo y multa de 100 a 500 Unidades Tributarias Mensuales.

Esta disposición no es aplicable a aquellas personas que, en virtud de ley o de autorización judicial, estén o sean autorizadas para ejecutar las acciones descritas

- En cuanto a lo relativo a la vida doméstica

El Código Civil en sus artículos 844, 874, 875 y 878 demuestran su propósito protector de la vida privada.

En efecto, la primera de dichas disposiciones faculta al dueño de un predio para cercarlo o cercarlo por todas partes, mientras que las restantes, que se refieren a las servidumbres de luz y vista, persiguen evitar las molestias causadas por miradas indiscretas.

- En relación a las acciones de filiación y la adopción:

Dentro del mismo cuerpo legal del Código Civil, tenemos que la ley faculta según el artículo 195 la investigación de la paternidad.

Sin embargo, y en lo relativo a la privacidad, el artículo 197 del cuerpo legal citado prescribe que el proceso respectivo tiene el carácter de secreto hasta la dictación de la sentencia de término, teniendo acceso a él solo las partes y sus apoderados judiciales.

Al verificar la institución de la adopción también se inserta dentro del ámbito de la intimidad familiar. Así es como conforme a lo prevenido en el artículo 35 de la ley 18.703, sobre adopción de menores, todas las tramitaciones, judiciales y administrativas y la guardas de documentos a que de lugar la adopción son reservados, salvo que los solicitantes, en su demanda de adopción, hayan manifestado lo contrario, en cuyo caso se dejará testimonio de ello en la sentencia.

- En cuanto a la situación económica personal

Se discute en la doctrina si la situación económica de una persona integra o no el contenido del derecho a la intimidad.

Estimamos que la situación económica personal y los aspectos que ella incluye: nivel de ingreso, patrimonio, inversiones, etc., deben entenderse comprendidas dentro de la vida privada.

De otro modo, la intromisión y divulgación maliciosa de datos personales que den cuenta de una mala situación económica o financiera, puede causar grave daño personal, familiar y profesional, efecto que se vera agravado si la situación es incorrecta o no actualizada.

Sobre el particular, atendido el cuantioso volumen de información que sobre esta materia maneja el Servicio de Impuestos Internos, en el articulo 35 del Código Tributario se prohibe al Director y demás funcionarios del Servicio divulgar, en forma alguna, la cuantía o fuente de las ventas de los contribuyentes, ni las perdidas, gastos o cualesquiera datos relativos a ellas que figuren en las declaraciones obligatorias.

En lo relativo a la información financiera y económica contenida en las operaciones bancarias, antes de la entrada en vigencia de la ley Nº 18.576, la costumbre mercantil que, con-forme al articulo 4° del Código del Ramo, tiene fuerza de ley, hacia regir entre nosotros el denominado secreto bancario, que se traducía en que las diversas operaciones efectuadas con las instituciones bancarias debían ser manejadas por estas con total reserva respecto de terceros, no obstante que en forma expresa el secreto solo se contemplaba en relación con las cuentas corrientes bancarias.

- En relación al proceso civil

Tenemos algunas normas vinculadas con la publicidad de la tramitación del respectivo proceso como por ejemplo en la contenida en el articulo 34 del Código de Procedimiento Civil, ubicada entre las disposiciones comunes a todo procedimiento, por lo tanto, de aplicación supletoria general, en virtud de la cual todas las piezas que deben formar el proceso, entendido este en su expresi6n material de expediente, deben agregarse a el conforme al orden de su presentación. Sin embargo, se exceptúan de tal agregación aquellas que por su naturaleza no pueden agregarse y las que por motivos fundados se manden reservar por el juez fuera del expediente. Piénsese por ejemplo en fotografías o cintas de video que puedan comprometer la reputación personal o familiar de una de las partes del proceso.

Por otro lado el artículo 349 del mismo Código, que contempla como mecanismo probatorio la exhibición de documentos solicitada por una de las partes y que existan en poder de la contraparte o de un tercero, la que es improcedente si dichos documentos tienen el carácter de secretos o confidenciales.

- En el ámbito económico y financiero

La Ley 19.812 prohíbe la comunicación de datos relativos a obligaciones extinguidas por algún medio legal o que, estando impagas, su monto por capital sea inferior a

$2.000.000.

También obliga a los responsables de registros o bancos de datos personales que comunican información financiera a eliminar todos los datos referentes a créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios.

Dispone también la eliminación, desde los registros históricos de obligaciones financieras, de los datos sobre créditos concedidos para la instalación de establecimientos por cuenta propia de chilenos retornados al país que hayan optado a los beneficios de la Ley 19.740, una vez aclarada la morosidad y previa solicitud del interesado.

- En el ámbito sanitario

El art. 24 de la Ley 19.628 modificó al artículo 127 del Código Sanitario estableciendo:

"Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relaciona-dos con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su con-tenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo. Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos.".

- En materia laboral

La Ley 19.812 introdujo un nuevo inciso sexto al artículo 2 del Código del Trabajo dice:

“ningún empleador podrá condicionar la contratación de trabajadores a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial que, conforme a la ley, puedan ser comunicadas por los responsables de registros o bancos de datos personales; ni exigir para dicho fin declaración ni certificado alguno. Exceptúanse solamente los trabajadores que tengan poder para representar al empleador, tales

como gerentes, subgerentes, agentes o apoderados, siempre que, en todos estos casos, estén dotados, a lo me-nos, de facultades generales de administración; y los trabajadores que tengan a su cargo la recaudación, administración o custodia de fondos o valores de cualquier naturaleza."

Luego la Ley 19.759 de 5 de octubre de 2001 agrega el siguiente primer inciso al art. 5 del Código del Trabajo:

"El ejercicio de las facultades que la ley le reconoce al empleador tiene como límite el respeto a las garantías constitucionales de los trabajadores, en especial cuando pudieran afectar la intimidad, la vida privada o la honra de estos."

En base a esta última norma, la Dirección del Trabajo emitió un Oficio Ordinario 0260/0019 de 24 de enero de 2002, determinando que el empleador puede regular las condiciones, frecuencia y oportunidad del uso de los correos electrónicos de la empresa, pero en ningún caso podrá imponerse del contenido de los correos electrónicos del trabajador.

- Lo relativo a la privacidad en leyes especiales:

1) Ley 16.346, sobre abusos de publicidad:

El artículo 24 establece ciertas limitaciones a la libertad de información. Así es como prohíbe, bajo sanción de multa, la divulgación por cualquier medio de difusión de la identidad o de cualquier otro antecedente que conduzca a ella, de menores de 18 anos de edad, ya sean autores, cómplices o encubridores o victimas de delitos.
Asimismo, de acuerdo al articulo 25, los tribunales pueden prohibir, bajo sanción de pena privativa de libertad, la divulgación por cualquier medio de difusión, informaciones concernientes a determinados juicios de que conozcan.

2) DFL 1, 18 de octubre de 1995 sobre estupefacientes y sustancias sicotrópicas:

El artículo 33 A menciona medidas tendientes a proteger la identidad de determinadas personas señalando que "…para proteger la identidad de los que intervengan en el

procedimiento, su domicilio, profesión y lugar de trabajo, el fiscal podrá aplicar todas o alguna de las siguientes medidas:
a) que no conste en los registros de las diligencias que se practiquen sus nombres, apellidos, profesión u oficio, domicilio, lugar de trabajo, ni cualquier otro dato que pudiera servir para su identificación…"

3) Ley Nº 19.733, la llamada Ley de prensa:

En el artículo 30 a propósito del delito de injuria se señala: "Se considerarán como pertinentes a la esfera privada de las personas los hechos relativos a su vida sexual, conyugal, familiar o doméstica, salvo que ellos fueren constitutivos de delito."
La anterior Ley de abusos de publicidad establecía en su artículo 22 ciertas circunstancias o actividades que no debían ser considerados como relativos a la vida privada o familiar. Esta norma se derogó, y se dejó pendiente para volver a reestablecerla, lo que hasta el momento no se ha hecho.

4) Ley N° 18.168 sobre telecomunicaciones:

El artículo 36 B letra b) señala sanciones para los que incurran en situaciones que atenten contra la privacidad. Las hipótesis de acción son el que "maliciosamente interfiera, intercepte o interrumpa un servicio de telecomunicaciones...", como asimismo "el que intercepte o capte maliciosamente o grabe sin la debida autorización, cualquier tipo de señal que se emita a través de un servicio público de telecomunicaciones..." y "la difusión pública o privada de cualquier comunicación obtenida con infracción a lo establecido en la letra precedente.."

5) Ley 19.628 sobre Protección de la vida privada en lo concerniente a datos personales.

El artículo 1º nos señala que "El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley…"

Esta ley regula el tratamiento de los datos personales, otorgando derechos a los titulares de datos, la utilización de los mismos y las responsabilidades por infracciones a la ley. Sin embargo, la protección que reconoce la ley 19.628 se circunscribe al "dato" y

no se extiende, -como lo sugiere equivocadamente el título de la ley, a una protección absoluta de la vida privada, expresión más amplia que escapa al contenido de ella-, para que este no sea tratado y convertido en información, sino para aquellos fines y personas autorizadas para ello. La ley constituye un límite a la informática para precaver una posible lesión a la intimidad de las personas coartando de esta manera el ejercicio legítimo del derecho[53].

- **TRATADOS INTERNACIONALES**

El fundamento de la garantía constitucional referida a la privacidad tiene sus antecedentes en el derecho positivo, específicamente, en la "Declaración de Derechos del Hombre y del Ciudadano" en Francia, en 1789. No obstante, ha ejercido una mayor influencia en nuestra legislación la "Declaración Americana de los Derechos y Deberes del Hombre", aprobada por la IX Conferencia Internacional Americana de Bogotá el 2 de mayo de 1948. En su artículo 5, la Declaración dispone que "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

Poco tiempo después, el derecho a la privacidad apareció nuevamente proclamado en el plano internacional, en la "Declaración Universal de Derechos del Hombre", aprobada por la Asamblea General de Las Naciones Unidas, reunida en París el 10 de diciembre de 1948. En su artículo 13 se establece que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Posteriormente, en 1950, la "Convención Europea de Derechos del Hombre", firmada en Roma el 4 de noviembre, agrega en forma más detallada que "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia".

El mérito de este precepto está en que propone expresamente el respeto de la vida privada como un derecho específico y autónomo, lo que solamente era inferible en otros textos.

[53] A nuestro entender esta es una de las principales leyes relativas a la privacidad y a las Tecnologías de la Información y las Comunicaciones, es por ello que le daremos un tratamiento y análisis íntegro en el capítulo IV de esta memoria, llamada "Protección Civil".

En el “Pacto Internacional sobre Derechos Civiles y Políticos” aprobado por la Asamblea General de la ONU en su XXI sesión del 16 de diciembre de 1966, volvió a reiterarse la existencia del derecho a la privacidad.

En ese Pacto se estableció que el derecho a la libertades de expresión supone deberes y responsabilidades, sujetos a restricciones fijadas por la ley, para asegurar el respeto a los derechos y a la reputación de los demás.

Luego, en la “Convención Americana de Derechos Humanos” firmada en 1969 en Bogotá, Colombia, se establece la protección de la honra de las personas, que se extiende incluso, hasta después de fallecidas. No obstante, esta convención habla confusamente de la vida familiar, del domicilio y de la correspondencia, como si se tratara de algo diferente de la vida privada, y enlaza a ésta última con el derecho al honor.

La “Convención Americana de Derechos Humanos” firmada en San José de Costa Rica, ratificó en el artículo 13 las responsabilidades ulteriores de la libertad de expresión, en lo referido al respeto a los derechos y a la reputación de los demás. En su artículo 14 se agregó una disposición relativa a una materia que no había sido abordada por las anteriores convenciones internacionales. Ella dispone que las empresas periodísticas deban crear una figura responsable que no esté protegida por inmunidades de fuero especial, para que se haga cargo de los delitos y transgresiones que afecten la honra y reputación de las personas.

También se establece el derecho de toda persona afectada por una información inexacta o agraviante en su perjuicio emitida en un medio de difusión, a efectuar en el mismo órgano su rectificación o respuesta en las condiciones que indique la ley. Dicha rectificación no eximirá de las demás responsabilidades legales que le caben.

En cuanto a los límites al derecho a la vida privada en los documentos internacionales, es un valor entendido en la sociedad occidental que no hay derechos absolutos. Todos los derechos de una persona quedan sometidos a ciertos límites y restricciones, necesarias e indispensables para una armónica convivencia entre los miembros de una comunidad. El derecho a la información no escapa a esta situación, como se comprueba en los documentos internacionales.

En la Declaración Universal de los Derechos Humanos no se prevé ninguna limitación específica para el derecho a la vida privada. En la parte final de la declaración, en los puntos segundo y tercero del artículo 29, se encuentran reglas que

marcan límites generales para el ejercicio de todos los derechos y libertades que enuncia. Las limitaciones propuestas son de dos órdenes. Uno, relativo a la restricción que impone todo derecho individual: los derechos y libertades de los demás (el derecho a la información, entre otros). Otro, la primacía que sobre los derechos individuales corresponde al interés público, en cuanto signifique lo que impone por exigencias de la moral, del orden público y del bienestar colectivo.

El Pacto internacional de Derechos Civiles y Políticos en su artículo 5 señala que "ninguna disposición del presente Pacto podrá ser interpretada en el sentido de conceder derecho alguno a un Estado, grupo o individuo para emprender actividades o realizar actos encaminados a la destrucción de cualquiera de los derechos y libertades reconocidos en el Pacto o a su limitación en mayor medida que la prevista por él".

Después, de revisar las limitaciones, que de una manera u otra, se le reconocen al derecho a la vida privada, podemos resumirla de la siguiente manera:

a) Limitaciones de orden personal, que se aplican en el caso de las personas célebres o notorias, en virtud de la condición o calidad que revistan.

b) Limitaciones generales, que no fundándose en el carácter que revisten las personas en cuestión, se aplican sin consideración a los sujetos concretos.

Estas, a su vez, pueden agruparse en las siguientes categorías:

a. La Seguridad del Estado: la defensa de la estabilidad y seguridad justifica que en algunas situaciones se limite el derecho a la intimidad de los particulares.

El fundamento de esta limitación residiría en el interés superior por la conservación de la comunidad políticamente organizada. La protección de la seguridad del Estado no se limita a estados de guerra o catástrofe, sino que también se extiende al resguardo del orden público, la paz social, la prevención y represión de los delitos y de todo aquello que se relacione con las bases mismas del Estado.

b. El bienestar e interés general: la protección de la moral pública y de las buenas costumbres justifica ciertas intromisiones del Estado o agentes particulares en la vida privada de la persona.

c. El legítimo ejercicio de derechos por parte de terceros: el ejercicio regular del derecho a intervenir en la vida privada de los demás no puede originar obligación

alguna de indemnizar, ni puede disponer el cese de los actos que, aunque interfieran en la vida privada, respondan a la ejecución normal de alguna facultad.

No es fácil dar con una fórmula general que fije con precisión los límites del derecho a la intimidad y a la vida privada y los llamados a decidir cuál de ellos deberá ceder en favor del otro, atendiendo a las circunstancias.

Ahora bien, se indicó ya que la garantía del derecho a la privacidad tiene sus antecedentes jurídicos en diversos pactos internacionales, que sirven como marco de referencia doctrinal. Sin embargo, parte de esa legislación internacional debe considerarse como integrante del ordenamiento constitucional chileno, como normas obligatorias, según la opinión de algunos autores.

El artículo 5º de la Constitución declara que el ejercicio de la soberanía reconoce como limitación el respeto a los derechos esenciales que emanan de la naturaleza humana. Agrega que es deber de los órganos del Estado respetar y promover tales derechos, garantizados por esta Constitución, así como por los tratados internacionales ratificados por Chile y que se encuentren vigentes.

De manera que las normas constitucionales deben ser complementadas con las que se refieren a este mismo tema, contenidas en tratados internacionales, siempre que hayan sido ratificados por Chile y que se encuentren vigentes.

El Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de las Naciones Unidas en 1966, y que entró en vigencia en Chile en abril de 1989 dispone:

a) Regla general: está contenida en el artículo 17:

1. Nadie será objeto de injerencia arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

b) Privacidad en los juicios: el artículo 14 establece como regla general la publicidad de los procesos judiciales, al señalar que

Toda persona tendrá derecho a ser oída públicamente y con las debidas garantías por un tribunal competente, independiente e imparcial, establecido por la ley, en la substanciación de cualquier acusación de carácter penal formulada contra ella o para la determinación de sus derechos u obligaciones de carácter civil.

Sin embargo, a continuación prescribe que:

La prensa y el público podrán ser excluidos de la totalidad o parte de los juicios por consideraciones de moral, orden público o seguridad nacional en una sociedad democrática, o cuando lo exija el interés de la vida privada de las partes...

Esta excepción no se extiende a las sentencias, ya que toda sentencia en materia penal o contenciosa será publicada, excepto en los casos en que el interés de menores de edad exijan lo contrario, o en las actuaciones referentes a pleitos matrimoniales o a la tutela de menores.

c) Libertad de manifestación religiosa en el ámbito público y privado:
Artículo 18:
1. Toda persona tiene derecho a la libertad de pensamiento, de conciencia y de religión; este derecho incluye la libertad de tener o de adoptar la religión a la creencia de su elección, así como la libertad de manifestar su religión o creencias, individual o colectivamente, tanto en público como en privado, mediante el culto, la celebración de los ritos, las prácticas y la enseñanza.

d) También consagra este Pacto, en el artículo 19, la libertad de opinión y de expresión. Respecto de esta última, previene que su ejercicio entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;
b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas,
Son aplicables también las normas contenidas en la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), que en sus artículos pertinentes dispone:
Artículo 11: Protección de la Honra y de la Dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.
Artículo 13: Libertad de Pensamiento y de Expresión
1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.
2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:
a) el respeto a los derechos o a la reputación de los demás...

Por tanto estas normas podríamos considerarlas complementarias y con un rango constitucional, aplicando las herramientas de protección que otorga el ordenamiento jurídico, tal como la interposición de recursos de protección y de amparo, cuando así lo ameriten las circunstancias

- Situación Jurídica del derecho a la privacidad en la Legislación Extranjera en el ámbito constitucional

A continuación verificaremos el sentido y contenido de la protección que se realiza en las constituciones contemporáneas de distintos países y podremos observar como a nivel de una máxima norma legal, se identifica y regula el llamado derecho a la privacidad.

ALEMANIA

Art. 10.

1. Será inviolable el secreto de la correspondencia, así como el del correo y los telégrafos.
2. Solo en virtud de una ley podrán establecerse limitaciones a este derecho. Si la restricción obedece al propósito de proteger el orden básico liberal y democrático o la existencia o salvaguardia de la Federación o de un Estado regional, podrá la ley disponer que no se comunique la restricción al afectado y que el control sea asumido por órganos y auxiliares designados por la representación del pueblo, en vez de correr a cargo de la autoridad judicial.

Art. 13.

1. El domicilio será inviolable.

2. Los registros solo podrán ser ordenados por la autoridad judicial y, cuando sea peligroso demorarlos, por los demás órganos previstos en las leyes y únicamente podrán realizarse en la forma establecida.

3. Por lo demás, solo podrán adaptarse intervenciones y limitaciones para la prevención de un peligro común o de un peligro de muerte para personas determinadas y en virtud de una ley también para la salvaguardia contra peligros que amenacen directamente la seguridad y el orden públicos, especialmente para subsanar la escasez de viviendas, combatir el riesgo de epidemias y proteger a los menores en peligro.

ARGENTINA

Art. 18. Ningún habitante de la Nación puede ser penado sin juicio previo fundado en ley anterior al hecho del proceso, ni juzgado por comisiones especiales, o sacado de los jueces designados por la ley antes del hecho de la causa. Nadie puede ser obligado a declarar contra si mismo; ni arrestado sino en virtud de orden escrita de autoridad competente. Es inviolable la defensa en juicio de la persona y de los derechos. El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; *y* una ley determinara en que casos *y* con que justificativos podrá procederse a su allanamiento y ocupación. Quedan abolidos para siempre la pena de muerte por causas políticas, toda especie de tormento y los azotes. Las cárceles de la nación serán sanas *y* limpias, para seguridad *y* no para castigo de los reos detenidos en ellas, *y* toda medida que a pretexto de precaución conduzca a modificarlos mas allá de los que aquella exija, hará responsable al juez que la autorice.

Art. 19. Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral publica, ni perjudiquen a un tercero, estén solo reservadas a Dios, y exentas de las 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.

BRASIL

Art. 5°. Todos son iguales ante la ley, sin distinción de cualquier naturaleza, garantizándose a los brasileños y a los extranjeros residentes en el país la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los siguientes términos:

X. Son inviolables la intimidad, la vida privada, el honor y la imagen de las personas, asegurándose el derecho a indemnización por el daño material o moral derivado de su violación;

XI. La casa es asilo inviolable del individuo, no pudiendo penetrar nadie en ella sin consentimiento del morador, salvo en caso de flagrante delito o desastre, o para prestar socorro, o, durante el día, por determinación judicial;

XII. Es inviolable el secreto de la correspondencia, de las comunicaciones telegráficas, de las informaciones y de las comunicaciones telefónicas, salvo, en el ultimo caso, por orden judicial, en las hipótesis yen la forma que la ley establezca para fines de investigación criminal o instrucción procesal penal;

LXXII. Se concederá el Habeas *data*

a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten registros o bancos de datos de entidades gubernamentales o de carácter publico;

b) Para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo;(...).

COLOMBIA

Art. 15. Todas las personas tienen derecho a su intimidad personal *y* familiar *y a* su buen nombre, *y* el Estado debe respetarlos *y* hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos *y* en archivos de entidades públicas *y* privadas.

En la recolección, tratamiento *y* circulación de datos se respetaran la libertad *y* demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Solo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

Con el fin de prevenir la comisión de actos terroristas, una ley estatutaria reglamentará la forma y condiciones en que las autoridades que ella señale, con fundamento en serios motivos, puedan interceptar o registrar la correspondencia y demás formas de comunicación privada, sin previa orden judicial, con aviso Inmediato a la Procuraduría General de la Nación y control judicial posterior dentro de las treinta y seis (36) horas siguientes. Al iniciar cada período de sesiones el Gobierno rendirá informe al Congreso sobre el uso que se haya hecho de esta facultad. Los funcionarios que abusen de las medidas a que se refiere este artículo incurrirán en falta gravísima, sin perjuicio de las demás responsabilidades a que hubiere lugar.

Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley"

COSTA RICA

Art. 23. El domicilio y todo otro recinto privado de los habitantes de la Republica son inviolables. No obstante pueden ser allanados por orden escrita de juez competente, o para impedir la comisión o impunidad de delitos, o evitar daños graves a la propiedad, con sujeción a lo que prescribe la ley.

Art. 24. Son inviolables los documentos privados, las comunicaciones escritas u orales de los habitantes de la Republica. Sin embargo, la ley fijara los casos en que los tribunales de justicia podrán ordenar el secuestro, registro o examen de documentos privados, cuando ello sea absolutamente indispensable para esclarecer asuntos sometidos a su conocimiento.

ECUADOR

El numeral 8 del artículo 23 de la Constitución garantiza la intimidad personal y familiar.

Su numeral 21 del artículo 23 prohíbe la utilización de la información personal de terceros referentes a sus creencias religiosas, filiación política ni sus datos sobre salud y vida sexual.

El artículo 94 de la Constitución de 1998 dispone lo siguiente:

"Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito"

"Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.

"Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización

"La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional"

EL SALVADOR

No existe previsión expresa, aunque el artículo 2 de la Constitución establece en su inciso segundo que se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

ESPANA

Art. 18.1. Se garantiza el derecho al honor, a la intimidad personal y familiar, a la propia imagen.

2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

Se garantiza el secreto de las comunicaciones y en especial de las postales, telegráficas y telefónicas, salvo resolución judicial.

3. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal *y* familiar de los ciudadanos *y* el pleno ejercicio de sus derechos.

ESTADOS UNIDOS

Enmienda 3. En tiempo de paz, ningún soldado deberá alojarse en una casa sin el consentimiento del propietario; ni en tiempo de guerra, pero de conformidad con que la ley prescriba.

Enmienda 4. El derecho de la población a la seguridad en sus personas, sus documentos *y* efectos, contra incautaciones *y* cateos arbitrarios no deberá ser violado, y no habrán de expedirse las Ordenes correspondientes si no existe una causa probable, apoyada por juramento o declaración solemne, que describa en particular el lugar que habrá de ser inspeccionado y las personas o cosas que serán objeto de detención o decomiso.

Enmienda 5. Ninguna persona podrá ser detenida para que responda por un delito capital o infamante por algún otro concepto, sin auto de denuncia o acusación formulado por un Gran Jurado, salvo en los casos que se presenten en las fuerzas terrestres o navales, o en la Milicia, cuando estas estén en servicio efectivo en tiempo guerra o de peligro publico; (...)

Enmienda 9. El hecho de que en la Constitución se enumeren ciertos derechos no deberá interpretarse como una negación o menosprecio hacia otros derechos que también son prerrogativas del pueblo.

ITALIA

Art. 14. El domicilio es inviolable. No se podrán efectuar inspecciones o registros ni embargos salvo en los casos y con las modalidades establecidas por la ley, y conforme a las garantías prescritas para la salvaguardia de la libertad personal. Se regularan por leyes especiales las comprobaciones e inspecciones por motivos de sanidad *y* de salubridad públicas o con fines económicos *y* fiscales.

Art. 15. Serán inviolables la libertad *y* el secreto de la correspondencia *y* de cualquier otra forma de comunicación.

La limitación de los mismos solo podrá producirse por auto motivado de la autoridad judicial con las garantías establecidas por la ley.

MEXICO

Art.16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

En toda orden de cateo, que solo la autoridad judicial podrá expedir, y que será escrita, se expresara el lugar que ha de inspeccionarse, la persona o personas que hayan de aprehenderse y los objetos que se buscan, a lo que únicamente debe limitarse la diligencia, levantándose, al concluirla, un acta circunstanciada, en presencia de dos testigos propuestos por el ocupante del lugar cateado o, en su ausencia o negativa, por la autoridad que practique la diligencia.

Las comunicaciones privadas son inviolables. La ley sancionara penalmente cualquier acto que atente contra la libertad y privada de las mismas. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal, que faculte la ley o del titular del Ministerio Publico de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente, por escrito, deberá fundar y motivar las causas legales de la solicitud expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Las intervenciones autorizadas se ajustaran a los requisitos y limites previstos en las leyes. Los resultados de las intervenciones que no cumplan con estos, carecerán de todo valor probatorio.

La autoridad administrativa podrá practicar visitas domiciliarias únicamente para cerciorarse de que se han cumplido los reglamentos sanitarios *y* de policía; *y* exigir la exhibición de los libros y papeles indispensables para comprobar que se han acatado las disposiciones fiscales, sujetándose, en estos casos, a las leyes respectivas y a las formalidades prescritas para los cateos.

La correspondencia que bajo cubierta circule por las estafetas, estará libre de todo registro, y su violación será penada por la ley.

En tiempo de paz ningún miembro del Ejército podrá alojarse en casa particular contra la voluntad del dueño, ni imponer prestación alguna. En tiempo de guerra los militares podrán exigir alojamiento, bagajes, alimentos y otras prestaciones, en los términos que establezca la ley marcial correspondiente.

NICARAGUA

"Artº. 5 Son principios de la nación nicaragüense: la libertad; la justicia; el respeto a la dignidad de la persona humana; el pluralismo político, social y étnico; el reconocimiento a las distintas formas de propiedad; la libre cooperación internacional; y el respeto a la libre autodeterminación de los pueblos.

Las diferentes formas de propiedad pública, privada, asociativa, cooperativa y comunitaria deberán ser garantizadas y estimuladas sin discriminación para producir riquezas, y todas ellas dentro de su libre funcionamiento deberán cumplir una función social".

"Artº. 26 Toda persona tiene derecho:

A su vida privada y a la de su familia.

A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo.

Al respeto de su honra y reputación.

A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información".

PERU

Art. 2. Toda persona tiene derecho:

7. AI honor *y a* la buena reputación, a la intimidad personal *y* familiar así como a la voz y a la imagen propia.

Toda persona afectada por afirmaciones inexactas o agraviadas en cualquier medio de comunicación social tiene derecho a que este se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.

9. A la inviolabilidad del domicilio. Nadie puede ingresar en el ni efectuar investigaciones o registros sin autorización de la persona que lo habita o sin mandato judicial, salvo flagrante delito o muy grave peligro de su perpetración. Las excepciones por motivos de sanidad o de grave riesgo son reguladas por la ley.

10. AI secreto *y a* la inviolabilidad de sus comunicaciones *y* documentos privados. Las comunicaciones, telecomunicaciones o sus instrumentos solo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las

garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen.

Los documentos privados obtenidos con violación de este precepto no tienen efecto legal.

Los libros, comprobantes *y* documentos contables *y* administrativos están sujetos a inspección o fiscalización de la autoridad competente, de conformidad con la ley. Las acciones que al respecto se tomen no pueden incluir su sustracción o incautación salvo por orden judicial.

PORTUGAL

Art. 26 (otros derechos personales)

1.- A todos se les reconoce el derecho a la identidad personal, a la capacidad civil, a la ciudadanía, al buen nombre *y* reputación, a la imagen, a la palabra *y a* la reserva de la intimidad de la vida privada y familiar.

2.- La Ley establecerá garantías efectivas contra la utilización abusiva, o contraria de la dignidad humana, de informaciones relativas a las personas y familias.

3.- La privacidad de la ciudadanía y las restricciones a la capacidad civil solo pueden imponerse en los casos yen los términos previstos por la ley, no pudiendo tener como fundamento motivos políticos.

Art. 34 (inviolabilidad del domicilio y de la correspondencia)

1.- El domicilio *y* el secreto de la correspondencia *y* demás medios de comunicación privada son inviolables.

2.- La entrada en el domicilio de un ciudadano contra su voluntad solo podrá ser ordenada por la autoridad judicial competente, en los casos y según las formas previstas por la ley.

3.- Nadie podrá entrar durante la noche en el domicilio de una persona sin su consentimiento.

4.- Se prohíbe toda injerencia de las autoridades publicas en la correspondencia y en las telecomunicaciones, salvo en los casos previstos en la ley en materia de enjuiciamiento.

Art. 35 (Utilización de la informática)

1.- Todo ciudadano tendrá derecho a tener conocimiento de los datos que consten en ficheros *y* registros informáticos que le afecten *y* de la finalidad a que se destinan esos

datos, pudiendo exigir su rectificación y actualización, sin perjuicio de lo dispuesto en la ley sobre secretos de Estado y secreto de actuaciones judiciales.

2.- Se prohíbe el acceso a ficheros y registros informáticos para el conocimiento de datos personales relativos a terceros y la respectiva interconexión, salvo en casos excepcionales previstos por la ley.

3.- La informática no puede ser utilizada para el tratamiento de datos referentes a convicciones filosóficas o políticas, afiliación a partidos o a sindicatos, fe religiosa o vida privada, salvo cuando se trate del tratamiento de datos estadísticos no identificables individualmente.

4.- La ley definirá el concepto de datos personales para fines de registro informático, así como las bases *y* bancos de datos *y* las respectivas condiciones de acceso, constitución *y* utilización por entes públicos *y* privados.

5.- Se prohíbe la asignación de un número nacional único a los ciudadanos.

6.- La ley definirá el régimen aplicable a los flujos de datos a través de las fronteras, estableciendo formas adecuadas de protección de datos personales y de otros cuya salvaguardia se justifique por razones de interés nacional.

URUGUAY

Art. 10. Las acciones privadas de las personas que de ningún modo atacan el orden público ni perjudican a un tercero, estén exentas de la autoridad de los magistrados.
Ningún habitante de la Republica será obligado a hacer lo que no manda la Ley, ni privado de los que ella no prohíbe.
Art. 11. El hogar es un sagrado inviolable. De noche nadie podrá entrar en el sin consentimiento de su jefe, y de día, solo de orden expresa de un juez competente, por escrito y en los casos determinados por la Ley.
Art. 28. Los papeles de los particulares y su correspondencia epistolar telegráfica o de cualquier otra especie, son inviolables, y nunca podrá hacerse su registro, examen o interpretación sino conforme a las leyes que se establecieron por razones de interés general.

VENEZUELA

En la Constitución de la República Bolivariana de Venezuela de 1999, aparece por primera vez la protección de datos consagrada en el ordenamiento jurídico venezolano, en los siguientes términos:

Artículo 28: "Toda persona tiene el derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley".

Artículo 60: "Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación.

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos."

En cuanto al ejercicio de las acciones de habeas data, éste se encuentra atribuido al Defensor del Pueblo, según lo previsto en el Artículo 281, numeral 3, del mencionado texto constitucional:

Articulo 281: " Son atribuciones del Defensor o Defensora del Pueblo:

(…)

3. Interponer las acciones de inconstitucionalidad, amparo, hábeas corpus, habeas data y las demás acciones o recursos necesarios para ejercer las atribuciones señaladas en los numerales anteriores, cuando fuere procedente de conformidad con la ley."

4) Derecho a la Privacidad y Tecnologías de la Información y las Comunicaciones. Crossing Over.

El análisis del Derecho de la Privacidad y las Tecnologías de la Información y las Comunicaciones, por estas enmaradas dentro de dos ciencias en teoría sin puntos comunes (como es Derecho e Informática) ha comenzado a surgir tras el avance irrefrenable de la llamada Sociedad de la Información que anteriormente analizábamos.

La revolución que ha generado en la sociedad la introducción de las nuevas tecnologías de la información es hoy indiscutible. Su influjo ha sido de tal magnitud que los especialistas no han dudado en advertir que las nuevas tecnologías han producido y producirán cambios tan profundos en la sociedad, que tales progresos han dado paso a una nueva etapa de la historia de la humanidad: la de la sociedad de la información.

Esta "intromisión" de la Informática (entendida como la ciencia del tratamiento automático de la información) a quebrantado la absoluta brecha que existía entre esta ciencia y el Derecho, por cuanto a obligado a adecuar el marco normativo de carácter general que cumplía la función de constituir los cimientos de los principios informadores comunes a todo el ordenamiento jurídico a la nueva realidad existente. En torno al tema del Derecho a la Privacidad esto se ve claramente reflejado, por cuanto la aparición de los ordenadores posibilitó la creación de bases de datos que permitían reunir mucha información sobre grandes cantidades de sujetos, información que podía ser copiada y almacenada con facilidad. En una segunda etapa, la interconexión entre diversas bases de datos antes de la aparición de Internet- permitió crear perfiles completos de las personas con la información cruzada-, pudiendo conocer, entre otros aspectos, sus gustos, hábitos de consumo, ingresos, etc. Internet, como un medio que supone la utilización de ordenadores, la conexión de éstos a redes, el acceso a miles de bases de datos, constituía así una síntesis exponenciada de todas las posibilidades que la informática había facilitado de intromisión a la intimidad.

Es por esta razón que países de todo el mundo, incluido Chile, con mayor o menor rapidez, han comenzado a gestar y perfeccionar una nueva normativa que regule temas tan delicados como el derecho a la privacidad sin limitar el crecimiento de las Tecnologías de la Información que son base del desarrollo de las naciones.

Las relaciones entre el Derecho y la Informática abren el camino a variados enfoques.

Por un lado, la Informática, como ciencia del tratamiento automático de la información, ofrece técnicas avanzadas de procesamiento de la información en las distintas áreas del conocimiento y una de ellas es la información jurídica. En este sentido, la informática como herramienta, ha ayudado a modernizar algunos aspectos de la actividad jurídica y constituye el área de la Informática Jurídica.

Por otro lado, el desarrollo vertiginoso de la informática que tiene lugar en este siglo, a partir de los avances en la microelectrónica, provoca la emergencia de toda

una problemática e interrogantes, a las que la sociedad toda y dentro de ella, los juristas, deben dar respuesta. Este último campo es el del Derecho Informático.

Como dice Delpiazzo[54] , pueden distinguirse en ese término, dos acepciones: el Derecho Informático como una rama del Derecho integrada por las normas y principios que se refieren a la actividad informática y por otro, una ciencia que tiene por objeto el estudio del sector jurídico antes mencionado.

Nos parece oportuno señalar algunos ejemplos del primer enfoque, lo que al mismo tiempo, nos permitirá visualizar algunos de los temas a los que debería poder responder el Derecho Informático:

a) Para atender el llamado "flujo de datos transfrontera" o "flujo internacional de datos", o sea, la circulación de información a través de los Estados Nacionales, puede recurrirse al Derecho Internacional Público.

b) El Derecho Internacional Privado debe asumir los temas relacionados con las relaciones jurídicas implícitas en el mercado informático, que crece rápidamente y cuyos productos son de naturaleza internacional.

c) El Derecho Constitucional debe contemplar la problemática emergente del manejo automático de grandes volúmenes de información, con el peligro que implica el trasiego de datos personales con fines distintos de aquellos para los que fueron recolectados, por ejemplo, con el consiguiente posible riesgo para las garantías personales fundamentales.

d) El Derecho Administrativo ha debido enfrentar las nuevas modalidades de contratación realizadas por los Organismos públicos en áreas informáticas y el cambio cualitativo de la actividad de contralor administrativo.

e) Gran parte de los delitos contenidos en los Códigos Penales pueden transformarse en delitos informáticos si intervienen elementos informáticos. Estos y otras figuras delictivas específicas deberían ser atendidos por el Derecho Penal.

---

[54] Delpiazzo,C.. Nuevamente sobre poder y libertad informáticos, en las Primeras Jornadas Nacionales de Derecho Informático. Montevideo 1987, pág 147 y sigtes.

f) El Derecho Comercial debe afrontar nuevas formas de contratos informáticos en los que intervienen, por ejemplo el soporte lógico o "software".

g) El Derecho Procesal ha debido plantearse la admisión o no y la valoración, de los soportes y medios no tradicionales como medio de prueba, cuando se necesita su presentación en un juicio, por ejemplo.

h) El Derecho Bancario ha debido enfrentar la transferencia electrónica de fondos y el documento sin firma, así como los grandes cambios que han tenido lugar en cuanto a la intermediación financiera.

La pregunta es entonces si todos esos problemas que se acaban de mencionar, desde la perspectiva de las distintas ramas del Derecho y muchos otros de la misma índole, que paralelamente al creciente desarrollo de la informática han surgido y seguirán surgiendo, merecerían ser considerados en forma global y autónoma.

Esa forma autónoma, aunque no aislada de las otras ramas jurídicas, debido justamente al cruce entre el Derecho (en este caso el Derecho a la Privacidad) y las Tecnologías de la Información y las Comunicaciones hace nacer al llamado Derecho Informático (el cual analizaremos en el capítulo 3º de esta memoria) y que en teoría permitiría lograr una mayor profundización y esclarecimiento de los problemas.

Capitulo III Derecho Informático

"Todos los libros del mundo no contienen más información que la que se emite como vídeo a una gran ciudad americana en un año. No todos los bits tienen igual valor."
Carl Sagan

1) Informática Jurídica

Entre el Derecho y la Informática se destacan, entre otros, dos tipos de interrelaciones. Si se toma comno enfoque el aspecto netamente instrumental, se está haciendo referencia a la Informática Jurídica. Pero al considerar a la Informática como objeto del Derecho, se hace alusión al Derecho de la Informática o simplemente Derecho Informático.

La cibernética juega un papel bastante importante en estas relaciones establecidas en el párrafo anterior. Por cuanto sabemos que la cibernética es la ciencia de las ciencias y surge como necesidad de obtener una ciencia general que estudie y trate la relación de las demás ciencias.

De esta manera, tenemos a la ciencia Informática y por otro lado a la ciencia del Derecho; ambas disciplinas interrelacionadas funcionan más eficiente y eficazmente, por cuanto el Derecho en su aplicación es ayudado por la Informática, con lo que se conforma la Informática Jurídica. Pero resulta que la Informática debe estar estructurada por ciertas reglas y criterios que aseguren el cumplimiento y respeto de las pautas tecnológicas; así pues, nace el Derecho Informático como una ciencia que surge a raíz de la cibernética, que trata la relación Derecho e Informática desde el punto de vista del conjunto de normas, doctrina y jurisprudencia, que van a establecer y regular en su complejidad las acciones, procesos, aplicaciones y relaciones jurídicas de la Informática.

En efecto, la Informática no puede juzgarse pura y llanamente en su simple exterioridad, como la utilización de aparatos o elementos físicos electrónicos; sino que, en el modo de proceder se crean unas relaciones intersubjetivas de las personas naturales o jurídicas y de entes morales del Estado y surgen entonces un conjunto de reglas técnicas conectadas con el Derecho, que vienen a constituir medios para la realización de sus fines, ética y legalmente permitidos; creando principios y conceptos que institucionalizan la ciencia Informática, con autonomía propia.

Esos principios conforman las directrices propias de la institución Informática, y vienen a constituir las pautas de la interrelación nacional-universal, con normas mundiales supranacionales y cuyo objeto será necesario recoger mediante tratados públicos que hagan posible el proceso comunicacional en sus propios fines con validez y eficacia universal.

Antes de comenzar con un análisis de este tema debemos definir en forma general una serie de dudas que podrían surgir al investigar estos tópicos..

- ¿Qué es una ciencia?

Según la Real Academia Española la Ciencia es:
"El conocimiento cierto de las cosas por sus principios y causas. //2. Cuerpo de doctrina metódicamente formado y ordenado que constituye un ramo particular del humano saber....//4. Habilidad, maestría, conjunto de conocimientos en cualquier cosa".

Sin duda alguna que tanto la Informática Jurídica como el Derecho Informático constituyen conocimientos, principios, doctrinas, que catalogan a estas disciplinas como ciencias, que tienen como marco estricto a la iuscibernética y como marco amplio a la cibernética.

- ¿Qué es Informática Jurídica?

Es una ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el Derecho; es decir, la ayuda que este uso presta al desarrollo y aplicación del Derecho. En otras palabras, es ver el aspecto instrumental dado a raíz de la Informática en el Derecho.

Don Daniel Altmark señala que "la Informática Jurídica como aplicación concreta de la informática al Derecho, comprende los sistemas de archivo y documentación jurídica, de asistencia en las tareas administrativas de apoyo a las actividades jurídicas y la construcción de modelos para la comprensión del sistema jurídico"[55].

Por su parte, don Antonio-Enrique Pérez Luño en su obra "Nuevas tecnologías, sociedad y Derecho", tomando como base aspectos recién mencionados que la comprenden, la ha definido como "la disciplina que estudia el tratamiento automatizado de la información jurídica, incidiendo en las fuentes de conocimiento jurídico, mediante el tratamiento de la documentación legislativa, jurisprudencial y doctrinal, así como las fuentes de producción jurídica, a través de la elaboración informática de los factores lógico-formales que concurren en el proceso legislativo y en la decisión judicial"[56].

En otras palabras, se destaca en la Informática Jurídica que su objeto es la aplicación de la tecnología de la información al Derecho y que a través de ella se efectúa un tratamiento automatizado de información jurídica. Por lo tanto, la definiremos como la técnica que tiene por finalidad almacenar, ordenar, procesar y entregar, según un criterio lógico y científico, todos los datos jurídicos necesarios para documentar o proponer la solución al problema de que se trate.

2) Derecho Informático especifico

- ¿Qué es el Derecho Informático o Derecho de la Informática?

El Derecho Informático es la otra cara de la moneda. En esta moneda encontramos por un lado a la Informática Jurídica, y por otro, entre otras disciplinas encontramos el Derecho Informático: que ya no se dedica al estudio del uso de los aparatos informáticos como ayuda al Derecho, sino que constituye el conjunto de

[55] Altmark, Daniel R. *Etapa precontractual en los contratos informáticos.* Informática y Derecho, vol.1. Ed. Depalma, Argentina. 1987, p. 7.
[56] Cartagena Díaz, Patricio. La protección legal del software en Chile y en el Derecho comparado". Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales de la Universidad Católica de Valparaíso, Chile. 1990, p. 16

normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la Informática. Es decir, que la Informática en general desde este punto de vista es objeto regulado por el Derecho.

Ahora bien, la Informática Jurídica constituye una ciencia que forma parte del ámbito informático, demostrando de esta manera que la Informática ha penetrado en infinidad de sistemas. Instituciones, etcétera; y prueba de ello es que ha penetrado en el campo jurídico para servirle de ayuda y servirle de fuente. Por lo tanto, la Informática Jurídica puede ser considerada como fuente del Derecho, criterio propio que tal vez encuentre muchos tropiezos debido a la falta de cultura Informática que existe en nuestro país.

Al penetrar en el campo del Derecho Informático, se obtiene que también constituye una ciencia, que estudia la regulación normativa de la Informática y su aplicación en todos los campos. Pero cuando se dice Derecho Informático, entonces se analiza si esta ciencia forma parte del Derecho como rama jurídica autónoma; así como el Derecho es una ciencia general integrada por ciencias específicas que resultan de las ramas jurídicas autónomas, tal es el caso de la Civil, Penal y Contencioso Administrativa.

- ¿Es el Derecho Informático una rama autónoma del Derecho?

Al respecto, según encuentros sobre Informática realizados en Facultades de Derecho en España a partir de 1987, organizados por ICADE, siempre surgían problemas a la hora de catalogar al Derecho Informático como rama jurídica autónoma del Derecho o simplemente si el Derecho Informático debe diluirse entre las distintas ramas del Derecho, asumiendo cada una de estas la parte que le correspondiese.

En el VI Congreso Iberoamericano de Derecho e Informática celebrado en Montevideo, Uruguay, en 1998, expuse las razones por las cuales el Derecho Informático es una rama autónoma del Derecho. Desde aquel momento surgieron diferentes criterios, algunos afirmaban que el Derecho Informático nunca comprendería una rama autónoma del Derecho, por cuanto dependía en su esencia de otras ramas del Derecho, otros comentaban acerca del Derecho Informático como una rama potencial del Derecho, debido a su insuficiente contenido y desarrollo. Por supuesto no podían faltar aquellos que temían emitir algún tipo de opinión al respecto y por otro lado aquellos que consideramos al Derecho Informático como una rama autónoma del

Derecho, simplemente porque se considera que el Derecho Informático no es una rama típica, pero sin embargo constituye conocimientos y estudios específicos que se encuentran entre la relación Derecho e Informática, y que claramente, aunque tal vez no tan desarrolladas como otras ramas del Derecho, pero se puede hablar de conocimientos específicos del humano saber que caracterizan a una rama del Derecho como autónoma, sino todos estos estudios y conferencias no tendrían sentido alguno. Claramente se ha demostrado que se necesita legislación, doctrina, centros de investigación, campo docente, campo científico, es decir, un tratamiento específico de estos conocimientos determinados y, desde ese primer momento en que expuse las razones de la autonomía del Derecho Informático, encontré y visualicé el contenido autónomo del Derecho Informático, es decir ya este tenía bases firmes.

Por exigencias científicas, por cuanto un conjunto de conocimientos específicos conllevan a su organización u ordenación, o por razones prácticas que llevan a la separación del trabajo en vías de su organización, se encuentra una serie de material de normas legales, doctrina, jurisprudencia, que han sido catalogadas y ubicadas en diversos sectores o ramas. Dicha ordenación u organización del Derecho en diversas ramas tiene en su formación la influencia del carácter de las relaciones sociales o del contenido de las normas, entonces se van formando y delimitando en sectores o ramas, como la del Derecho Civil, Penal, Constitucional, Contencioso Administrativo..., sin poder establecer límites entre una rama jurídica y otra, por cuanto existe una zona común a todas ellas, que integran a esos campos limítrofes. De manera que esta agrupación u ordenación en sectores o ramas da origen a determinadas Ciencias Jurídicas, que se encargan de estudiar a ese particular sector que les compete.

Para analizar esta situación, es necesario mencionar las bases que sustentan a una rama jurídica autónoma, y al respecto se encuentran:

- Una legislación especificada (campo normativo).
- Estudio particularizado de la materia (campo docente).
- Investigaciones, doctrinas que traten la materia (campo científico).
- Instituciones propias que no se encuentren en otras áreas del Derecho (campo institucional).

Ahora bien, ¿qué sucede con el Derecho Informático?

Generalmente el nacimiento de una rama jurídica surge a consecuencia de cambios sociales reflejados en las soluciones normativas al transcurso de los años. Pero

resulta que, en el caso del Derecho Informático no hubo ese transcurrir del tiempo en los cambios sociales, sino que el cambio fue brusco y en poco tiempo, como consecuencia del impacto de la Informática en la sociedad, lográndose sociedades altamente informatizadas, que sin la ayuda actual de la Informática colapsarían

No obstante, a pesar de esta situación, existen países desarrollados como España en los que no se debería dudar acerca de una verdadera autonomía en el Derecho Informático, haciendo la salvedad de que esta ciencia constituye una rama jurídica atípica, que apenas nace y se desarrolla sin límites en su contenido ni en el tiempo.

En el caso de Chile, son muy pocos los sustentos que encontramos para el estudio de esta materia, tal vez su aplicación se limita fundamentalmente a la aparición de libros con normativas (doctrina), y comentarios de Derecho Informático. Pero tal vez sea más fácil para los abogados buscar esta normativa en las otras ramas del Derecho, por ejemplo; acudirían al Código Civil para ver lo relativo a las personas, protección de datos, derecho a la intimidad, responsabilidad civil, entre otras. Resulta, sin embargo, que esta situación no se acopla con la realidad Informática del mundo, ya que existen otras figuras como los contratos electrónicos, comercio electrónico, firmas digitales, habeas data y documentos electrónicos, que llaman a instituciones que pertenezcan a una rama autónoma del Derecho.

En este orden de ideas, es menester entonces concluir que en el Derecho Informático sí existe legislación específica, que protege al campo informático. Tal vez no con tanta trayectoria y evolución como la legislación que comprenden otras ramas del Derecho, pero sí existe en el Derecho Informático legislación basada en leyes, tratados y convenios internacionales, además de los distintos proyectos que se llevan a cabo en los entes legislativos de nuestras naciones, con la finalidad del control y aplicación lícita de los instrumentos informáticos.

Con respecto a las instituciones propias que no se encuentren en otras áreas del Derecho (campo institucional), se encuentra el contrato informático, el documento electrónico, el comercio electrónico, delitos informáticos, firmas digitales, *habeas data*, entre otras, que llevan a la necesidad de un estudio particularizado de la materia (campo docente), dando como resultado las investigaciones, doctrinas que traten la materia (campo científico). En efecto, se pueden conseguir actualmente grandes cantidades de investigaciones, artículos, libros e inclusive jurisprudencia que esté enmarcada en la interrelación entre el Derecho y la Informática, creándose sus propios principios e

instituciones, como se ha constatado en los Congresos Iberoamericanos de Derecho e Informática.

Por lo tanto, no hay excusa, ni siquiera en un país donde el grado de informatización sea bajo para que se obvie la posibilidad de hablar del Derecho Informático como rama jurídica autónoma del Derecho, si bien se puede llegar a ella, no solo por la integración de las normas jurídicas, sino también por la heteroaplicación, cuando en un sistema jurídico existan vacíos legales al respecto, porque es de tomar en cuenta que ante el aumento de las ciencias dogmática-jurídicas, el Derecho es un todo unitario, puesto que las normas jurídicas están estrechamente vinculadas entre sí, ya sea por relaciones de coordinación o de subordinación, con lo que se concluye que para la solución de una controversia con relevancia jurídica, se puede a través de la experiencia jurídica buscar su solución en la integración de normas constitucionales, administrativas, financieras, entre otros, o llegar a la normativa impuesta por convenios o tratados internacionales que nos subordinan a la presión supranacional.

Para concluir, se advierte que aquellos que niegan la autonomía del Derecho Informático, tendrán que analizar nuevamente los principios que rigen la autonomía de una rama del Derecho, por cuanto es evidente que estas características están contenidas contundentemente en el Derecho Informático. Con respecto a aquellos que consideran como rama potencial al Derecho Informático, deben tener cuidado, debido a que se podrían quedar con ese criterio de potencialidad para siempre, porque es de resaltar que el Derecho Informático, a diferencia de otras ramas del Derecho, no tiene ningún tipo de restricciones en su desarrollo, ya que este siempre estará evolucionando en el tiempo hacia el futuro, y así como no se puede divisar el límite del desarrollo informático, tampoco el del Derecho Informático, debido a que este siempre tratará de darle solución a los conflictos que surjan consecuentes del desarrollo de la tecnología. Este punto debe ser exaltado, porque una de las razones que sustenta la doctrina que estima potencial la autonomía del Derecho Informático, es que este no da solución de inmediata a ciertas situaciones; al respecto este humilde autor responde, que por las características antes expuestas referentes a que el Derecho Informático constituye una rama atípica del Derecho, se encuentra sin límites visibles, siempre tratará de buscar protección y soluciones jurídicas a nuevas instituciones Informáticas, lo que no quiere decir que no sea una rama autónoma del Derecho, al contrario, desarrollará aún más sus bases.

3) Características

- ¿Cúal es la naturaleza jurídica del Derecho Informático?

El Derecho Informático es una rama del Derecho que se constituye en el estudio del conjunto de normas, aplicaciones, procesos, relaciones jurídicas, doctrina, jurisprudencia, que surgen como consecuencia de la aplicación y desarrollo de la Informática, encontrando pautas para la consecución de fines específicos, como los siguientes:

- Desarrollo adecuado de la industria Informática, buscando la extensión y propagación de la misma.
- Y desde otra perspectiva, ya no enfocando la regulación de los instrumentos informáticos, sino la regulación específica de su aplicación; en otras palabras, se refiere al hecho del manejamiento lícito de los instrumentos informáticos.

Estos dos son los puntos de vista que en general se identifican en el Derecho Informático, porque cualquier otra vertiente que exista y pudiera existir en el futuro, es fácilmente ubicable en ellos.

Cuando se refiere al punto de la naturaleza jurídica del Derecho Informático, se debe realizar un exhaustivo análisis de la ubicación del mismo en el campo del Derecho Privado o del Derecho Público.

- ¿El Derecho Informático se ubica dentro del Derecho Privado o del Derecho Público?

Al tratar el punto del Derecho Público y del Derecho Privado, se encuentra una gran complejidad en su desarrollo, en el sentido de que a pesar del establecimiento de ciertas pautas, que separan no con gran nitidez a ambas ramas generales del Derecho, se presentan ciertas diferencias entre los ordenamientos jurídicos mundiales. Tanto así que, por ejemplo, el Derecho penal en Francia es considerado de Derecho Privado, por cuanto se ocupa de la sanción de los delitos, a pesar de que en muchos países es abarcado como de Derecho Público, ya que tiene por objeto asegurar el orden del Estado.

"La delimitación de los ámbitos respectivos del Derecho Privado y del Derecho Público, tal como ha sido enseñada siempre, resulta sencilla: el Derecho Privado regula las relaciones de los individuos entre sí; el Derecho Público, las de los individuos con el Estado. Oposición fundamental que justifica métodos y soluciones distintas; porque los mismos problemas vistos desde el ángulo del Derecho Privado y del Derecho Público revisten aspectos por completo diferentes... "[57]

Y agrega Mazeaud que "el legislador (no hay que escribir: el Estado) dicta cada vez más reglas imperativas en las relaciones de Derecho Privado. Para ellos allí donde hay ley imperativa, existe Derecho Público"[58].

Cuando se ubica al Derecho Público en el Estado de Derecho en que vivimos actualmente, comprende los siguientes aspectos:

- Todo lo referente a la organización, el funcionamiento y actividad de los entes públicos estatales, estaduales y/o municipales.
- Abarca la regulación de actividades de interés colectivo.

Uno de los puntos claves cuando se hace referencia al Derecho Privado es la de la palabra particulares, de allí se salta a lo que se llamaría la libertad de los particulares en ese acuerdo de voluntades, para la determinación, por ejemplo, de las pautas que determinarán un contrato. Tomando en cuenta que jus privatum, sub tutela iuris publici, latea es decir, el Derecho Privado se acoge bajo la tutela del Derecho Público.

4) Ámbitos de Aplicación

- ¿Cuál es la relación del Derecho Informático con las otras ramas del Derecho?

Con el Derecho Constitucional:

El Derecho Informático tiene una estrecha relación con el Derecho Constitucional, por cuanto la forma y manejamiento de la estructura y órganos fundamentales del Estado es materia constitucional. De allí que actualmente se debe resaltar que dicho manejamiento y forma de controlar la estructura y organización de los órganos del Estado, se lleva a cabo por medio de la Informática, colocando al Derecho

[57] MAZEAUD, Jean. Lecciones de Derecho Civil. Parte Primera. Volumen I. Ediciones Jurídicas Europa-América. Buenos Aires, 1959, pág. 47.
[58] MAZEAUD, Jean. Lecciones de Derecho Civil. Parte Primera. Ob. Cit. Pág. 48.

Informático en el tapete, porque con el debido uso que se le den a estos instrumentos informáticos, se llevará una idónea, eficaz y eficiente organización y control de estos entes. De lo que se puede desprender una serie de relaciones conexas con otras materias como sería el caso del Derecho Tributario y el Derecho Procesal.

Debemos indicar que lo relativo al resguardo constitucional de la privacidad en cuanto al uso de las Tecnologías de la Información y las Comunicaciones está visto en el capítulo II de esta memoria.

Con el Derecho Penal:

En este punto se nota una estrecha relación entre el Derecho Informático y el Derecho Penal, porque el Derecho Penal regula las sanciones para determinados hechos que constituyen violación de normas del Derecho y en este caso del Derecho Informático, en materia del delito cibernético o informático, entonces se podría comenzar a hablar del Derecho Penal Informático.

Con los Derechos Humanos:

Los Derechos humanos, indispensables para defender los Derechos fundamentales del hombre, tales como el de la vida, el de la igualdad, el respeto moral, vida privada e intimidad que llevan al hombre a ser dignos y por consiguiente a tener dignidad, con lo que permite catalogar a las personas como íntegras, conviviendo en ambiente de respeto, de libertad y haciendo posible sociedades verdaderamente civilizadas.

Comentábamos que existen diversos tratados internacionales referidos a los Derechos Humanos que amparaban temas como lo es la privacidad e intimidad, que podrían ser burladas por utilización ilícita de los medios informáticos.

Con el Derecho Civil

Ya se está comenzando a implantar normas legales relativas a la responsabilidad civil producto del uso de herramientas propias de la Informática. Asi señalaremos en su oportunidad, en el caso de Chile, las responsabilidades civiles fruto de la violación de la

privacidad de los datos personales, responsabilidad por envío de Spam a través de infracciones a la ley del Consumidor, etc.

Con el Derecho Procesal

Cada vez que se regula sobre nuevas materias en la legislación de un país, es necesario establecer normas precisas en cuanto al procedimiento para aplicar lo que el derecho sustantivo sistematiza. Asi, es claramente necesaria la formación y confección de normas procesales. Cuando hacemos referencia a legislación chilena y tal como veremos en su oportunidad, revisaremos las acciones que se han visto plasmadas a través del llamado “Habeas Data”.

Por último debemos considerar que es indiscutible la estrecha y tan importante relación que existe entre el Derecho Informático y el Estado; produciendo consecuencias al bien colectivo y general. Por lo que existe el Derecho Informático Público; en otras palabras, el Derecho Informático de carácter Público.

Ahora bien, el Derecho Informático si bien se relaciona a pesar de su autonomía, con otras ramas del Derecho, no es igual tradicionalmente hablando, por cuanto el Derecho Informático es tan amplio que necesariamente penetra en todo, así como la Informática ha penetrado en todos los ámbitos. También se puede hacer referencia al Derecho Informático Privado; es decir, al Derecho Informático de carácter Privado, ya que existen innumerables situaciones que son de carácter privado, como por ejemplo, el contrato electrónico, el contrato informático, el comercio electrónico, el documento electrónico, y así un sin número de figuras jurídicas pertenecientes al ámbito particular o privado, donde se permite ese acuerdo de voluntades, clave para determinar la existencia del Derecho Informático Privado.

Se concluye entonces, que al hablar de la naturaleza jurídica del Derecho Informático, tomando en cuenta que este constituye una rama atípica del Derecho y que nace como consecuencia del desarrollo e impacto que la tecnología tiene en la sociedad; así como la tecnología penetra en todos los sectores, tanto en el Derecho Público como en el privado, igualmente sucede con el Derecho Informático, este penetra tanto en el sector público como en el sector privado, para dar soluciones a conflictos o planteamientos que se presenten en cualquiera de ellos. De manera que el Derecho

Informático sería un caput mortuum, es decir, cosa sin valor o cabeza muerta, si la tecnología no hubiese nacido y no se hubiese desarrollado.

Capitulo IV Protección civil

"Los ordenadores facilitan hacer un montón de cosas, la mayoría de las cuales no necesitan ser hechas".
Andy Rooney

1) Concepto General:

Antes de comenzar a hablar sobre lo que titulamos "Protección Civil", debemos que señalar un par de consideraciones, a nuestro entender necesarias, para englobar y restringir nuestro análisis y estudio.

Por una parte, al referirnos a protección civil de la privacidad, no nos estamos refiriendo a buscar las herramientas jurídicas que el legislador nos otorga para la protección de la privacidad en el Código Civil, como bien podría malinterpretarse al considerar en forma restrictiva la palabra "civil". Cuando hablamos del "protección civil" nos enmarcamos en los medios que existe a nivel privado, en el ámbito de la ley, referido a las relaciones entre las personas, excluyendo a su vez las relaciones, derechos y obligaciones que surgen de los contratos, puesto que tendríamos que revisar las normas pertinentes contractuales.

Al mismo tiempo debemos indicar que en nuestra finalidad de encontrar normas relativas a una llamada protección civil de la privacidad dice relación directamente con el uso de las Tecnologías de la Información y las Comunicaciones, excluyendo por ende las regulaciones relativas a intimidad y privacidad que no dicen relación al uso de las nuevas Tecnologías. Esta advertencia es necesaria, puesto que actualmente se encuentra en el Congreso, un proyecto de ley que se titula "Protección civil del honor y la intimidad de las personas.", cuya iniciativa surge por moción parlamentaria del 20 de julio de 1999 y que actualmente se encuentra en la etapa de segundo trámite constitucional, más específicamente en el primer informe de Comisión de Constitución, Legislación, Justicia y Reglamento.

En términos generales, el proyecto pretende regular las relaciones entre la protección civil de la intimidad y el ejercicio de la actividad de buscar y difundir información. Además orienta por medio de criterios amplios la decisión del juez y

concede acciones reparatorias a aquellos que sean objeto de intromisión ilegítima. Por tanto en este proyecto se encuentra en disputa el derecho a la información y el derecho a la intimidad y el honor.[59]

2) Legislación Chilena, Ley 19.628

Basándonos en lo relativo a la privacidad y su protección civil y considerando las advertencias antes señaladas, comenzamos a verificar la existencia de leyes vigentes. Nos encontramos en primer lugar con la opinión del profesor de la Universidad Diego Portales don Carlos Peña que señala "…no hay una regulación legal específica desde el punto de vista civil en materia de privacidad - dice-. Está en la Constitución y nada más. En materia penal lo que hay son los tipos penales relativos a la privacidad" (a.- El delito que castiga la violación de secreto; b.- La violación de morada -ingreso sin permiso-; y c.- Los artículos 161-A y 161B del Código Penal)".[60]

Sin embargo, a contrario de la opinión anterior sí existe una ley que reglamenta y protege nuestra privacidad cuando ha sido vulnerada por el uso de las Tecnologías de la Información y de las Comunicaciones.

Esta ley es la ley nº 19.628 sobre Protección de Datos de carácter Personal que fue publicada en el Diario Oficial, con fecha 28 de agosto de 1999 y que tuvo su origen en una moción presentada ante el Senado con fecha 5 de enero de 1993, y tenía por propósito llenar un vacío manifiesto en el ordenamiento jurídico chileno mediante el otorgamiento de una adecuada protección al derecho de la vida privada de las personas, en el ámbito del derecho civil, ante eventuales intromisiones ilegitimas. Este objetivo tan ambicioso motivó que el texto fuera sometido a largas discusiones y cambios en cada uno de los trámites constitucionales que debió superar tanto ante el Senado como en la Cámara de Diputados. Finalmente, y con el objeto de superar las divergencias entre el Senado y la Cámara de Diputados, se formó una Comisión Mixta integrada por integrantes de cada una de las cámaras.

El texto aprobado se limitó a regular uno de los aspectos de la protección de la vida privada, como lo es el tratamiento que los organismos públicos y los particulares

[59] Es importante recalcar que el legislador ha hecho muy bien en nombrar el proyecto de ley con los términos intimidad y honor y no incluyó el vocablo "privacidad", conforme a nuestra opinión sobre el correcto uso y segregación de conceptos de privacidad e intimidad, opinión presente en el capítulo 2 de la presente memoria.

[60] Para leer en forma completa la entrevista http://www.colegiodeperiodistas.cl/documentos_neu_37.htm

efectúen de los datos de carácter personal almacenados en registros o bancos de datos sean estos de carácter automatizado o no. La aspiración de regular el fenómeno de la protección de la vida privada como un todo, tuvo una vez más que ser pospuesta. Este es el motivo por el cual la Ley se denomina "Sobre Protección de la Vida Privada", cuando en realidad, solo regula un aspecto de tal importante materia.

Si bien en el proyecto original se tomaron como parámetros orientadores los principales criterios esbozados por el derecho comparado y los tratados y convenciones internacionales, pareciera ser que a medida que la discusión de la Ley se fue desarrollando, la injerencia de la derogada Ley Orgánica española 5/92 de 29 de octubre de 1992, Sobre Regulación de Tratamiento Automatizado de Datos, fue cada vez mayor.

Por tanto y para verificar la protección otorgada por el legislador debemos comenzar analizando la ley en cuestión.

3) Análisis de la ley 19.628

En cuanto al ámbito de aplicación de la presente ley, debemos considerar que esta es bastante restrictiva porque contrariamente a lo que su título sugiere, la ley no regula orgánicamente todos los aspectos de la vida privada de las personas, entre los que podrían haber quedado comprendidas materias tales como la violación de domicilio, la violación de la correspondencia, la interceptación de las comunicaciones y, en general, la protección del honor, la imagen y la intimidad de las personas.

Por el contrario, la norma regula de una manera muy específica el tratamiento de los datos de carácter personal en registros o bancos de datos (art. 1°). La ley protege la vida privada de las personas naturales en cuanto ésta puede verse afectada por la recolección, registro, procesamiento, comunicación o utilización que se haga de cualquier forma, manual o automatizada, de sus datos personales, en registros o bancos de datos, por parte de personas u organismos públicos o privados.

A la hora de establecer el ámbito de aplicación de la ley resulta crucial precisar lo que ésta entiende por tratamiento de datos personales (arts. 1° y 2°).

La letra o) del artículo segundo proporciona una amplísima definición de "tratamiento de datos". Ésta comprende básicamente toda operación o procedimiento

técnico que permita recolectar, almacenar, procesar, comunicar o utilizar datos personales. La norma se refiere concretamente a la recolección, almacenamiento, grabación, organización, elaboración, selección, extracción, confrontación, interconexión, disociación, comunicación, cesión, transferencia, transmisión, cancelación o utilización en cualquier forma, largo listado de operaciones que revela el propósito del legislador de definir un concepto lo más amplio posible a este respecto. Es en todo caso indiferente que dicho tratamiento se efectúe por medio de procedimientos automatizados o no.

Por otro lado, la letra f) del artículo segundo define a los datos personales o de carácter personal como aquellos "relativos a cualquier información concerniente a personas naturales, identificadas o identificables".

Es interesante también hacer notar que el tratamiento de datos personales objeto de regulación por la ley es aquel que se hace en registros o bancos de datos, definidos como conjuntos organizados de datos personales, manuales o automatizados, que permiten relacionar los datos entre sí y realizar todo tipo de tratamiento de los mismos (art. 2°, letra m).

Un punto a considerar es que la ley no distingue si el tratamiento es efectuado por sujetos de derecho público o de derecho privado y, en consecuencia, los somete básicamente a las mismas reglas.

Por último, es menester puntualizar que la ley excluye de su ámbito de aplicación el tratamiento de datos personales que se efectúe en ejercicio de las libertades de opinión y de informar consagradas en el número 12, del artículo 19 de la Constitución Política del Estado,

Tenemos que tener presente además que la ley reconoce en general la conveniencia social de los registros y bancos de datos y, de una u otra manera, se refiere a algunos registros que de paso legitima. Es el caso de los bancos de datos con información económica, financiera, bancaria y comercial, que sirven de sustento al sistema crediticio (art. 4°). Así también, la norma se refiere a los bancos de datos con información de salud, que existen en apoyo del sistema de seguros de salud y del sistema previsional (art. 10). Implícitamente se comprenden también los bancos de datos con información de contribuyentes, en sustento del sistema impositivo del Estado (arts. 15 y 20). Igualmente, es el caso de los bancos de datos con información procesal y penal (art. 21), en apoyo del sistema procesal, penal y otras muchas instituciones y actividades en que como requisito se exige una conducta intachable de las personas. Un

rol de evidente importancia corresponde a los bancos de datos con información civil, como base del sistema de identificación y determinación del estado civil de las personas (Art. 20). Asimismo, la existencia de bancos de datos con información sobre las personas, sus ideologías, actividades, opiniones, etc., se justifica como relevante para la seguridad nacional (art. 15).

Considerando lo anteriormente dicho podríamos preguntarnos ¿en que momento existe una protección de la vida privada?

Como contrapartida al reconocimiento de la conveniencia socia de los registros y bancos de datos, la ley busca amparar a la: personas que pueden ver afectada su vida privada y, particularmente, su honor, imagen e intimidad, por el tratamiento organizado de sus datos personales.

En vista a armonizar los intereses comprometidos, en primer lugar, junto con legitimar el tratamiento organizado de datos personales sólo en ciertas y determinadas circunstancias, la ley regula e desarrollo de esta actividad por parte de personas y organismo tanto públicos como privados.

En segundo término, la norma en estudio reconoce y regula determinados derechos de las personas, concretamente del titula: de los datos, con miras a evitar que el tratamiento organizado de sus datos personales pueda atentar en contra de su vida privada y como se ha dicho, de su honor, imagen e intimidad.

Dentro del desarrollo de la actividad de tratamiento organizado de datos personales por parte de encargados de bases de datos, existen principios matrices que establece la ley

En primer lugar, dicho tratamiento de datos permitido por la legislación debe efectuarse de conformidad a la ley en estudio y, muy específicamente, sólo para las "finalidades permitidas por el ordenamiento jurídico".

En segundo lugar, el tratamiento de datos debe llevarse a cabo respetando el pleno ejercicio de los derechos fundamentales de los titulares de datos y de las facultades que la misma ley en estudio les reconoce.

Se precisa por parte de la ley que dicho tratamiento sólo puede efectuarse cuando lo autoriza el titular de los datos o la ley (art. 4°).

En efecto, una primera posibilidad es que el propio titular de los datos personales autorice el tratamiento de los mismos, caso en el cual la autorización se sujeta a las siguientes reglas:

a) La autorización debe ser escrita e informada: la información que debe proporcionarse al titular de los datos debe cubrir tanto la finalidad dentro de la cual se enmarcará el tratamiento de dato: corno su posible comunicación al público, lo que dice relación con el grado de divulgación de sus datos personales que el titular está dispuesto a tolerar.

b) La autorización puede ser revocada: la revocación debe hacerse igualmente por escrito y en ningún caso opera con efecto retroactivo (art. 4°).

Una segunda posibilidad es que el tratamiento de los datos personales sea autorizado por la ley, sea que la autorización esté contenida en una ley especial (art. 4°) o que genéricamente se encuentre establecida en la Ley N° 19.628. En forma algo inorgánica esta ley, en definitiva, autoriza genéricamente el tratamiento organizado de datos personales en cuatro casos, a saber:

a) En el evento de tratamiento de datos personales proveniente: de fuentes accesibles al público (no reservado a solicitantes), y siempre que se trate alternativamente:

i) de datos personales de carácter económico, financiero bancario o comercial;

ii) de datos personales que se contengan en listados relativos a categorías de personas, que se limiten a indica: antecedentes tales como: pertenencia a un grupo, profesión o actividad, títulos educativos, dirección, fecha de nacimiento, o

iii) de datos personales que sean necesarios para comunicaciones comerciales de respuesta directa, o comercialización o venta directa de bienes y servicios (art. 4° inc. 5°).

b) Cuando se trate del tratamiento de datos personales que efectúen personas jurídicas privadas, siempre que se trate, copulativamente:

i) de datos personales para uso de la misma persona privada, sus asociados o afiliados, y

ii) se traten sólo con fines estadísticos de tarificación u otros de beneficio general de los mismos (art. 4° inc. final). Quedará entonces por determinarse la amplitud de esos otros fines, por ejemplo en lo relativo a investigación histórica o científica.

c) En los casos de tratamiento de datos personales que efectúen personas u organismos públicos respecto de materias de su competencia (art. 20).

d) Cuando el tratamiento de datos personales se efectúe para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares (art. 10). Se trata aquí de un caso especialísimo, en el que la ley autoriza incluso el tratamiento de datos

sensibles, que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, los estados de salud físicos o psíquicos y su vida sexual. De acuerdo a la letra g) del artículo segundo, son también datos sensibles, aunque en otro orden de materias, las ideologías, opiniones políticas y creencias o convicciones religiosas.

Las normas comentadas anteriormente y otra serie de disposiciones de la ley permiten distinguir los principios rectores a que en definitiva está sometido el tratamiento organizado de datos personales, a saber:

a) No puede efectuarse el tratamiento organizado de datos personales sin previa autorización del titular o de la ley (especialmente en el caso de datos sensibles).

b) El tratamiento organizado de datos personales sólo puede efectuarse con una finalidad determinada, explícita y legítima.

c) El tratamiento organizado de datos personales debe respetar el pleno ejercicio de los derechos fundamentales y legales del titular de los datos y, muy concretamente, la veracidad de la información y la reserva y custodia de la información, para que ella no sea comunicada o interceptada por personas no autorizadas por el titular o la ley.

d) El tratamiento de datos personales está entregado a la responsabilidad del sujeto, sea persona u organismo público o privado, a quien competen las decisiones relacionadas con el tratamiento de los datos personales.

Es importante resaltar que la ley no contempla organismos administrativos a cargo del control de esta actividad y el principio, en definitiva, es que cualquier persona puede efectuar el tratamiento organizado de datos en la forma que dispone la ley, sin necesidad de registro previo. La única norma que hace excepción a este principio es aquella que obliga a los organismos públicos a comunicar al Servicio de Registro Civil e Identificación, cuando corresponda, la creación de un registro o banco de datos, los fundamentos jurídicos del mismo, su finalidad, tipo de datos almacenados y descripción del universo de personas que comprende. Al Servicio de Registro Civil e Identificación la ley encomienda llevar un registro de los bancos de datos a cargo de organismos públicos (art. 22).

4) Derecho de las personas sobre los responsables de bancos de Datos

Ahora bien, debemos considerar que sucede si existen infracciones a la presente ley y que sanciones incluye en beneficio de la protección de la privacidad de las personas.

La ley contempla varios órdenes de infracciones y sanciones según sea el caso, las que pueden sintetizarse como sigue:

1) En caso de infracción al deber de pronunciarse sobre la solicitud de entrega de información, modificación, eliminación, o bloqueo de datos: en estos casos, la persona afectada puede reclamar mediante un recurso especial de amparo, a través del cual puede obtenerse precisamente la información, modificación, eliminación o bloqueo de datos personales requerida y, además, la imposición de multas o suspensión del cargo a los responsables (art. 16), el denominado "Habeas Data" cuya análisis la veremos a continuación.

2) En caso de infracción a las normas sobre utilización de datos personales, relativos a obligaciones de carácter económico, financiero, bancario o comercial: en estos supuestos la persona afectada puede reclamar, también mediante recurso especial de amparo, a través del cual puede obtenerse el cumplimiento de las obligaciones infringidas y, además, la imposición de multas o suspensión del cargo a los responsables (art. 19).

3) En caso de otras infracciones: fuera de los casos tratados en los números precedentes, la persona afectada puede reclamar a través de demanda en juicio sumario especial, en el que se aprecia la prueba en conciencia y el juez deberá tomar todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece (art. 23).

- ¿Existe pues, una responsabilidad civil por las infracciones cometidas?

La ley dispone que, sin perjuicio de lo ordenado por el juez en su caso, la persona u organismo a cargo del registro o banco de datos deberá indemnizar el daño patrimonial y moral que causare el tratamiento indebido de los datos (art. 23).

Cabe entender que la responsabilidad civil impuesta sobre el responsable del registro o banco de datos es de naturaleza extra-contractual y, por lo tanto, deben cumplirse al respecto los requisitos exigidos por la ley al efecto (art. 23).

En cuanto al autor de la infracción, es claro puede tratarse de una persona natural o jurídica, pública o privada. A su vez, el hecho ilícito estará constituido por el tratamiento indebido de datos personales, lo cual supone un tratamiento con infracción de ley o que no respeta los derechos fundamentales o legales del titular de los datos (art. 23). En lo que atañe a la causalidad entre el hecho ilícito y el daño, la ley no aporta reglas especiales.

Respecto de la imputabilidad, a lo largo de la ley es posible encontrar una serie de normas que establecen los deberes del sujeto responsable del registro o base de datos personales. Así, dicho sujeto se encuentra obligado a contar con la autorización del titular o de la ley para el tratamiento de los datos; a sujetar dicho tratamiento a la finalidad del respectivo registro; a cuidar la veracidad de la información, proporcionando la información que se le solicite respecto del mismo, modificando, eliminando y bloqueando los datos personales cuando ello proceda, y a cuidar los datos almacenados con la debida diligencia.

De esta manera, el sujeto responsable del registro o base de datos personales debe responder de las obligaciones apuntadas en el párrafo precedente y de las demás que específicamente señala la ley al regular estas materias, responsabilidad o deber de cuidado que, de acuerdo al derecho común, se extiende hasta la culpa leve.

En lo concerniente a los daños, se responde de daño material y moral. Tratándose del daño material y concretamente del daño emergente y lucro cesante, cabe entender que se aplican las reglas generales, de acuerdo a las cuales el daño debe ser debidamente acreditado. A su vez, al daño moral se aplicaría la regla contenida en el artículo 23 de la ley, de acuerdo a la cual la avaluación del daño la hace el juez prudencialmente, considerando las circunstancias del caso y la gravedad de los hechos (art. 23).

Desde el punto de vista de la acción civil, ésta puede interponerse conjunta o separadamente con la reclamación destinada a establecer la infracción, esto es, conjunta o separadamente con la acción de amparo del artículo 16, la del artículo 19, o la demanda en juicio sumario en el caso de otras infracciones. Es motivo de reflexión el que junto con una acción de amparo se autorice discutir sobre la existencia del derecho a una indemnización e incluso sobre la especie y monto de los perjuicios.

En todo caso, la ley admite litigar sobre el derecho a la indemnización y separadamente sobre la especie y monto de los perjuicios (173 CPC). Si se sigue este procedimiento separado cabría entender que la acción de indemnización de perjuicios se sometería a las reglas del juicio sumario especial antes aludido (art. 23).

- ¿La ley contempla una responsabilidad penal?

Esta ley no contempla sanciones penales, sin perjuicio de las penas que puedan establecer las leyes en casos específicos, como las relativas a los llamados "delitos informáticos" y que serán analizados en el capítulo V de la presente memoria.

5) El llamado Hábeas Data Chileno

Antes de señalar que es lo que consideramos como "Hábeas Data Chileno", podemos indicar como introducción al tema que suele afirmarse que el abuso de las posibilidades computacionales constituye la amenaza por excelencia contra la privacidad, porque cruzándose telemáticamente datos personales o nominativos puede obtenerse un perfil de las personas cuyos antecedentes son procesados. Esta imagen inmaterial del titular de los datos debe ser resguardada porque puede ser creada errada o dolosamente, lo que eventualmente se traducirá en discriminaciones, en la imposibilidad de ejercer algún derecho, o en la pérdida de algún beneficio.

Conceptualmente, un dato es un antecedente que da cuenta de un hecho o de una característica determinada. El conjunto organizado de datos constituye información y, sociológicamente hablando, un nuevo bien económico de alto valor y una forma de poder.

Un dato es personal o nominativo cuando permite identificar cualquiera característica de una persona para relacionarse en sociedad, por ejemplo al consignarse en una guía de teléfonos datos generales, o cuando son de mayor importancia o sensibilidad como ocurre con la filiación política, el credo religioso que se profesa, los antecedentes laborales, la situación de salud, la mayor o menor riqueza, las operaciones comerciales que se realizan, las acciones en empresas que se poseen, los depósitos en cuenta corriente o a plazo, los impuestos pagados, etc.

Por un lado está el legítimo interés de aquellas personas cuyos datos nominativos se procesan computacionalmente, en resguardar su vida privada y la necesaria confidencialidad de antecedentes como sus creencias religiosas, su filiación política, sus tendencias sexuales, su estado de salud, el monto de su patrimonio, etc.

Por el otro, un interés –también muy legítimo– que poseen los gobiernos y los particulares para acceder a cierta información: los Estados para cumplir con sus fines promocionales y asistenciales de orden público, como por ejemplo saber quiénes tienen SIDA al momento de fijar políticas de salud, y los particulares, generalmente constituidos en empresas de servicios o entidades gremiales, que para asegurar la vigencia de un orden público económico necesitarán conocer los antecedentes comerciales irregulares o negativos de las personas que actúan en la vida comercial.

Se trata, por ende, de lograr un equilibrio y establecer límites entre el derecho a la privacidad que consagra el artículo 19 N°4 de la Constitución y un derecho a la información –consagrado en el artículo 19 N°12– fundado en razones de orden público.

La interrogante a dilucidar o la hipótesis de trabajo, en consecuencia, puede ser la siguiente: ¿cómo conciliar el Derecho a la Información con el Derecho a la Privacidad?; ¿cómo equilibrar por un lado la máxima libertad o acceso a la información con un adecuado resguardo de la privacidad? Se trata de una cuestión importante por cierto, no de meras disquisiciones teóricas o doctrinarias, porque si bien el orden público social y económico de una Nación requiere que tanto el Estado como los particulares manejen determinados datos personales, sea para fijar políticas de salud o para evitar la morosidad comercial, esto no puede traducirse, al extremo, en abusos contra las personas. Así ha ocurrido con la información comercial o sobre los antecedentes patrimoniales de los chilenos, que en base a inexistentes argumentos legales o erradas interpretaciones constitucionales hasta antes de la ley era procesada y comercializada sin límite alguno y hoy en día, al tenor de la nueva ley aprobada que se informa, se hace con límites mínimos o meramente formales.

Se produce (doctrinaria y legalmente) la conciliación entre el Derecho a la Intimidad y el Derecho a la Información a través del control que para el titular de los datos posibilita el denominado Derecho de Acceso o Hábeas Data, una nueva garantía fundamental (o un nuevo mecanismo de resguardo y tutela) que contemplan en el Derecho Comparado tanto algunas Cartas Fundamentales como las llamadas Leyes de Protección de Datos, y una consagración del principio de la autodeterminación informativa.

El Hábeas Data es una acción cautelar de rango constitucional (en diversas legislaciones extranjeras) o de rango legal (como es el caso chileno), heredera de otro recurso y tan importante como el Hábeas Corpus, que en las modernas sociedades de la información permite a los titulares de los datos personales y patrimoniales –al decir de una sentencia histórica del Tribunal Constitucional alemán– "autodeterminar" el uso que se haga de sus antecedentes cuando ellos son recopilados, registrados y cruzados computacionalmente.

Atendida la relevancia de este Derecho de Acceso él ha sido consagrado en tratados internacionales y en Constituciones como las de Portugal, España, Paraguay y –en 1994– en Argentina, considerándosele como un instituto del derecho procesal constitucional del que conocen órganos autónomos ad hoc y los Tribunales Superiores de Justicia porque de lo que se trata es de proteger la privacidad de las personas.

¿Cuál es la realidad en Chile?

La ley 19.628 establece una acción que podríamos calificar con Hábeas Data Chileno, y en la cual encontramos numerosas enunciaciones de obligaciones, deberes y derechos. Así, por ejemplo, la obligación de efectuar tratamiento de datos sólo cuando exista autorización expresa del titular o de la ley (art. 4°.1), la de resguardar los derechos de los titulares en la transmisión de datos (art. 5°), las de eliminar, modificar o bloquear datos sin necesidad de requerimiento (art. 6°), las de guardar reserva de las personas que trabajan en el tratamiento de información personal (art. 7°), la de no procesar datos sensibles salvo casos de excepción (art. 10).

En todos esos casos estamos frente a deberes que se imponen a los responsables de bancos de datos, esto es, a las personas naturales o jurídicas privadas u organismos públicos, a quienes competen las decisiones relacionadas con el tratamiento de datos de carácter personal (art. 2°, letra n), y cuya infracción podrá generar sanciones de carácter infraccional o disciplinario y también responsabilidad civil por los daños y perjuicios producidos. No estamos sin embargo en el ámbito de los derechos subjetivos.

Frente a estos deberes la ley N° 19.628 reconoce o concede a los particulares verdaderos derechos subjetivos. Es así como el título II de la ley, que se compone de los artículos 12 a 16, se denomina "De los derechos de los titulares de datos".

En realidad, sólo los artículos 12 a 15 contienen una regulación de los derechos de los titulares, mientras el artículo 16 se dirige a reglamentar la acción típica mediante la cual se busca asegurarles una tutela judicial efectiva.

La terminología de la ley, unida a la caracterización que ella hace de las facultades otorgadas a los particulares, o titulares de datos, hacen inexcusable la conclusión de que estamos frente a derechos subjetivos, esto es, a facultades morales que permiten a su titular exigir de otra persona una determinada conducta.

En primer lugar debemos individualizar a los titulares de los datos como sujetos de derechos.

La ley ha concedido estos derechos a los "titulares de datos". Según la terminología fijada en el artículo segundo, titular de los datos es "la persona natural a la que se refieren los datos de carácter personal" (art. 2°, letra ñ). En otros términos, es lo que los autores españoles suelen denominar "persona concernida".

Tal como lo hemos señalado, se excluyen como sujetos de derechos a las personas jurídicas. La razón debe buscarse en la naturaleza de la información de que estamos hablando. En rigor, sólo sobre las personas naturales puede existir información de carácter personal. Esto aparece reafirmado en el artículo 2°, letra f, que define datos de carácter personal.

Hay que tener presente que los legisladores optaron por identificar a los sujetos de derechos como "titulares de los datos", modificando así el proyecto que fuera aprobado por la Cámara de Diputados que confería la titularidad de los datos a los administradores de bancos de datos. De esta forma, la ley reconoce que existe un nexo entre la persona y el dato o información que concierne a ella.

¿Cuál es la naturaleza de este nexo? Para algunos autores existiría un verdadero derecho de propiedad sobre estos datos, considerando la protección constitucional sobre toda clase de bienes corporales como incorporales. Sin embargo para otros parece que debe descartarse que estemos aquí frente a una propiedad, ya que el dato como tal, con independencia del soporte físico, electrónico o informático en el que se encuentre recogido, no es ni una cosa corporal ni una cosa incorporal (derecho real o personal) ni una cosa intelectual (como una obra literaria o una marca o invención). El dato es un conocimiento adquirido por un tercero sobre una persona en cuanto representado funcionalmente para ser comunicable a un número indeterminado de usuarios. La persona tiene un cierto poder de control, entonces, no sobre el dato en sí, que es incorpóreo, sino sobre los medios empleados para su representación y comunicación.

Esta idea de propiedad será analizada posteriormente, sin embargo si consideramos que los datos tienen una apreciación pecuniaria, consideramos que

existiría por ente un bien, el que se encontraría resguardado por el derecho a la propiedad.

Para un estudio más sistematizado del Hábeas Data Chilenos debemos:

1) En primer lugar debemos analizar los derechos que aparecen legalmente recogidos en la ley.
2) en segundo término haremos referencia a la forma de ejercicio de dichos derechos.
3) Pasaremos luego a exponer la acción cautelar que se ha conocido en doctrina como hábeas data o amparo digital y que la ley regula en su artículo 16
4) Verificaremos el recurso del particular para hacer efectiva la responsabilidad civil del responsable de banco de datos personales en caso de incumplimiento de los deberes que establece la ley .
5) Terminaremos con algunas reflexiones conclusivas sobre la naturaleza única o múltiple de estos derechos y su relación con la protección de la vida privada y la acción constitucional de protección.

1) DERECHOS LEGALMENTE RECONOCIDOS

Nos parece que los derechos que la ley concede son los de acceso, de modificación, de bloqueo y de cancelación de datos. A ellos deben agregarse dos que son variantes de los anteriores: el de copia y el de aviso a terceros. Finalmente, existe un supuesto restringido de derecho de oposición al tratamiento de datos.

- DERECHO DE INFORMACIÓN O ACCESO

El llamado derecho de acceso significa tener la posibilidad de conocer la existencia de un determinado registro o banco de datos y la información que posee sobre una determinada persona.

El derecho, según el artículo 12 de la ley, consiste en la "facultad de exigir... información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente" (art. 12 ley N° 19.628).

En consecuencia, el derecho puede ejercerse con varios objetivos, a saber:

– Para saber si un determinado banco de datos contiene información sobre el

requirente;

– Para saber el contenido de la información que posee el banco sobre el requirente;

– Para conocer el origen de los datos;

– Para conocer el destinatario para el cual fueron recogidos;

– Para conocer el propósito u objeto de su almacenamiento, y

– Para conocer las personas u organismos a los cuales los datos son transmitidos, esto es, comunicados, de manera regular.

Entendemos que el requirente en el ejercicio de este derecho deberá indicar si necesita toda la información referida. Si nada dice, lo razonable es pensar que el derecho de acceso se satisface con la información sobre la existencia y contenido de datos sobre el requirente en un determinado banco.

- DERECHO DE MODIFICACIÓN

La ley denomina derecho de modificación a la facultad que tiene un titular de datos para alterar un registro de un banco de datos.

La necesidad de modificar puede provenir de las siguientes causas:

– Existencia de un dato erróneo o inexacto (art. 12.2): aunque la ley diferencie los vocablos, nos parece que coinciden; lo erróneo es inexacto y viceversa. Por ejemplo, la persona se llama Pedro y no Juan, o es chilena y no brasileña.

– Existencia de un dato equívoco (art. 12.2): se trata de una información que puede interpretarse en maneras diversas por falta de claridad. Por ejemplo, si aparece como oficio de una persona la de "procurador".

– Existencia de un dato incompleto (art. 12.2): es una información que aunque exacta es parcial. Por ejemplo, si se contempla que una persona viajó al extranjero, pero no se registra su regreso al país.

En verdad, sólo tratándose de los datos erróneos o equívocos cabe hablar de derecho a la modificación. Cuando existen datos incompletos, no hay propiamente modificación, sino complementación o integración. No obstante, la ley habla en general de modificación también en el caso de los datos incompletos: "En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen" (art. 12.2).

- DERECHO DE BLOQUEO

El derecho a bloquear los datos consiste en la facultad de exigir que se suspenda temporalmente el tratamiento de datos que estén almacenados, es decir, que se suspenda cualquier operación o conjunto de operaciones o procedimientos técnicos destinados a utilizar los datos en cualquier forma (art. 2°, letras b y o).

El bloqueo no procede de manera general para todos los titulares de datos, sino sólo en los casos precisos determinados por la ley. Éstos son: 1°) que se trate de datos que el titular haya proporcionado voluntariamente; 2°) que se trate de datos que se usen para comunicaciones comerciales. Respecto de este segundo caso, debe tenerse en cuenta que la ley exime de la necesidad de obtener autorización del interesado para registrar sus datos, entre otros supuestos, a los listados de datos "que sean necesarios para comunicaciones comerciales de respuesta directa" (art. 4°.5).

En los dos casos señalados, el titular puede exigir al respectivo banco de datos que su información deje de ser utilizada de un modo temporal (art. 12.4).

No indica la ley el plazo por el cual procede el bloqueo, pero debe entenderse que la duración es indefinida, es decir, hasta que exista expresión de voluntad en contrario del requirente. Esta conclusión se impone si se observa, como veremos a continuación, que por las mismas causales el titular puede pedir, no ya el bloqueo temporal, sino la eliminación o cancelación definitiva de sus datos.

- DERECHO DE CANCELACIÓN

La eliminación o cancelación de los datos es "la destrucción de os datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello" (art. 2°, letra h).

El derecho a exigir la eliminación o cancelación procede en diferentes supuestos, a saber:

- Si el almacenamiento carece de fundamento legal (art. 12.3); es decir, por regla general si no aparece autorizado ni por el titular ni por la ley N° 19.628 ni por otra disposición legal.

- Si los datos tienen el carácter de caducos (art. 12.3), esto es, si han perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consignan (art. 2°, letra d).

- Si los datos han sido proporcionados voluntariamente o se usan para comunicaciones comerciales (art. 12.4).

- DERECHO DE COPIA

Cuando el titular ejerce el derecho de modificación o cancelación, la ley le reconoce además el derecho de obtener copia del -registro alterado en la parte pertinente (art. 12.5). Mejor que copia, o que la ley exige es que se otorgue al particular afectado la representación en soporte físico del dato sobre el que se ha producido la modificación, o del resto del asiento referido a él, del cual se ha eliminado un elemento sobre el que se pidió la cancelación.

La obtención de esta copia es gratuita para el solicitante. Pero Para evitar abusos se establece que si, efectuada una primera modificación o cancelación y ejercido el derecho de copia respecto de se ejerce nuevamente el derecho de modificación o cancelación, el particular deberá pagar la copia, salvo que haya transcurrido un plazo mínimo de seis meses entre la primera y la segunda petición. La ley dice que el plazo de seis meses se cuenta "desde la precedente oportunidad en que se haya hecho uso de este derecho" (art. 12.5). Nos parece que el momento desde el cual se debe contar este plazo no es la fecha de la petición, sino aquella en la que el banco de datos otorgó la respectiva copia, ya que sólo en este momento puede decirse que el solicitante "usó" (ejerció) este derecho.

- DERECHO DE AVISO A TERCEROS

La ley supone que los datos que son objeto del derecho de modificación o cancelación pueden haber sido comunicados por el banco de origen a otras personas determinadas o determinables. De allí que obligue al responsable del banco a avisarles a esas personas la operación efectuada "a la brevedad posible" (art. 12.6).
En caso de que no sea posible determinar las personas a las que se hubieren comunicado los datos, el responsable deberá poner "un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos" (art. 12.6). La norma es poco precisa, y en caso de discordia será materia a resolver por el juez.

- DERECHOS DE OPOSICIÓN

Aunque en título aparte, la ley menciona otro derecho de los titulares de los datos, es el derecho de oposición, según el cual, "El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión" (art. 3°.2).

2) CONDICIONES DE EJERCICIO DE LOS DERECHOS

- LEGITIMACIÓN ACTIVA

La legitimación activa de estos derechos parece corresponder a las personas naturales que la ley llama titulares de datos.

No obstante, pensamos que el derecho de acceso o de información es más extensivo ya que corresponde, como el mismo texto del inciso primero del artículo 12 señala, a "toda persona". Esto es así por cuanto no es necesario demostrar, para hacer uso de este derecho, que existe un dato del cual se es titular. Justamente, el derecho consiste en la posibilidad de una persona de indagar sobre la existencia de información suya registrada y tal gestión puede concluir positiva como negativamente. En este último evento, habrá hecho uso del derecho de información sin tener la cualidad de titular de datos.

Los derechos de modificación, bloqueo y cancelación, en cambio, corresponden a quienes efectivamente tengan un nexo con una información personal que les atinge.

No pueden ser ejercidos por terceros para la protección de otros beneficiarios. La ley en el artículo 12 habla de derechos sobre "datos relativos a su persona", es decir, a la persona natural interesada.

¿Procederá la representación voluntaria o legal en el ejercicio de estos derechos? ¿Podrán, por ejemplo, el padre o la madre que ejerce la patria potestad ejercer estos derechos en representación del menor? ¿O un mandatario en representación de su mandante? Aunque podría objetarse que estamos frente a derechos de la personalidad que no admiten representación, somos de la opinión de que deben en este caso aplicarse las reglas generales de la representación y del mandato. De hecho, en forma explícita la ley señala que para el tratamiento de datos personales se admite el mandato, el que se rige por las reglas generales (art. 8°.1).

Únicamente respecto del derecho de copia, la ley exige ejercicio personal: "El

derecho a obtener copia gratuita sólo podrá ejercerse personalmente" (art. 12.5). A contrario sensu, debemos admitir entonces que los restantes derechos admiten representación.

- ¿ANTE QUIÉN SE HACEN VALER?

Conforme al artículo 12, los derechos que reconoce la ley se pueden exigir "a quien sea responsable de un banco..." (art. 12.1). Es decir, se ejercen frente a:

- La persona natural que mantenga un registro o banco de datos;
- La persona jurídica de derecho privado que mantenga el mismo registro, o
- Un organismo público que mantenga el mismo registro.

Tratándose de personas naturales o personas jurídicas es claro a quién debe dirigirse la petición. No parece claro el sujeto pasivo si se trata de organismos públicos que carezcan de personalidad jurídica propia. Pareciera que la exigencia debe hacerse a la autoridad superior del respectivo organismo, sin perjuicio de que las acciones legales que procedan deberán interponerse en contra del Consejo de Defensa del Estado como representante del Fisco.

Debe señalarse que la ley facilita el acceso al conocimiento de registros de organismos públicos, estableciendo a su vez un registro público de dichos registros que queda a cargo del Servicio de Registro Civil e Identificación (art. 22).

Se ha contemplado también el caso de un banco de datos de utilización plural por parte de varias empresas o instituciones. De esta manera, se dispone que si los datos personales están en un banco al cual tienen acceso diversos organismos, "el titular puede requerir información a cualquiera de ellos" (art. 14). Como la norma es restringida a la petición de "información" pensamos que los restantes derechos de modificación, bloqueo y cancelación deberán ejercerse ante el responsable del banco mismo, y no ante alguna de las entidades que tienen acceso a él.

- FORMAS DE REQUERIMIENTO. GRATUIDAD

La ley no regula la forma en que debe ejercerse el requerimiento, por lo que debemos entender que puede tratarse de petición verbal o escrita, en la que se especifique claramente el objeto de la solicitud: acceso, modificación, bloqueo, cancelación, copia u oposición.

La ley establece la gratuidad en el uso de estos derechos, por lo que el costo que represente su satisfacción deberá soportarlo el respectivo responsable del banco de datos: "La información, modificación o eliminación de los datos serán absolutamente gratuitas" dispone el artículo 12.5 de la ley.

Es curioso que no se haya incluido el derecho a bloqueo dentro de esta enumeración. Interpretada literalmente la norma, opción que parece imponerse por el carácter excepcional de la gratuidad, deberíamos sostener que en caso de bloqueo el costo respectivo debe soportarlo el peticionario.

En cuanto al derecho de copia la gratuidad está condicionada a que transcurra un plazo mínimo de seis meses entre cada ejercicio
de este derecho (art. 12.5).

- IRRENUNCIABILIDAD

Los derechos que establece la ley N° 19.628 son de orden público, ya que se relacionan con la garantía constitucional del respeto a la vida privada. Esto queda de manifiesto en lo que preceptúa el artículo 13: "El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención".

De esta manera, se prohíbe la exclusión o limitación del ejercicio de estos derechos. Cualquier pacto en contrario adolecerá de nulidad absoluta, conforme a los artículos 10 y 1466 del Código Civil.

De nuevo al legislador se le escapan derechos que no aparecen en esta disposición, como son el derecho de copia del artículo 12.5 y el derecho de oposición del artículo 3°.2. A pesar de la falta de mención en el artículo 13, opinamos que lo mismo debe predicarse de estos derechos, porque no hay razón para hacer diferencias y porque se aplica el mismo principio de que se trata de facultades que tienen el carácter de normas de orden público.

- CESIÓN Y TRANSMISIBILIDAD

No ha tratado la ley el problema de si los derechos que ella establece son cesibles, a título gratuito u oneroso, o si son transmisibles mortis causa.

La cesión de los derechos no parece que pueda ser admitida tratándose de

facultades tan esencialmente vinculadas a la persona. Además, no imaginamos en qué supuestos podría un tercero adquirir el derecho de otro para pedir acceso, modificación o cancelación de datos que conciernen al cedente.

Un poco más problemático puede resultar el caso de la transmisión mortis causa. ¿Fallecido el titular de los datos, pueden sus herederos ejercer los derechos del artículo 12? El carácter personalísimo de los derechos indicaría una respuesta negativa: los derechos se extinguirían con la persona del titular. Pero es cierto que los herederos pueden tener interés en la rectificación de un asiento relativo a su causante, que puede afectar incluso la posibilidad de obtener créditos para la sucesión.

Pensamos que una solución razonable puede ser considerar que los herederos no pueden actuar ejerciendo el derecho de su causante, puesto que éste ya se ha extinguido, pero sí podrían ejercer esos derechos iure proprio, es decir, porque al referirse a su causante los datos han pasado también a afectarles y concernirles;

Podrán entonces alegar que ellos son ahora los titulares de dichos datos.

Los derechos de acceso, modificación, bloqueo o cancelación no podrán ejercerse en dos casos de excepción que establece la ley. Éstos son:

1°) Si el ejercicio del derecho impide o entorpece el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido;

2°) Si el ejercicio del derecho afecta la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional (art. 15.1).

Los derechos de modificación, bloqueo o cancelación no pueden además ejercerse respecto de datos almacenados por mandato legal, salvo en los casos contemplados en la ley que ordena ese almacenamiento (art. 15.2). Debe notarse que, respecto de tales registros, procede el derecho a la información o acceso.

3) EL AMPARO DIGITAL O HÁBEAS DATA

- CAUSALES POR LAS QUE PROCEDE

De acuerdo con el artículo 16 de la ley, la acción de amparo procede en dos supuestos:

1°) Si el responsable del banco de datos no se pronuncia sobre la solicitud del requirente dentro de los dos días hábiles siguientes.

2°) Si el responsable deniega la solicitud. El procedimiento será especial si la causal de

denegación es la seguridad de la Nación y el interés nacional.

- NATURALEZA Y CARACTERES DE LA ACCIÓN

El hábeas data ha surgido en las últimas décadas prácticamente en todas las legislaciones para otorgar protección expedita al que se ve afectado por el tratamiento de datos de carácter personal, bajo el modelo del recurso de amparo o hábeas corpus que protege la libertad personal.

Se trata, por tanto, de una acción judicial específica y autónoma, de objeto definido y de tramitación concentrada.

No pensamos que se trate de una acción propiamente cautelar, ya que la sentencia que se dicte producirá cosa juzgada tanto material como formal. Incluso la sentencia incluye la posible aplicación de sanciones.

- OBJETO DE LA ACCIÓN

La res petita en la acción de hábeas data es según la ley el "amparo a los derechos consagrados en el artículo precedente" (art. 16.1). El artículo anterior, el 15, menciona los derechos de información, modificación, bloqueo y cancelación. Cualquiera de ellos puede ser objeto de la acción de amparo digital.

No son mencionados en el artículo 15 los derechos de copia y de oposición. No parece haber razón para excluirlos de esta protección específica. Respecto del derecho de copia, puede decirse que está implícito en el artículo 15 ya que nace del ejercicio del derecho de modificación o cancelación.

Este recurso interpretativo no podemos aplicarlo al derecho de oposición que establece el artículo 3°.2, por lo que parece quedar excluido del ámbito de protección que brinda esta acción. Ello no obsta para que el derecho pueda ejercerse mediante una acción ordinaria de responsabilidad civil o mediante la acción constitucional de protección.

Pero aparte del amparo de los derechos referidos, la acción puede tener por objeto además la indemnización de los perjuicios causados (art. 23) y la constatación de una responsabilidad infraccional sobre la que proceden sanciones administrativas (art. 16 in fine).

- TRIBUNAL COMPETENTE

La competencia corresponde al juez de letras en lo civil del lugar del domicilio del responsable del banco de datos.
Aunque en la tramitación de la ley se pensó en dar más facilidades al particular afectado otorgando competencia al tribunal de su propio domicilio, primó la opinión de que debían mantenerse las reglas generales de competencia que privilegian el domicilio del demandado (art. 134 COT).

- LEGITIMACIÓN ACTIVA Y PASIVA

La acción puede interponerse sólo por el "titular de los datos" (art. 16.1). De nuevo, hacemos la advertencia que si se trata del derecho de acceso o información la acción podrá interponerse por cualquier persona que tema estar incluida en la respectiva base de datos personales.
Lo que hemos dicho anteriormente en cuanto a la representación, a la cesión y la transmisión de estos derechos, resulta plenamente aplicable para el ejercicio de la acción que los ampara.
La acción debe interponerse contra el responsable del registro o banco de datos. Si se trata de persona jurídica habrá que demandar a quienes ostenten su representación judicial; si se interpone respecto de un organismo público sin personalidad jurídica propia habrá que emplazar al Consejo de Defensa del Estado.

- PROCEDIMIENTO

a) Reclamación de amparo
La reclamación debe señalar la infracción cometida y los hechos que la configuran. Entendemos que para la ley el no respeto de los derechos por ella concedidos es suficiente para hablar de infracción a sus normas. Aunque la ley no lo diga expresamente, se deduce que la reclamación ha de ser escrita.
Además, la reclamación debe ir acompañada "de los medios de prueba que los acrediten, en su caso" (art. 16, letra a). La expresión "en su caso" denota que este requisito no es perentorio y que dependerá de la naturaleza de la infracción el que existan o no medios de prueba que puedan acompañarse.

b) Notificación y contestación

La reclamación debe notificarse por cédula dejada en el domicilio del responsable del banco de datos (art. 16, letra c). No parece oportuno haber hecho excepción a la regla general de que la primera notificación debe hacerse personalmente.

El plazo para que el banco de datos conteste, presentando sus descargos, es de cinco días hábiles desde la notificación. La contestación será también hecha por escrito, y a ella deben acompañarse los medios de prueba que acrediten los hechos en los que se funda (art. 16, letra b).

c) Audiencia de prueba

Si el banco de datos no dispone de medios de prueba para acompañar en su contestación, debe indicar en ella esta circunstancia y el juez fijará una audiencia dentro del quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada (art. 16, letra c). Pensamos que esta audiencia también debe practicarse cuando sea el requirente el que no haya podido acompañar en la reclamación sus medios de prueba, si expresa esta circunstancia y ofrece rendir prueba.

d) Sentencia

La sentencia definitiva debe dictarse dentro del tercer día hábil de vencido el plazo para contestar, se hayan o no presentado descargos, o desde que vence el plazo fijado para la audiencia de prueba (art. 16, letra d).

La sentencia definitiva debe notificarse por cédula (art. 16, letra b).

e) Recursos

La resoluciones dictadas en el proceso se notifican por el estado diario y no son apelables (art. 16, letra e).

La sentencia definitiva es apelable en ambos efectos. El recurso de apelación debe interponerse en el plazo de cinco días (aunque la ley no lo diga debemos entender hábiles) desde la notificación de la parte que entabla el recurso. El escrito de la apelación deberá contener los fundamentos de hecho y de derecho y las peticiones concretas que se formulan (art. 16, letra f). Al decir esto, la ley no hace más que repetir a la letra el artículo 189 inciso primero del Código de Procedimiento Civil

La ley agrega que el Presidente de la Corte de Apelaciones debe ordenar dar

cuenta preferente del recurso, sin esperar la comparecencia de las partes (art. 16, letra g). En principio, el recurso se ve en cuenta, pero la Sala que debe conocer, si lo estima conveniente o se le solicita con fundamento plausible, puede ordenar traer los autos en relación para oír los alegatos de los abogados de las partes. En tal caso, la causa se agrega extraordinariamente a la tabla de la misma sala (art. 16.4).

La sentencia de segunda instancia no es susceptible de los recursos de casación (art. 16, letra h). Parece que procedería entonces el recurso de queja, conforme con lo dispuesto en el artículo 545 del Código Orgánico de Tribunales.

f) Procedimiento especial en caso de seguridad de la Nación o interés nacional

Si la causal que el responsable de los datos ha invocado para denegar la solicitud del requirente es la seguridad de la Nación o el interés nacional, la reclamación debe deducirse directamente ante la Corte Suprema.

La Corte debe pedir informe al responsable del modo más expedito y le fijará un plazo. Vencido el plazo resolverá en cuenta.

Si se recibe la causa a prueba, ésta debe consignarse en un cuaderno separado y reservado. Este cuaderno mantendrá el carácter de reservado si la reclamación es denegada (art. 16.3).

La sala de la Corte Suprema puede también, si lo estima conveniente o se le solicita con fundamento plausible, ordenar traer los autos en relación, caso en el cual la causa se agrega extraordinariamente a la tabla. Pero el Presidente de la Corte debe disponer que la audiencia no sea pública (art. 16.5).

- CONTENIDO Y EJECUCIÓN DE LA SENTENCIA

La sentencia que acoge la reclamación el juez debe fijar un plazo prudencial para que el banco de datos dé cumplimiento a lo resuelto.
Además puede sancionar la infracción con una multa de una a diez unidades tributarias mensuales (art. 16.5) y determinar los perjuicios si le han sido solicitados (art. 23).

En caso de que el responsable no cumpla dentro del plazo en la forma que decrete el tribunal, puede aplicar multas de dos a cincuenta unidades tributarias mensuales. Y si el requerido es un organismo público, el juez puede sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

SI analizamos esta norma podremos señalar anticipadamente como crítica que

las sanciones son realmente muy poco significativas.

4) RESPONSABILIDAD CIVIL Y DERECHO A LA INDEMNIZACIÓN DE PERJUICIOS.

- NATURALEZA DE LA RESPONSABILIDAD

El artículo 23 de la ley establece que la persona natural o jurídica privada o el organismo público responsable del banco de datos debe indemnizar los perjuicios que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido o, en su caso, lo ordenado por el tribunal.

Como la ley no establece mayores precisiones sobre esta responsabilidad, debemos indagar sobre su naturaleza para ver cuáles reglas del derecho común le son aplicables.

En primer lugar, hay que dilucidar si estamos frente a una responsabilidad contractual o extracontractual. La respuesta no puede ser sino que se trata de un supuesto de responsabilidad extracontractual. Aunque la presencia de una autorización expresa y por escrito de un titular de datos para la utilización de éstos podría hacer surgir dudas sobre si hay un contrato que fija el marco de actuación entre las partes, pensamos que dicha autorización es un acto unilateral y no la aceptación de un acuerdo contractual. Por lo demás, la ley se refiere a la responsabilidad civil como aneja a la responsabilidad infraccional (art. 23.2), lo que sólo se condice con la responsabilidad civil extracontractual.

En lo no previsto, por lo tanto se aplicarán las normas de los artículos 2314 y siguientes del Código Civil.

Una segunda cuestión es la relativa al factor de imputación de la responsabilidad: ¿estamos aquí frente a un nuevo supuesto de responsabilidad objetiva, respecto del cual el perjudicado sólo debe probar los perjuicios, el acto injusto y el nexo de causalidad pero no la culpa o dolo del agente? De la expresión perentoria que aparece en el artículo 23: "deberá indemnizar", alguien podría deducir que estamos ante un caso de objetivación de la responsabilidad. Nos parece que ello no es así, por varias razones:

1°) El régimen común de la responsabilidad es el principio de la culpa, y para que haya

excepción a este principio debe existir una norma inequívoca al respecto.
2°) La expresión "deberá indemnizar" no dice más que, cumplidos los presupuestos de la responsabilidad, nace la obligación de indemnizar.
3°) La responsabilidad civil en el artículo 23 aparece como aneja a la infracción legal, y ésta no puede existir sin negligencia o culpa. No hay responsabilidad contravencional sin dolo o culpa.
4°) La historia de la tramitación de la ley confirma esta conclusión, pues consta que se agregó el calificativo de "indebido" al tratamiento de datos que produce responsabilidad, justamente para enfatizar la necesidad de la aplicación de las reglas generales de la responsabilidad por culpa. Se lee en el Informe de la Comisión Mixta: "La Comisión Mixta estimó apropiada la sugerencia de ACTI de precisar que la indemnización de perjuicios que se consagra procederá cuando exista un tratamiento 'indebido' de los datos de una persona, ya que ello despeja cualquier duda acerca de la aplicación de las reglas generales de responsabilidad extracontractual consagradas por el Código Civil".

- PERJUICIOS INDEMNIZABLES

El artículo 23 aclara que se puede obtener indemnización de todos los perjuicios causados por el tratamiento indebido de los datos, incluyéndose tanto la reparación de los daños materiales como de los daños morales.

Debe considerarse que ya al realizarse la modificación o cancelación de los datos hay una forma de reparación de los daños, y que si se pretende obtener una indemnización adicional deberán probarse estos perjuicios, incluso los morales. El juez apreciará esta prueba en conciencia (art. 23.2).

- TRIBUNAL COMPETENTE Y PROCEDIMIENTO

La acción para solicitar indemnización de perjuicios puede deducirse conjuntamente con la de amparo del artículo 16 ante el mismo tribunal y con el mismo procedimiento regulado para conocer de ella. Procede en este caso diferir la discusión sobre el monto de los perjuicios en la ejecución del fallo o en otro juicio, de acuerdo con el artículo 173 del Código de Procedimiento Civil (art. 23.1).

Si la responsabilidad surge por una conducta infraccional que no es de las

señaladas en el artículo 16 (y en el art. 19 que se remite a él), según el artículo 23.2, debe aplicarse el procedimiento sumario tanto para el establecimiento de la infracción como para la indemnización de perjuicios. No se indica quién es el juez competente ni tampoco las sanciones que proceden por estas infracciones no mencionadas en los artículos 16 y 19, por lo que vemos muy difícil que pueda articularse esta responsabilidad.

Podría sí ejercerse en forma separada la acción de responsabilidad civil, y en ese caso será competente el juez de letras en lo civil del domicilio del demandado y se aplicará el procedimiento sumario (art. 23.2).

- MEDIDAS CAUTELARES

El artículo 23.2 dispone que "el juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece". Parece curioso que esta norma relativa al amparo de los derechos se encuentre en el artículo que regula la responsabilidad civil, pues debió haberse dispuesto en general para todos los procedimientos.

5) DERECHOS DE LOS TITULARES DE DATOS Y LA PROTECCIÓN A LA VIDA PRIVADA

- ¿UN ÚNICO DERECHO DE FACULTADES DIFERENCIADAS?

Analizada ya la preceptiva de la ley, se nos presentan varias cuestiones de interés teórico, pero con repercusiones prácticas.

En primer lugar, hay que resolver si estamos frente a un único derecho de protección de datos personales o ante un haz de derechos diversos y autónomos entre sí.

La cuestión tiene relieve práctico pues si se trata de un derecho único, aunque con diversas modalidades de ejercicio o facultades, la petición de una de estas modalidades de ejercicio incluye necesariamente las otras, si es del caso. En cambio, si se trata de derechos diferentes, debe plantearse una acción para cada derecho. En el primer caso, la sentencia producirá cosa juzgada sobre todas las modalidades de aplicación del derecho; mientras que en el segundo ella sólo se aplicará a la facultad

concreta que se discutió en el juicio.

En nuestra opinión, se trata de derechos diferentes, aunque todos ellos tienen en común la finalidad de proteger un interés jurídico común: la protección de la intimidad e identidad frente al tratamiento de datos personales. Solamente el derecho de copia puede conceptualizarse como una facultad derivada de los derechos de modificación o eliminación.

- ¿DERECHOS DIVERSOS CON TUTELA UNIFICADA?

La tutela judicial a través de una sola acción de amparo no necesariamente obliga a pensar que estamos frente a un solo derecho, siguiendo la regla clásica de que a todo derecho corresponde una acción.

La acción de amparo digital o hábeas data es una forma de tutela judicial amplia que cubre la protección de un conjunto de derechos que, aunque con fisonomías propias, tienen en relación que responden al mismo interés.

- ¿APLICACIÓN O COMPLEMENTACIÓN DE LA GARANTÍA CONSTITUCIONAL DEL RESPETO A LA VIDA PRIVADA?

Nos queda por determinar si los derechos que reconoce la ley N° 19.628 a los particulares son aplicaciones particulares del derecho al respeto y protección de la vida privada consagrado en el artículo 19, N° 4 de la Carta Fundamental, o si, por el contrario, vienen a complementar esa preceptiva innovando así en la protección del individuo.

Debe señalarse en abono de la segunda opinión que en varias Constituciones se prescribe en forma especial el derecho al amparo digital o hábeas data.

La tramitación de la ley, que partió como una normativa dirigida a proteger el derecho a la intimidad y se convirtió finalmente en una ley de protección de datos, nos habla también de este problema. La dicotomía de objetivos se advierte en su publicación en el Diario Oficial en el que curiosamente se alude a la ley "sobre protección de la vida privada", en tanto que el decreto de promulgación señala que el proyecto de ley sancionado se titula "protección de datos de carácter personal".

Pareciera que, si bien en parte los derechos de la ley N° 19.628 son formas de aplicación del derecho general al respeto a la vida privada, en cuanto permiten excluir

datos que se refieren al ámbito de intimidad que una persona razonablemente reserva para sí y su entorno familiar, por otro lado, también sirven para resguardar el llamado "derecho a la identidad", que no está como tal contemplado en el artículo 19 N° 4 de la Constitución, pero que puede caber en la alusión que hace el precepto al respeto de la "vida pública" de la persona. Los derechos de modificación tienden muchas veces a resguardar este derecho a la identidad en la vida pública, más que el derecho a la intimidad.

Por las razones expuestas, el recurso de protección que el artículo 20 de la Constitución reserva para las amenazas, privaciones o perturbaciones del derecho al respeto y protección a la vida privada puede interponerse en los casos de infracciones a la ley 19.628 si el atentado al derecho se comete a través del tratamiento de datos de carácter personal. La deducción del recurso y su fallo no obstará a que posteriormente el particular pueda ejercer la acción de amparo digital o hábeas data, ya que el artículo 20 de la Constitución señala expresamente que la acción constitucional es "sin perjuicio de los demás derechos que pueda hacer valer ante la autoridad o los tribunales correspondientes". Se aplicará lo mismo que sucede con el llamado amparo económico.

Para aquellos atentados que no son dirigidos propiamente a la vida privada, sino que tienden a distorsionar la presentación de la persona en la vida social, procederá también, a nuestro juicio, el recurso de protección, esta vez por afectación del derecho al respecto a la vida pública, sin perjuicio de la procedencia igualmente del amparo digital que establece la ley N° 19.628. Para el caso de no considerarse procedente la interpretación que hacemos de la locución "vida pública" del artículo 19 N° 4 de la Constitución, la acción de la ley N° 19.628 será el único medio jurisdiccional de que disponga el afectado para resguardar el derecho a su identidad.

La tutela de la información digitalizada como una forma especial de protección a la vida privada y como un complemento a ella (derecho a la identidad) debe considerarse un paso positivo en la configuración de recursos efectivos que resguarden a las personas de los peligros que enfrentan ante una utilización abusiva y dañina de las nuevas tecnologías del mercado de la información.

6) Propiedad Privada, Libre Iniciativa Particular y respeto a la Vida Privada

El N° 21 del artículo 19 de la Constitución Política de la República, en su inciso primero, asegura a todas las personas "el derecho a desarrollar cualquiera actividad económica que no sea contraria a la moral, al orden público o a la seguridad nacional, respetando las normas legales que la regulen". Los titulares del derecho son, en principio, únicamente las personas privadas, sean éstas naturales o jurídicas, pero no el Estado y sus organismos, pues éstos únicamente pueden desarrollar o participar en actividades empresariales si una ley de *quórum* calificado los autoriza. Así lo dispone el inciso segundo del mismo precepto.

Como todo derecho de libertad, el de desarrollar cualquiera actividad económica lícita es un derecho que se tiene frente a todos, *erga omnes*, e implica que existe una obligación general de no hacer que recae sobre autoridades y particulares. Todos los obligados, entonces, han de abstenerse de cualquier comportamiento lesivo al derecho que se reconoce, el cual faculta a sus titulares para actuar libre de interferencias, dentro, naturalmente, de las regulaciones legales establecidas. Pero incluso estas regulaciones, conforme lo garantiza el N° 26 del artículo 19 de la Constitución Política, no pueden ser excesivas y llegar a afectar la esencia del derecho o su libre ejercicio.

Evans de la Cuadra explica certeramente quiénes son los titulares del derecho y los obligados a respetarlo:

"Si la Constitución asegura a todas las personas el derecho de desarrollar libremente cualquier actividad económica, personalmente o en sociedad, organizadas en empresas, en cooperativas o en cualquier otra forma de asociación lícita, con el único requisito de respetar las normas que regulan la respectiva actividad [...], la obligación de no atentar en contra de esta garantía no sólo se extiende al legislador, al Estado y a toda autoridad, sino también a otros particulares que actúen en el ámbito de la economía nacional. Una persona, natural o jurídica, que desarrolla una actividad económica dentro de la ley, sólo puede salir de ella voluntariamente o por ineficiencia empresarial que la lleve al cierre o a la quiebra".[61]

Este derecho, denominado por la Comisión de Estudio de la Nueva Constitución Política de la República como "libre iniciativa privada para desarrollar cualquiera actividad económica" y usualmente "derecho a desarrollar cualquiera actividad

[61] Evans de la Cuadra, Enrique: "Los derechos constitucionales", Santiago de Chile 1986, tomo II, pág. 318.

económica lícita", significa, entonces, que toda persona privada, sea ésta persona natural o jurídica, tiene la facultad de iniciar y mantener con libertad, exenta de toda interferencia indebida, cualquiera actividad lucrativa en las diversas esferas de la vida económica. Garantiza, por consiguiente, la norma constitucional, entre otras actividades, la explotación de recursos naturales, realización de actividades productivas, de servicios y de comercialización de todo tipo de bienes, bajo dos grandes condiciones: la primera, que la actividad a realizar no sea considerada en sí misma, ilícita, y son tales sólo las que la propia Constitución menciona genéricamente, esto es, las contrarias a la moral, al orden público y a la seguridad nacional, y la segunda, que la actividad económica a realizar se ajuste a las normas legales que la regulen.

Los límites del derecho a desarrollar actividades económicas son, como se ha indicado, dos: que la actividad sea lícita, y que no infrinja las normas legales que la regulen. En cuanto a lo primero, Evans de la Cuadra estima que corresponderá a los tribunales de justicia pronunciarse cuándo ciertas actividades hayan de ser consideradas contrarias a la moral, al orden público o la seguridad nacional, pues existe una imposibilidad de hacerlo previamente mediante una ley.

"No creemos –dice– que sea posible una ley que complemente estas limitaciones, ya que, o bien aborda con criterio general la explicitación de los conceptos de moral, orden público, etcétera, lo que no parece propio de la tarea legislativa, o bien busca precisar las actividades específicas que serán prohibidas, lo que implica entrar en una regulación casuista imposible de concebir".[62]

Entre los derechos reconocidos constitucionalmente que toda ley que regula una actividad económica debe respetar se encuentra el derecho de propiedad. Ello significa que la normativa legal que enmarca la realización de una actividad determinada, como es la de tratamiento de datos, no debe afectar los derechos de propiedad existentes. De ahí la necesidad de precisar cuál es el ámbito de la protección constitucional de la propiedad.

Un primer aspecto del que puede llamarse estatuto constitucional de la propiedad es el acceso amplio a la titularidad de todo tipo de propiedades. Por ello, la Constitución asegura a toda persona en el N° 23 del artículo 19 "La libertad para adquirir el dominio de toda clase de bienes, excepto aquellos que la naturaleza ha hecho comunes a todos los hombres o que deban pertenecer a la Nación toda y la ley lo declare así". Es el

[62] Evans de la Cuadra, op. cit., pág. 318.

llamado derecho a la propiedad, que es la norma general en materia de acceso al dominio, y es la base o supuesto que permite la existencia de derechos de propiedad sobre cualquier bien susceptible de apropiación.

Respecto al derecho de propiedad, la norma que lo reconoce y protege, como es sabido, es el N° 24 del artículo 19, disposición esta que en su inciso primero asegura a toda persona "El derecho de propiedad en sus diversas especies sobre toda clase de bienes corporales o incorporales", que, luego, en el inciso segundo establece la regulación y, también, la limitación por ley de la propiedad para hacer efectiva su función social, y que en el inciso tercero reafirma la protección amplia de toda propiedad al disponer que "Nadie puede, en caso alguno, ser privado de su propiedad, del bien sobre que recae o de alguno de los atributos o facultades esenciales del dominio, sino en virtud de ley general o especial que autorice la expropiación por causa de utilidad pública o de interés nacional, calificada por el legislador".

Es comprensible que como resultado de la aplicación de las nuevas normas constitucionales relativas a la libertad para adquirir el dominio de toda clase de bienes, y al derecho de propiedad en sus diversas especies sobre toda clase de bienes corporales e incorporales, la jurisprudencia haya reconocido y otorgado protección de modo amplísimo sobre diversos y numerosos derechos de significación patrimonial.

En tal sentido, y sin que la enumeración sea exhaustiva, puede recordarse cómo además de la propiedad de derechos reales –entre ellas la del derecho real de hipoteca y la de servidumbres– se ha admitido la propiedad de numerosísimos derechos personales, sea que se tengan respecto de un particular o de una institución pública, sin importar tampoco que tengan su fuente en contratos particulares, en la aplicación de normas legales o en disposiciones de índole administrativa. Incluso, en casos que pueden resultar audaces pero que no son sino el producto de la aplicación de las normas constitucionales a nuevas situaciones de la vida económica y social, se ha aceptado la propiedad sobre una concesión, la propiedad sobre los derechos de uso de un bien nacional de uso público, la propiedad sobre la zona de concesión otorgada a un concesionario eléctrico, la propiedad de los derechos que emanan de la calidad de estudiante, la que existe sobre el derecho a ejecutar una obra en virtud de la autorización administrativa otorgada y la propiedad sobre el derecho inmaterial de un recorrido de una línea de movilización colectiva.

Los ejemplos anteriores, que podrían alargarse fácilmente, no son sino una demostración de la amplitud con que la Constitución Política reconoce y protege el

derecho de propiedad, sin que sea necesario para reconocer la existencia de una propiedad garantizada constitucionalmente que tenga un estatuto legal propio, pues basta para ello que de la vida jurídica haya surgido una situación o una relación en que concurran las características propias del dominio.

En lo relativo a las bases de datos, conforme a las normas constitucionales vigentes resulta indiscutible que la persona que efectúa operaciones de tratamiento de datos y elabora un registro o banco de los mismos, tiene un derecho de propiedad sobre la base de datos que goza de reconocimiento y protección constitucional. El contenido de una base de datos puede, en efecto, representar un activo de gran valor patrimonial y de ahí la importancia de reconocer a su dueño el ejercicio exclusivo de las tradicionales facultades del dominio, esto es el uso, goce y disposición, quien podrá celebrar a su respecto los actos y contratos que permita la legislación vigente y no podrá ser privado de su propiedad sino a través del correspondiente proceso expropiatorio.

- ¿Cómo podríamos exigir un respeto a la vida privada y un resguardo a la privacidad en la N° 19.628?

Para abordar esta materia es preciso analizar en particular las disposiciones del Título Primero de la ley. Un aspecto central en la estructura de dichas normas es el concepto de "datos personales" o "datos de carácter personal". Según la letra f) del artículo 2° de la ley, datos personales son "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables" según ya lo habíamos definido anteriormente. Con ello, parece excluirse la protección de los datos que conciernen a personas jurídicas. Surge entonces la duda acerca de si el derecho de toda persona al tratamiento de datos del artículo 1° de la ley no contendrá una restricción inconstitucional al no permitir que se traten datos de personas jurídicas.

Los datos personales, definidos en el párrafo anterior, pueden en general ser clasificados en tres grupos, según su índole y procedencia, a saber:

a) Datos personales que provengan o se recolecten de fuentes accesibles al público

Según la definición de la letra i) del artículo 2°, fuentes accesibles al público son "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes". Tales datos, en los supuestos del artículo 4°, inciso quinto, de la ley, no requieren autorización de su titular para ser objeto de

tratamiento.

Dichos supuestos, conforme a la norma legal mencionada, ocurren cuando los datos son de carácter económico, financiero, bancario o comercial; cuando se contienen en listados relativos a una categoría de personas que se limitan a indicar antecedentes tales como la pertenencia del individuo a un grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, y también cuando son necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta de servicios.

De lo expuesto resulta, entonces, que los datos mencionados en el inciso quinto del artículo 4° de la ley, cuando se obtienen de fuentes accesibles al público, no requieren de la autorización de su titular para ser objeto de tratamiento.

Sin embargo, cuando hablamos de datos de carácter económico, debemos señalar que nos referimos al sentido estricto, y contrariamente a la denominación de "dato con significación económica", puesto que estamos concordes con diversos autores que señalan que podríamos dar una calificación económica, y por tanto, un valor económico, pecuaniario y cuantificable a los datos de las personas.

Asi tenemos, por ejemplo cada vez que se realiza una compra (sobre todo, si es 'on line'), los vendedores exigen una serie de datos personales al comprador, que pasan a formar parte de enormes bases de datos con referencias de miles de ciudadanos. ¿Cuál es el precio de esa ingente y valiosa información, que los vendedores consiguen de manera gratuita?

Existe en Internet actualmente un sitio web llamado "Swipe"[63] que proporciona un conjunto de herramientas que ayuda a descifrar, por ejemplo, los complicados códigos de barras de los permisos de conducir de varios estados de EEUU, una información codiciada por determinadas empresas que luego la venden a terceros (partidos políticos, empresas de servicios, etc.). Además, proporciona gratis una 'calculadora'[64] para averiguar cuánto cuesta cada dato que se proporciona a una empresa determinada (domicilio, nombre, código portal, estado civil, etc...).

Esta calculadora permite que se determine lo que valen sus bits de datos en el mercado abierto de EEUU (en este caso). Por ejemplo, una compañía típica de telefonía celular pedirá su dirección, la fecha de nacimiento, el número de teléfono, el número de Seguridad Social y la licencia de conductor de abrir una nueva cuenta. Consultando

[63] http://www.we-swipe.us/
[64] Para observar esta herramienta hay que visitar http://turbulence.org/Works/swipe/calculator.html

dicha calculadora de los datos arroja que tales datos cuestan $13.75 (es decir, más de $7.000).

A pesar que lo anterior suene un poco descabellado y es variable su apreciación, no es menos discutible que con el fenómeno de la globalización, las estadísticas, los estudios de mercados, etc, cada dato nuestro tiene una significación económica mas o menos importante.

b) Datos personales en general

Los datos personales en general, esto es, todos aquéllos no comprendidos en el inciso quinto del artículo 4° –referido a datos obtenidos de fuentes accesibles al público–, por una parte, y tampoco los que queden incluidos dentro de la categoría de datos sensibles de la letra g) del artículo 2°; por otra, pueden ser utilizados por las personas responsables de un registro o banco de datos en los casos y bajo las condiciones que contempla la Ley N° 19.628.

El artículo 4°, inciso primero, de la ley, prescribe en tal sentido que "el tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello". En otras palabras, existe un tratamiento de datos que es lícito realizar sin la voluntad del titular de los mismos, y otro que únicamente es lícito efectuar previa autorización de los titulares de los datos.

Casos en que la ley permite efectuar tratamiento de datos sin que sea necesario contar con la autorización de sus titulares son los contemplados en el inciso sexto del artículo 4° y en los artículos 17 a 19 de 12 ley.

La primera de las disposiciones citadas excluye de la necesidad de autorización "el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros beneficios de carácter general de aquéllos".

El segundo grupo de disposiciones se refiere, por su parte, a las informaciones que versen sobre obligaciones de carácter económico, financiero, bancario o comercial contenidas en los documentos protestados a que se refiere el artículo 17, o las informaciones que den cuenta del incumplimiento de las obligaciones de dinero a que se refiere esa misma disposición.

A su vez y conforme a lo dispuesto en el artículo 4° de la ley, el tratamiento de datos personales con autorización de su titular exige que ella reúna las siguientes

características:

i) consentimiento expreso del titular de los datos;

ii) consentimiento manifestado por escrito;

iii) consentimiento informado respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público;

iv) autorización vigente o no revocada por escrito. Además, otras disposiciones contenidas en el título I de la ley "De la utilización de datos personales" imponen diversas obligaciones a las personas u organismos responsables de registros o bancos de datos, entre las que conviene destacar las contenidas en el artículo 7°, que impone el deber de guardar secreto sobre los datos personales recolectados de fuentes no accesibles al público a las personas que trabajan en el tratamiento de los mismos, y en el artículo 9° que establece la obligación de utilizar los datos personales sólo para aquellos fines para los que fueron recolectados cuando no provienen de fuentes accesibles al público.

c) Datos personales sensibles

Los datos sensibles, por último, definidos en la letra g) del artículo 2°, en principio no pueden ser objeto de tratamiento según lo dispuesto en el artículo 10 de la ley, aunque esta disposición contempla luego algunas excepciones que en cierta manera aproximan los datos sensibles a los datos personales privados en general.

Datos sensibles, según la norma legal que los define, son "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual". Como puede apreciarse de la definición citada, estos datos constituyen un conjunto restringido dentro de la totalidad de los datos personales, ya que, aunque participan de lo que distingue a estos últimos que es la referencia a cualquier información concerniente a una persona natural, identificada o identificable, son relativos a determinadas informaciones más íntimas o privadas de las mismas.

No es extraño, por consiguiente, que la Ley N° 19.628 haya tenido el propósito de ser más restrictiva en el tratamiento de datos personales. Al respecto, el artículo 10 de la misma dispone que "no pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para

la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares".

A modo de conclusión, de las normas examinadas precedentemente es posible colegir tres principios claves en la ley:

1° Tratándose de datos personales que provengan o se recolecten de fuentes accesibles al público (artículo 4° inciso quinto), la ley establece amplios supuestos en los cuales el tratamiento no requiere autorización de su titular.

En efecto, en estos casos no se requiere autorización del titular cuando se esté en presencia de alguno de los tres tipos de datos a que se refiere el inciso quinto del artículo 4° de la Ley N° 19.628, y que son:

i) los de carácter económico, financiero, bancario o comarcial (con la excepción propuesta);

ii) los que se contengan en listados relativos a una categoría de personas y que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, y

iii) los necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios, esto es los datos para el marketing directo.

En los demás casos, los datos recolectados de fuentes accesibles al público requerirán autorización para su tratamiento, tal como se dispone para los datos, llamémosle privados, según se comenta a continuación.

2° En el caso de los datos personales que no provienen o son recolectados de fuentes accesibles al público –datos privados–, el tratamiento puede efectuarse sólo con consentimiento de su titular, por regla general.

Excepcionalmente, el artículo 4° inciso primero, explicado más arriba, excluye de la necesidad de contar con la autorización de su titular el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que estén afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos.

También por vía de excepción y según ya se ha comentado, el tratamiento de estos datos puede efectuarse sin mediar autorización del titular cuando la ley en comento u otras lo autoricen; como ocurre en los casos de comunicación de datos personales relativos a

obligaciones de carácter económico, financiero, bancario o comercial, reguladas en el título III de la ley.

3° Finalmente, tratándose de los datos sensibles, definidos más arriba, éstos en principio no pueden ser objeto de tratamiento (artículo 10°), pero luego la misma disposición contempla diversas excepciones que los aproximan a los datos personales privados. Por consiguiente, la autorización del titular para su tratamiento debiera sujetarse a los términos del artículo 4, comentados con anterioridad. Lo anterior, sin perjuicio de los casos en que conforme al propio artículo 10 u otras disposiciones legales estos datos sensibles puedan ser objeto de tratamiento

7) Críticas y defectos de la ley 19.628. Vacíos Legales.

Las intenciones de la ley, al iniciarse su tramitación en el Congreso, eran buenas. Estaban destinadas a poner fin a la arbitrariedad que significaba que cualquier comerciante o institución crediticia podía poner como deudor moroso en empresas que registraran deudas (como es el caso de DICOM), a cualquier persona sin ningún documento de respaldo. Y podía usar su calidad de moroso por tiempo indefinido para bloquear acceso al crédito y señalarlo como persona de pocos antecedentes. Esto operaba casi automáticamente mediante convenios entre las casas e instituciones comerciales, con las empresas de datos. La información se enviaba desde una pantalla de computador, a la pantalla de DICOM sin más trámite ni control.

La exigencia de que solo documentos protestados pudieran incluirse en las bases de datos, pareció suficiente para controlar la arbitrariedad. Pero mediante una redacción engañosa y cediendo a las presiones de parlamentarios vinculados a las casas comerciales, se incluyó a otro tipo de obligaciones que no requieren de protesto y se autorizó a las llamadas "sociedades administradoras de créditos otorgados para compras en casas comerciales" a enviar a las bases de datos como morosos a su simple arbitrio y sin documentos de respaldo.

La presencia en el Boletín de Informaciones Comerciales y en DICOM, se está usando ahora, no sólo para negar nuevos créditos , sino como un instrumento de

opresión en que al deudor se le impide incluso buscar trabajo.

Además, en la ley no se estableció que las modificaciones a las bases de datos debían hacerse gratuitamente cuando contenían datos erróneos. Evidentemente si una persona figura como deudor moroso y paga esa deuda, la información está errónea. Pero para hacer la aclaración de la deuda, la ley en una incalificable protección al Boletín de Informaciones Comerciales que pertenece a la Cámara de Comercio de Santiago, en una evidente contradicción con otro artículo de la ley, respetó el derecho del Boletín de continuar cobrando por las aclaraciones.

El cobro de las aclaraciones le representa un ingreso al Boletín de más de tres mil millones de pesos al año. Suma que debe ser pagada por los deudores que, además de pagar sus deudas, deben pagarle al Boletín.

Finalmente, la ley estableció un plazo de tres años, para sacar de la base de datos al deudor que pagó su deuda. Sin embargo, la ley no consideró que en 1999 Chile ya vivía una seria crisis económica y que varios cientos de miles de personas estaban sin empleo y buscando trabajo. Al estar en DICOM no son aceptadas para muchos puestos de trabajo. Al no encontrar trabajo, no pueden pagar sus deudas.

Por otro lado, como lo habíamos indicado, la Ley sobre Protección de Datos regula el tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares, exceptuado del que se efectúa en el ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que alude la Constitución en el artículo 19 Nº 12.[65] No cabe duda que este cuerpo legal regula el ejercicio de una de las garantías constitucionales más importantes de la actual sociedad informatizada, como lo es la referida al respeto y protección de la vida privada de las personas y de su familia estatuida en el artículo 19 Nº 4 de nuestra Constitución.[66]

Queda en suspenso, pues, la posibilidad –más conveniente a nuestro parecer- de que a través de una reforma constitucional se hubiere plasmado, como lo está en otros

[65] Artículo 1º inciso 1º de la Ley Nº 19.628.

66 El profesor HUMBERTO NOGUEIRA A. sostiene que el proyecto de ley respectivo al tratamiento de datos personales (su ponencia al respecto data de 1997 cuando aún se encontraba en trámite parlamentario el proyecto de ley respectivo) busca asegurar un derecho fundamental no contemplado explícitamente en el texto de nuestra Constitución, el que sólo puede deducirse de otros derechos asegurados y de los derechos reconocidos por los tratados internacionales ratificados por el Estado de Chile y vigentes (artículo 5º inciso 2º, oración final). Ver al respecto la ponencia del profesor Nogueira al Seminario sobre "Derecho a la autodeterminación informativa y acción de Habeas Data en Iberoamérica", dictado en la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, intitulada "Reflexiones sobre el establecimiento constitucional del Habeas Data y del Proyecto en tramitación parlamentaria sobre la materia", publicado en la Revista Ius et Praxis de la mencionada Facultad, ob. cit., pág. 265.

ordenamientos fundamentales (los que veremos a continuación), el derecho a la autodeterminación o libertad informática y al mismo tiempo se hubiese introducido con rango constitucional el instrumento tutelar de tal prerrogativa, denominado Hábeas Data, el cual ya habíamos revisado con anterioridad.

Se ha planteado un debate en relación a la referida normativa legal centrado a su presunta inconstitucionalidad, sosteniéndose que ella se ha propuesto aclarar o determinar el sentido y alcance de los derechos constitucionales a la vida privada y a la intimidad, por un lado, y el derecho o libertad para informar, por el otro, de tal manera que, tratándose de una norma interpretativa de dichos preceptos constitucionales, hubiera requerido para su aprobación del quórum especial que la Carta Fundamental estatuye para tal categoría de leyes y, al no haberse dado cumplimiento a dicha exigencia, por haberse aprobado con la concurrencia de las mayorías previstas para una ley simple, sería inconstitucional.[67]-[68]

En contrario a lo anteriormente planteado, se sostiene que la regulación legal sólo ha venido a llenar un vacío de nuestro ordenamiento jurídico en una materia de tal relevancia en el mundo moderno como lo son las bases de datos, partiendo de la tesis que el derecho a la vida privada consagrado en nuestra Constitución comprende lo que la doctrina denomina el "derecho a la autodeterminación informativa".[69] Esto es, como ya ha sido expresado, este derecho constitucional en su doble enfoque; no sólo es comprensivo actualmente de la fase negativa que sustrae de todo tipo de intromisiones perturbadoras de la intimidad aquellos espacios no deseados por el titular que sean conocidos, sino que obligadamente debemos entenderlo en su dimensión activa y dinámica consistente en la prerrogativa de conocer, acceder y, por supuesto, controlar el flujo de informaciones concernientes a la persona. Esta se ha constituido en la faceta más importante de la privacidad en el mundo actual y permite al individuo controlar el

[67] El profesor de Derecho Constitucional de la Universidad Finis Terrae, JOSÉ IGNACIO VÁSQUEZ M., sostiene esta postura en un artículo denominado "*Análisis crítico sobre la naturaleza jurídica de la Ley de Protección de la Vida Privada*", publicado en la *Revista de Derecho* de la Universidad Finis Terrae, Año III, Número 3, 1999, págs. 43 y siguientes.

[68] Sostiene el profesor VÁSQUEZ en su estudio ya mencionado que, al ser aprobada la ley sin los quórums requeridos, se ha vulnerado el principio de supremacía constitucional en su aspecto formal, consagrado en el art. 6º de la Carta Fundamental, pero al mismo tiempo a través de la interpretación denominada actualizadora de los preceptos constitucionales, ampliando el supuesto alcance de las normas originales, se las ha desvirtuado, no guardando las normas dictadas ninguna relación ni proporción con el carácter y amplitud que el propio constituyente les dio originalmente y, con ello, también se vulneraría la supremacía constitucional en su dimensión material.

[69] Según la tesis sostenida por el profesor de Derecho Administrativo de la Universidad de Chile, CARLOS CARMONA SANTANDER, en "*Protección de datos personales. Ley Nº 19.628*", en Informativo Jurídico de Derecho en Línea (dirección internet).

manejo y circulación de la información que sobre su persona ha sido confiada a un tercero.[70] Para que este aspecto de la vida privada, en su dimensión dinámica que permite un control sobre la información que se dispone de la persona, haciendo uso ésta del derecho a la autodeterminación informativa, el titular del mismo debe contar con los instrumentos necesarios para restablecer su ejercicio en caso de vulneración. Para ello la ley debe dotarlo de recursos o acciones necesarios para hacer realidad el derecho ante el ataque de terceros, especialmente en los casos en que su titular no consiente en la utilización o tratamiento de sus datos personales más sensibles. En cuanto al denominado "*derecho a la autodeterminación informativa*", el profesor HUMBERTO NOGUEIRA A. sostiene que éste tiene un carácter implícito, deriva de libertades negativas constituidas por la protección del derecho a la vida privada, a la intimidad, a la propia imagen, a la honra de la persona y de su familia, que emanan de la dignidad de la personalidad, como asimismo de los valores y principios de igualdad, verdad y libertad. Su contenido comprende la facultad de la persona de disponer de la información personal privada, íntima o sensible, que debe ser protegida por el orden social y regulada por el ordenamiento jurídico, evitando las distorsiones del proceso comunicativo informático en especial. Igualmente este derecho a la autodeterminación informativa puede ser concebido –en opinión del profesor Nogueira– como la facultad de la persona concernida por los datos almacenados en un archivo base de datos público o privado, para autorizar su recolección, conservación, uso y circulación, como asimismo para conocerla, actualizarla, rectificarla o cancelarla. Es decir, es una prerrogativa del ser humano, fundada en su dignidad y libertad, para determinar por sí mismo cuándo y dentro de qué límites procede develar situaciones relativas a su propia vida. Se busca, mediante este derecho, resguardar a las personas frente al inmenso poder invisible cada más fuerte que opera en la penumbra, constituido por los ficheros, registros y bases de datos informatizados o no, que operan como poderes fácticos dentro de la sociedad, desarrollados por el poder público o por particulares, transformándose en fuentes de poder social, de invasión de la intimidad y de control político.[71] En consecuencia, el derecho a la autodeterminación informativa requiere de la regulación legal para fijar los marcos del adecuado uso y control de las bases de datos personales y, en ese sentido, la Ley Nº 19.628 constituye un avance en la materia, pero no es la ley

[70] CARLOS CARMONA S. Ob. cit.
[71] HUMBERTO NOGUEIRA, "*Reflexiones sobre el establecimiento constitucional del Habeas Data...",* en Revista *Ius et Praxis*, ob. cit., págs. 265 y 266

que se requiere en estos días, existiendo por tanto una verdadera laguna legal en esta materia.

Sin perjuicio de compartir la tesis del profesor Carmona, queremos destacar que, atendidas las precisiones conceptuales acerca del derecho consagrado en nuestra Carta Fundamental en el artículo 19 Nº 4, que tiene un contenido doctrinario difícil de delimitar con precisión, debido, entre otras razones, al extraordinario auge que en la época moderna han experimentado las comunicaciones con todo su bagaje de "adelantos" tecnológicos, es evidente que, interpretando adecuadamente la Carta Magna, hay que tener presente que ésta ha constituido como de reserva legal exclusiva la regulación del ejercicio de los derechos fundamentales. Lo que sí es imperioso que el legislador tenga en consideración al desplegar su actividad normativa en punto a este objetivo es que al hacerlo, regulando o complementando las garantías constitucionales o limitándolas en los casos que así lo autoriza la Ley Fundamental, no podrá en ningún caso afectar los derechos en su esencia, ni imponerse condiciones, tributos o requisitos que impidan su libre ejercicio.Es por ello que nuestro Código Político en vigor se halla claramente comprometido con valores matrices del Constitucionalismo como lo es, sin duda, este derecho a que sea siempre reconocida y respetada por la ley, tanto la esencia o núcleo característico de cada derecho asegurado cuanto el libre ejercicio del mismo.

Es decir, la constitucionalidad de los preceptos de la ley sobre protección de datos de carácter personal debe examinarse a la luz de aquellas de sus disposiciones que posibiliten la invasión o entrada a ciertos recintos que pudieran estimarse por su titular que integran su vida privada, pero que en atención a los requerimientos sociales pueden ser conocidos y divulgados asegurando en todo momento un control democrático de la información.

Sin embargo, propugnamos la tesis de que, aun cuando la ley dictada pueda considerarse como un avance en la necesaria regulación de la materia para proteger adecuadamente derechos tan sensibles y con un alto riesgo de vulneración en la actualidad, como lo son la vida privada e intimidad del hogar y de las comunicaciones personales, se hace imprescindible la constitucionalización del derecho a la autodeterminación informativa y de la acción tutelar de *habeas data*. Sin embargo, para evitar que sea afectada en su esencia tal acción tutelar, no basta con que la Ley Fundamental la reconozca y asegure ampliamente a través de un procedimiento sencillo, rápido y eficaz, exento de formalismos, sino que es necesario que la Carta expresamente entregue la regulación de su tramitación a la ley y que ésta, al igual que la destinada a

reglamentar el ejercicio del derecho, sea de quórum calificado.

Como expresa el profesor Nogueira, la constitucionalización de este instituto jurídico se basa en la necesidad de delimitar el núcleo esencial del derecho protegido, garantizándolo ante cualquier desnaturalización o limitación que los órganos instituidos puedan realizar de él bajo pretexto de regularlo, ya que este contenido esencial del derecho queda fijado por la propia Constitución y garantizado por la normativa del artículo 19 Nº 26, sin perjuicio que el legislador complemente y regule su ejercicio. Con ello, incluyendo además en la Carta Fundamental el reconocimiento a la acción de *habeas data*, se limita igualmente la actuación de otros poderes constituidos: Congreso, a través de actividad legislativa; Gobierno, a través de la potestad reglamentaria, y Tribunales ordinarios o de jurisdicción constitucional, a través de sus resoluciones.[72]

8) Jurisprudencia Chilena

En 1995 se produjo el robo de la base de datos de los clientes de una conocida multitienda nacional. Más de 1 millón de personas figuraba en aquel listado, que fue vendido en 3 millones y medio de pesos a una empresa que posteriormente lo ofreció a los competidores de la firma afectada.

En ese entonces, se habló sobre las pérdidas monetarias que ello implicaba para la entidad en cuestión, pero poco se dijo en relación al daño al que habrían estado expuestos quienes figuraban en ese registro. Una situación que en nuestro país no parece ser mayormente cuestionada, pues es común que empresas e instituciones que manejan bases de datos computacionales comercialicen esa información.

En Chile, la Cámara de Comercio de Santiago era el único organismo que en este momento está bajo tutela, a través de un decreto supremo sobre el manejo de información de conductas comerciales irregulares. No existía una ley específica que regule la privacidad de los datos personales recopilados en estos sistemas. Y aunque la Constitución Política en su artículo 19 número 4, resguardaba el derecho a la intimidad y privacidad, en la práctica resultaba casi imposible probar el uso indebido de este tipo

[72] HUMBERTO NOGUEIRA ALCALÁ. "*Reflexiones sobre el establecimiento constitucional del Habeas Data...",* en Revista Ius et Praxis, ob. cit., pág. 275.

de información.

Es por eso que el método de defensa jurídica más recurrida por personas que se sentían lesionadas en su derecho a la privacidad en lo relativo al uso de Tecnologías de la Información (específicamente con el tratamiento de sus datos), era a través del recurso de protección.

De modo fragmentario citaremos jurisprudencia de nuestros Tribunales Superiores de Justicia sobre protección del derecho a la intimidad y del derecho al honor (art. 19 N° 4 C.P.R.) frente al poder informático, en concreto a bancos de datos:

- Sentencia Corte de Apelaciones de Santiago (S.C.A.S.) de 21 de octubre de 1981:

"4° Que la negativa del director del Boletín a recibir la aclaración que el interesado quiere publicar lesiona sus derechos como quiera que su crédito y honorabilidad se siente en el consenso publico";

"5° Que, además, es de notar que la dirección del Boletín ha debido tomar precauciones para evitar el daño que pueda producirse a personas que no han incurrido en deudas morosas, asentando, junto con el nombre de la persona, otros datos que permitan identificarla..., y"

"6° Que, en consecuencia, la petición formulada debe acogerse, pues la resolución de que se trata lesiona un derecho que la Constitución Política del Estado garantiza en el articulo 19 N° 4 y 21°"[73]

- Sentencia Corte de Apelaciones de Concepción de 7 de marzo de 1988:

"6° Que, además, es incuestionable que este acto arbitrario de la recurrida vulnera la garantía constitucional consagrada en el articulo 19 N° 4 de la Constitución, puesto que al hacer aparecer al recurrente como una persona que no cumple sus obligaciones comerciales afecta la honra de este, e incluso, como consecuencia de ello, el normal

[73] Revista de Derecho y Jurisprudencia y Gaceta de los Tribunal Tomo LXXVIII, N° 3, Secc. 58, pp. 296-300.

desenvolvimiento de sus actividades económicas".[74]

- Sentencia Corte de Apelaciones de Punta Arenas de 1 de junio de 1988:

"7° Que, la dinámica de esta actuación antijurídica y arbitraria, que se inició con la inserción equivocada de un dato de identificación comercial propio del recurrente en operaciones bancarias de un tercero y que se tradujo posteriormente en la publicación de protestos de documentos bajo ese signo erróneo en un medio de información especializado de circulación nacional, como lo del Boletín de Informaciones Comerciales, que difunde el nombre de las personas que incurren en incumplimiento de ciertas obligaciones pecuniarias, no pudo menos que producir serio menoscabo en la honra del afectado, un deterioro de la reputación y la buena fama que todo individuo se granjea en el seno de la sociedad por la suma de sus valores morales, entre los que se cuenta, en el ámbito de las relaciones comerciales, el cumplimiento estricto y oportuno de las obligaciones contraídas";

"9° Que, tanto el derecho a la honra de una persona como el ejercicio de cualquier actividad económica que no sea contraria a la moral, el orden publico o la seguridad nacional se encuentran elevados o rango de garantías fundamentales que la Constitución Política del Estado reconoce con tal carácter en su articulo 19 N°s. 4 y 21, y cuyo ejercicio cautela mediante el arbitrio especial de protección consagrado en su artículo 20" [75].

- Sentencia Corte Suprema de 19 de abril de 1989.

"2° Que, como se desprende de la disposición transcrita (art. 4° del Decreto N° 950, del Ministerio de Hacienda, de 1928) las personas afectadas por la publicación de datos que efectuó el Boletín tienen derecho para exigir de este se inserten las aclaraciones que dichas personas pueden dar respecto de los datos que les afecten, y esto es lo que la actual recurrente y apelante ha solicitado de la demandada, o sea, que las letras cuyos protestos han sido publicados, no fueron aceptadas por sus representante legales, no

[74] Revista de Derecho y Jurisprudencia y Gaceta de los Tribunal , Tomo LXXXV, N° 1, *Secc.* 58, pp. 65-67.
[75] Revista de Derecho y Jurisprudencia y Gaceta de los Tribunal , Tomo LXXXV, N° 2, pp. 217-223.

siendo suyas las firmas, lo que consta de informes periciales producidos en la causa criminal incoada por querella suya, según consta del certificado del secretario del Tribunal". [76]

- Sentencia Corte de Apelaciones de Rancagua, de 26 de mayo de 1994;

"7° Que, la inclusión de antecedentes financieros desfavorables en las situaciones mencionadas no afectan la vida privada, publica y la honra de la entidad en cuyo favor se recurre, y además, por ser ella una persona jurídica carece de familia, en los términos del articulo 19 Nº 4 de la Constitución Política de la Republica, no obstante que la existencia de antecedentes desfavorables a la persona en cuyo favor se recurre en los mencionados Informes o Boletines Comerciales, implica una perturbación al derecho que todo individuo tiene de desarrollar cualquiera actividad económica que no sea contraria a la moral, al orden publico o a la seguridad nacional, que garantiza el Nº 21 del articulo 19 antes citado, toda vez que quien registre esos antecedentes, así lo sea por razones históricas, tendrá menos oportunidad de acceder a una actividad comercial o económica que aquel que no les tiene y jamás ha dejado de pagar una deuda o de cumplir una obligación";

Nota: Sentencia revocatoria de la Excma. Corte Suprema de 23 de junio de 1994 en sede de apelación:

"1° Que, la circunstancia que la recurrida mantenga, en forma Integra y según su historia cronológica, información recogida de una publicación oficial, reconocida por la ley, y la proporcione a sus usuarios, no constituye un acto ilegal o arbitrario, por lo que este recurso carece del presupuesto indispensable para prosperar.

"2° Que, además los hechos que el recurrente estima ilegales o arbitrarios, que motiven su accionar, no han podido privarlo, perturbarlo o amenazarlo en el legitimo ejercicio de la garantía establecida en el Nº 4 del articulo 19 de la Constitución Política, desde que se trata de una persona jurídica";

[76] Revista de Derecho y Jurisprudencia y Gaceta de los Tribunal , Tomo LXXXVI, N° 1, pp. 15-17

"3° Que, a mayor abundamiento, debe considerarse que la normativa del decreto supremo Nº 950, de 1928, del Ministerio de Hacienda, al establecer que pierden vigencia, en determinados casos, ciertas publicaciones aparecidas en el Boletín de Informaciones Comerciales, no ha podido significar la desaparición física de tales publicaciones ni impedir el registro de ellas en los sistemas o mecanismos de procesamiento de información - como es el caso de los servicios proporcionados por la recurrida -, sino que, como se lee en la Circular de la Superintendencia de Bancos que en fotocopia rola a fojas 1, "equivale a que si una institución financiera tiene que resolver, por ejemplo, si va a otorgar un crédito o abrir una cuenta corriente a una persona que registra un protesto aclarado o uno que lleve mas de cinco anos publicado, debe pura y simplemente abstraerse de la existencia de esos protestos y proceder como si no hubieren existido jamás".[77]

También la tutela del "secreto" bancario y tributario por via del articulo 19 N° 5 de la Constitución, es decir, la inviolabilidad del hogar y de toda forma de comunicación privada ha tenido una débil recepción en nuestra jurisprudencia. De modo fragmentario citaremos los fundamentos jurídicos más significativos recogidos en folios sobre la materia:

- Sentencia Corte Suprema de 12 de septiembre de 1988.

"4° b) Que, como puede apreciarse, solo algunos aspectos de la cuenta corriente bancaria están sujetos a "estricta reserva, respecto de terceros", cuales son, como se dijo, "el movimiento de la cuenta corriente y sus saldos", como señala el inciso segundo, y ni aun estos en forma absoluta, como quiera que, como ya se dijo, los tribunales podrán aun "ordenar la exhibición de determinadas partidas" de la cuenta corriente en causas civiles y criminales seguidas con el liberador, como lo prescribe el inciso tercero ya antes referido, y

"5° Que lo dicho precedentemente respecto de la reserva de la cuenta corriente en los limitados términos previstos en el articulo 1° de la Ley de Cheques es igualmente aplicable a la reserva o secreto de que trata el articulo 20 de la Ley General de Bancos,

[77] Revista Gaceta *Juridica* , N° 168, 1994, pp. 54-57. Tambien sentencia de Corte Suprema de 3 de diciembre de 1996 Gaceta Juridica N°198, 1996, pp. 52-54.

pues en el caso de autos no se han solicitado por el Superintendente de Bancos antecedentes relativos a las "operaciones" que los recurrentes han realizado o realicen respecto de los "depósitos" que tuvieron en los bancos, sino exclusivamente acerca de la solo existencia de los mismos, lo que reafirma también el texto mismo de dicho articulo 20, de cuyo tenor se desprende que lo que se procura con tal institución es el evitar se ocasione "daft patrimonial al cliente".[78]

- Sentencia Corte Suprema de 19 de enero de 1989.

"5° Que, la estricta reserva impuesta a los bancos en los términos recordados en el fundamento segundo, hace que lógicamente los instrumentos en que constan la existencia del contrato de cuenta corriente, los depósitos, giros y demás operaciones que le son propias, deben asimilarse a los "documentos privados" comprendidos en la garantía de inviolabilidad contemplada en el N° 7 del articulo 19 de la Constitución Política y cuyo "registro" solo se permite en los casos y formas determinados por la ley"

"6° Que, ahora bien, como la orden de informar expedida en la resolución calificada de ilegal implica propiamente el "registro" o examen de los respectivos instrumentos, resulta evidente que aquella garantía constitucional ha sido vulnerada; y con ello corresponde acoger el recurso en examen, respecto del cual este tribunal ya declare su admisibilidad por resolución de doce de mayo del año ultimo"[79]

9) Comentario jurisprudencial. Privacidad y tratamiento de datos personales en el portal del Poder Judicial.

Con fecha 08 de Marzo de 2001, una mujer interpuso con la asesoría de la Red Nacional Género, Comercio y Derechos Humanos (RENAGECO), ante la Ilustrísima

[78]Revista de Derecho y Jurisprudencia y Gaceta de los Tribunal, Tomo LXXXV, N° 3, de 1988, pp. 223-237

[79] Revista de Derecho y Jurisprudencia y Gaceta de los Tribunal, Tomo LXXXVI, N° 1, de 1989, pp. 1-4

Corte de Apelaciones de Santiago un recurso de protección de garantías constitucionales en contra de la Corporación Administrativa del Poder Judicial.

En el recurso la recurrente señala, a grandes rasgos, que se enteró por intermedio de una amiga, quien ingresó a través de Internet al recién inaugurado sitio Web del Poder Judicial de Chile, que en dicha página al introducir su nombre en el sistema de búsquedas, (estado de causas de Santiago), aparecen los datos de una demanda que interpuso por la reclamación de paternidad de su hija. Indica que con el objeto de indagar más antecedentes acerca de tal circunstancia, ingresó a la referida página web -(www.poderjudicial.cl)- y en ella constató que al pulsar en el vínculo "Cuaderno Principal" fuera de figurar los nombres de los abogados patrocinantes aparecían individualizadas las partes con nombre completo y número de cédula nacional de identidad, tanto los de ella como los del demandado. Luego señala que al ver el cuadro "Materia" decía "HIJO LEGITIMO, ACCIÓN", habiendo interpuesto la demanda en cuestión, bajo la vigencia de la ley 19.585 (*que estableció la igualdad filiativa en nuestro ordenamiento*), por ende se trataba de una acción de reclamación de paternidad en filiación no matrimonial, y no una acción de legitimación.

Sostiene que la citada información vulnera lo dispuesto en el artículo 197 del Código Civil que establece el carácter secreto de los procesos en los que se ha deducido una acción de filiación, y resulta además contraria a las normas contenidas en la ley N° 19.628, sobre Protección a la Vida Privada, al divulgar datos relativos a hechos o circunstancias de su vida privada.

Estos hechos para la recurrente implican un acto ilegal y arbitrario que conculca una serie de garantías constitucionales que indica, cuales son las contenidas en el artículo 19 número 1 “El derecho a la integridad psíquica de la persona”, número 4 “El respeto y protección a la vida privada y pública y a la honra de la persona y su familia”; la garantía contenida en el numeral 2 de dicho artículo, esto es, la igualdad ante la ley, para finalmente invocar la violación del numeral 24 que asegura a todas las personas el derecho de propiedad en sus diversas especies sobre toda clases de bienes corporales e incorporales.

Concluye en esta parte, señalando que recurre de protección en contra de la Corporación Administrativa del Poder Judicial, por publicar datos sensibles y expresiones discriminatorias en el banco o base de datos que mantiene en la Internet, lo que considera una actuación ilegal y arbitraria que causa privación, perturbación y amenaza en el legítimo ejercicio de su derecho a la privacidad y honra y de su familia y

un acto de discriminación contra su hija, lo cual, a su vez, daña profundamente su dignidad humana, amenazando y perturbando su integridad psíquica, moral y emocional.

En su petitorio, solicita a la Corte de Apelaciones de Santiago que a fin de restablecer el imperio del Derecho, se ordene a la recurrida eliminar los datos sensibles y expresiones discriminatorias referidos que mantiene en el banco o base de datos del sitio en Internet ya indicado.

Informando el recurrido, a través del entonces Presidente de la Exma Corte Suprema y Presidente de Consejo Superior de la Corporación Administrativa del Poder Judicial, Hernán Alvarez García se solicita el rechazo de la acción constitucional interpuesta, con costas, por los razonamientos que siguen:

- El sitio se encuentra en desarrollo.
- En la actualidad las causas ingresadas en materia de filiación. se identifican, haciendo mención a la ley respectiva: "Acción Ley 19.585".
- Las búsquedas que efectúa el usuario sólo le permiten que se le proporcione información y a guiar a las partes que están en juicio, pero en ningún caso están orientadas a dar a conocer información sustantiva acerca del contenido del proceso que se encuentra en tramitación.
- Respecto de la terminología utilizada para denominar la materia objeto del juicio "Hijo Legitimo, Acción", dice que ella estuvo en conocimiento de todas las partes del proceso desde el momento en que ingresare la causa a la Corte de Apelaciones para su distribución sin que la recurrente, al parecer solicitara al Juzgado respectivo que se caratulara correctamente el expediente, ni que se mantuviera en secreto, sabiendo que los jueces en materia civil se rigen por el principio de pasividad.
- Hace presente además que el artículo 9 del Código Orgánico de Tribunales señala que los actos de los tribunales son públicos, salvo las excepciones expresamente establecidas por la ley, consagrando así una de las bases fundamentales de la Administración de Justicia, esto es, su publicidad. Una de esas excepciones, es la que contemple el artículo 197 del Código Civil en materia de acción de filiación, al establecer que el proceso tendrá carácter de secreto, hasta que se dicte sentencia de término, y que sólo tendrán acceso a él las Partes y sus apoderados judiciales. Por consiguiente, señala, que al igual que el sumario criminal, ello significa que el detalle de estos procesos, es decir, el

contenido de sus actuaciones, resoluciones o diligencias, no podrá ser de público conocimiento, teniendo el carácter de secreto. Sin embargo, añade, jamás podrá tener ese carácter, la existencia de la causa respectiva. Prueba de ello, son los libros de ingresos de causas de los tribunales de Justicia, los cuales pueden ser consultados por cualquier individuo y tomar conocimiento de la existencia de esta clase de juicios, pudiendo conocer el nombre de las partes, la materia y el rol de la causa.

- Por último señala que la Corporación que preside, no ha procedido indebidamente en el tratamiento de los datos, ya que se ha limitado a mostrar aquella información que las mismas partes entregan al Tribunal, con el fin de otorgarles un mejor servicio.
- Sin perjuicio, de lo expuesto, manifiesta que la Corporación está realizando un estudio acucioso, dentro del período de marcha blanca, de todas aquellas materias que revisten algún grado de sensibilidad, con la finalidad de precaver situaciones como las que se reclaman a través del presente recurso. Consecuencia de ello, es la sustitución de la glosa, "hijo legítimo, acción" por la de "acción Ley 19.585".

La primera sala de esta Corte, integrada por los ministros Gabriela Pérez Paredes, Juan Araya Elizalde y el abogado integrante Eduardo Jara Miranda, en fallo redactado por el ministro Araya, rechazó el recurso interpuesto por unanimidad. Luego, la recurrente apeló tal sentencia ante la Corte Suprema de Justicia, solicitando alegatos. A la solicitud de alegatos la Corte Suprema negó lugar, y con respecto a la apelación, la sentencia de primera instancia fue confirmada, sin ningún tipo de modificación u observación, por los ministros Orlando Alvarez G., Jorge Medina, Domingo Kokish M. y los abogados integrantes René Abeliuk M. y Franklin Geldres A.

Los considerandos de la sentencia que se comenta giran en torno a tres líneas argumentativas -que hacen suyo, en gran medida lo informado por la recurrida. La primera de ellas, es establecer que no se ha infringido la ley sobre protección a la vida privada, pues al entender de los ministros: “...tampoco se advierte que mediante ese sitio de Internet, se hayan proporcionado o se estén proporcionando datos sensibles relativos a la vida privada de la recurrente, ya que no se ha divulgado ningún hecho o circunstancia cuya privacidad resguarda la Ley 19.628”. La segunda línea, se refiere al principio de publicidad de las actuaciones judiciales al fallar que los datos que se

publican en el sitio web en cuestión, son los mismos que cualquier persona puede obtener de los libros de ingreso de causas de los Juzgados correspondientes, de los estados diarios que se exhiben en los Tribunales y los que se consignan en las tablas para anunciar las causas en las Cortes de Apelaciones; datos todos que son de público conocimiento. Luego señala, que no se ha transgredido el carácter secreto que reviste un proceso de filiación de la naturaleza del iniciado por la actora ya que ni su contenido, ni sus resoluciones se han dado a conocer a través de la página WEB del Poder Judicial.

Para terminar, razona que en el presente caso se ha armonizado por una parte lo que dispone el artículo 9 del Código Orgánico de Tribunales, que consagra que los actos de los Tribunales son públicos, con la reserva que debe resguardarse acerca del contenido de un proceso de filiación como lo preceptúa el artículo 197 del Código Civil. Finalmente, se indica como tercer razocinio que una demanda de la naturaleza de la iniciada por la recurrente, sólo puede identificarse actualmente por la cita de la ley que sirve de sustento, esto es, "Acción Ley 19.585", sin que se pueda acceder a ningún dato acerca del contenido del proceso respectivo, o da las resoluciones que en él han recaído.

En base a estas argumentaciones, la Corte indica que no se está en presencia de un acto u omisión ilegal, por lo que es innecesario analizar el quebrantamiento de las garantías constitucionales que se invocan por de la recurrente.

Ya establecidos los fundamentos de la recurrente y del recurrido y el contenido de la sentencia que falla el asunto discutido, pasaremos a continuación a analizar la real problemática planteada aquí, para luego proceder a criticar la sentencia, dando a su vez, luces acerca de las posibles soluciones que se debieron dar al problema de ilegalidad esbozada.

El marco normativo en el caso que nos ocupa, dice relación con dos asuntos, a saber: la protección de la vida privada, la protección de datos (ley 19.628) porque claramente nos encontramos frente una cuestión que se relaciona con el derecho a la intimidad y a la vida privada, y más específicamente a los datos sensibles, y la otra, la dicotomía principio de publicidad de los actos de los Tribunales (artículo 9 Código Orgánico de Tribunales) versus excepciones a él, esto es, secreto de las actuaciones judiciales. (en el caso en cuestión, artículo 197 Código Civil), porque es este principio de publicidad uno de los fundamentos basales del fallo para el rechazo de la acción de protección intentada. Estas normas han de interpretarse en armonía y dentro del marco de las derechos fundamentales del hombre contenidos tanto en nuestra Carta Fundamental, como en los tratados de derechos humanos que han sido suscritos por

Chile y que se encuentran vigentes (artículo 5 inciso 2° de la Constitución).

La Ley 19.628 de Agosto de 1999 sobre “Protección de la Vida Privada”, invocada como norma violada por la recurrente con el acto que se reclama, y aplicable al asunto que falla la sentencia, trata entre otros asuntos, instituciones y conceptos que debemos tomar en consideración, como los datos personales y su tratamiento, el concepto de fuentes accesibles al público y el tratamiento de datos por organismos públicos.

La ley establece a prima facie tres categorías de datos, los que requieren distintos niveles de protección, en primer término, los “datos de carácter personal o datos personales” que se encuentran definidos en el artículo 2 letra f) de la ley, como los relativos a cualquier información concerniente a personas naturales, identificadas o identificables, a estos datos se les aplica una protección ordinaria, se encuentran protegidos con las disposiciones generales de la ley. Luego están los denominados “datos públicos o de mera identificación”, que son aquellos que se recolectan de una “fuente accesible al público", concepto que es definido en el mismo artículo 2 letra i) como los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes, con respecto a estos datos la ley establece menos limitaciones al tratamiento. Finalmente, se encuentran aquellos datos que tienen una mayor y especial protección en la ley, son los denominados “datos sensibles”, entendiéndose por tales, según la letra g) del ya mencionado artículo 2, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

Entendemos que los datos pertenecientes a una causa judicial, denominados doctrinariamente “datos judiciales”, “datos jurisdiccionales”, o “datos personales contenidos en ficheros jurisdiccionales” constituyen datos sensibles según la definición legal que el ordenamiento jurídico nacional hace de ellos. Basamos esta afirmación, en la característica esencial del dato sensible, cual es que a partir de su tratamiento automatizado (lo que faculta el cruce de datos), pueden los tenedores de esa información tomar decisiones arbitrarias o discriminatorias respeto de los titulares de esos datos.

Es claro, entonces, el carácter sensible del dato judicial, algunos ejemplos aclararán esta asevero. Imaginemos a una empresa de corretaje de propiedades que para arrendar los inmuebles acude a las bases de datos del poder judicial para que con el solo

dato del nombre de una persona pueda ver si ésta se encuentra demandada en un juicio de arrendamiento, o el caso del empresario que para contratar a algún trabajador, acude a las bases de datos para determinar si por ejemplo ha demandado a empleadores anteriores, y en el caso que comentamos, la discriminación escolar que pudiera sufrir la hija de la recurrente frente a la solicitud de matrícula.

A partir de esta información que se encuentra tratada automatizadamente se pueden efectivamente tomar decisiones arbitrarias o discriminatorias, lo que nos lleva a concluir que los datos judiciales cuando son tratados automatizadamente, -lo que implica la posibilidad de cruce de datos- son datos sensibles.

Esta cualidad del dato judicial se hace más evidente aún en el caso de la sentencia analizada, ya que el dato se refiere a la calidad filiativa de una persona que a todas luces encuadra dentro del concepto legal de dato sensible, ya que se refiere a hechos o circunstancias de la vida privada o intimidad de las personas.

Habiendo ya categorizado los datos contenidos en la causa judicial de acción de reclamación paternidad en filiación no matrimonial, como datos sensibles, es necesario ahora, analizar la normativa establecida en la ley para ellos.

El artículo 10 de la ley 19.628, establece que los datos sensibles no pueden ser objeto de tratamiento, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares. Se establece acá, entonces, un principio general: nadie puede tratar datos sensibles, salvo las tres hipótesis mencionadas en la norma. Por lo demás, este artículo recibe plena aplicación a los órganos del estado, según lo indica el artículo 20 de la misma ley al señalar perentoriamente que el tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular. Por su parte, el artículo 1 de la ley al fijar su ámbito de aplicación indica que el tratamiento de datos de carácter personal en registro o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de la ley..... En todo caso, deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.

En el caso en cuestión, se infringió lo dispuesto en estos tres artículos, ya que se efectuó un tratamiento automatizado de datos de carácter sensible (y lo que es peor, se publicaron), estando ello prohibido por la ley, para todos, incluso para los órganos

públicos, de otra parte no se configuraban en los hechos de la causa ninguna de las tres hipótesis que indica el texto legal, para autorizar el tratamiento de este tipo de datos, esto es, autorización legal, del titular de los datos, o bien que sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares, de manera que el acto que se recurre es, por lo menos en este capítulo, ilegal.

Tampoco podríamos razonablemente señalar que el tratamiento que se efectuó de los datos en cuestión, se hizo dentro de la competencia de la Corporación Administrativa del Poder Judicial, o dentro de las atribuciones del Poder Judicial, ya que en esta materia los artículos 6 y 7 de la Constitución Política de la República, que establecen el principio de juricidad, son claros: "Los órganos del Estado actúan válidamente previa investidura regular de sus integrantes, dentro de su competencia y en la forma que prescriba la ley", Así, la competencia para efectuar esta publicación por Internet por parte del Poder Judicial, no está establecida ni en la Constitución ni en la ley, ni en ningún cuerpo normativo, y teniendo en cuenta que en derecho público sólo se puede hacer aquello que está expresamente permitido, colegimos que el actuar del Poder Judicial, no tiene fundamento jurídico, es inconstitucional, además, de no estar cumpliendo con lo establecido en la ley 19.628.

De esta manera, estamos en absoluto desacuerdo con lo fallado en el considerando sexto de la sentencia que se comenta cuando indica que: "no se advierte que mediante el sitio de Internet, se hayan proporcionado o se estén proporcionando datos sensibles relativos a la vida privada de la recurrente, ya que no se ha divulgado ningún hecho o circunstancia cuya privacidad resguarda la Ley 19.628".

Además señala el mismo considerando dentro del marco de la primera línea argumentativa indicada, que "no se ha transgredido el carácter secreto que reviste un proceso de filiación de la naturaleza del iniciado por la actora ya que ni su contenido, ni sus resoluciones se han dado a conocer a través de la página WEB del Poder Judicial".
Esta aseveración es simplemente falaz. El artículo 197 del Código Civil que se encuentra bajo el epígrafe "de las acciones de filiación", aplicable a la materia que trataba el juicio cuyos datos se publicaron en Internet señala que "El proceso tendrá carácter de secreto hasta que se dicte sentencia de término, y sólo tendrán acceso a él las partes y sus apoderados judiciales".

El carácter de secreto del proceso no se refiere solamente a la imposibilidad material de acceso por parte de cualquier persona distinta de las partes y de sus apoderados al expediente, sino que también abarca la imposibilidad de acceder a las

resoluciones dictadas en él, y no sólo a ellas, sino que a todo su contenido, esto es, a la información relativa a las partes, la materia, etc. De manera que al efectuarse el tratamiento automatizado de estos datos (nombres y RUN de las partes y apoderados, materia) de un proceso judicial, que según la ley ha de ser secreto, y aún más, al ser publicados en Internet efectivamente se transgrede la norma contenida en el 197 del Código Civil, por lo que el asevero contenido en la sentencia recién mencionado no se encuentra ajustado a Derecho.

Por otra parte, el considerando cuarto de la sentencia al señalar: "Que de este modo cabe concluir que la información que suministra el sitio WEB del Poder Judicial respecto de procesos iniciados de conformidad con las normas de la Ley 19.585, está limitada única y exclusivamente a lo que es posible obtener, por cualquier persona, de los libros de ingreso de causas de los Juzgados correspondientes cuyos datos son de público conocimiento", da a entender que por el solo hecho que los datos publicados en el sitio web poderjudicial.cl estén, en el vocabulario utilizado por el legislador en una "Fuente Accesible al Público", legitima tal actuar. Sin embargo, esto no es correcto, pues, lo que la ley establece y sanciona es el tratamiento de datos (automatizado o no), estableciendo que con respecto a los datos sensibles este tratamiento no es permitido, aun cuando conste la información en fuentes accesibles al público. A mayor abundamiento, no todos los datos que se encuentran en el sitio web en cuestión, se encuentran en los libros de ingresos de las causas, ya que en estos no se menciona el Rol Unico Nacional, que sí aparece mencionado en Internet.

La sentencia termina señalando en esta parte que se han armonizado de esta manera lo estatuido en el artículo 9 del Código Orgánico de Tribunales (publicidad actuaciones de los tribunales), con lo señalado en el artículo 197 del Código Civil (reserva respeto proceso de filiación) (considerando sexto). Ya se encuentra demostrado con lo dicho, que tal aplicación armónica de la norma no se ha producido, ya que si bien se ha aplicado en su integridad y con un criterio laxo el principio de publicidad, no ha ocurrido lo mismo con la excepción a este principio que recibía aplicación en el caso que estudiamos.

Finalmente, el tercer argumento basal del fallo, y sobre el cual se erigen las dos otras fundamentaciones, es el que indica que en el momento de dictarse el fallo la causa en cuestión ya no se singularizaba como "HIJO LEGITIMO, ACCIÓN", sino que "Acción Ley 19.585", al igual que todas las otras de su especie, sin que se pueda acceder a ningún dato acerca del contenido del proceso respectivo.

Con respecto a este punto, si bien el cambio, en la catalogación de la acción produce una variación en cuanto a la conculcación de la garantía de igualdad ante la ley, no ocurre lo mismo en cuanto a la vulneración del derecho a la intimidad, ya que a partir de esos datos publicados, y de libre acceso a quienquiera consultarlos, efectivamente se vulnera lo estatuido en la Carta Fundamental y los tratados Internacionales, que establecen el derecho de toda persona a la intimidad y a la vida privada.

En todo caso, la utilización de este fundamento formal para esgrimir la inexistencia del acto ilegal de que se trata, resulta del todo insuficiente para esos efectos, ya que como vemos, el acto ilegal persiste en la vulneración de la garantía señalada.

Habiendo revisado y cuestionado las argumentaciones piedras angulares del fallo, debemos indicar que el acto recurrido efectivamente es un acto ilegal, y lo es doblemente, ya que infringe dos estatutos legales, por una parte el Código Civil en su artículo 197, y por otra, la ley 19.628.

Corresponde ahora revisar un asunto con respecto al cual la Corte no se pronunció – debido a que a su entender no existía acto ilegal-, esto es, la conculcación de las garantías constitucionales mencionadas por la recurrente. Como ya indicáramos se recurrió de protección por la vulneración de las garantías que se analizan a continuación:

a.- En primer lugar, con este acto ilegal se conculca en grado de perturbación el derecho fundamental establecido en el numeral 4 del artículo 19 de la Carta Fundamental, esto es, "El respeto y protección a la vida privada y pública y a la honra de la persona y de su familia", pues, la Corporación Administrativa del Poder Judicial al hacer públicas, en el sitio web del Poder Judicial, las bases de datos que contienen la información de las causas que se tramitan en los Tribunales de Justicia (nombre y rut de las partes, materia y tipo de causa), permitiendo el conocimiento de esta información a quien lo solicite, vulnera la garantía que doctrinariamente se conoce como derecho a la intimidad y que es la que se protege con el numeral recién indicado, ya que los datos que se informan por este sitio web, en la materia que nos concierne (filiación de una persona), corresponden efectivamente a una información que está situada dentro de la esfera de la vida privada de la persona, dentro del ámbito de su intimidad, esto es, de todo aquello que no es o no queremos que sea de público conocimiento, de manera que al hacerlos públicos estos datos a través de Internet, se está afectando este derecho.

Por otra parte, en el caso en estudio, no sólo se afecta la vida privada, la

intimidad, la privacidad, como quiera que se le llame, sino que también, y por otro lado, en el entendido que son bienes jurídicos protegidos de distinta entidad o naturaleza, el honor de la persona y de la familia, es decir, el conjunto de cualidades éticas que permiten que la persona merezca y reciba consideración de los demás, esto porque lamentablemente en la sociedad en que vivimos un menor de edad del que se sabe está siendo discutida su filiación en Tribunales ve vulnerado su honor y también el de su familia, en los términos recién expuestos.

b.- En segundo lugar, se ve afectada la garantía constitucional establecida en el N° 1 del artículo 19 de la Constitución "El derecho a la vida y a la integridad física y psíquica de la persona", en grado de perturbación y amenaza, ya que con el acto ilegal se puede producir un deterioro psíquico en razón de posibles arbitrariedades o discriminaciones que se produzcan tanto con respecto a la recurrente como a su hija.

c.- Finalmente, se priva con este acto ilegal la garantía contendida en el inciso segundo del N° 2 del artículo 19, que señala que "ni la ley ni autoridad alguna podrán establecer diferencias arbitrarias", ya que al catalogar la causa, como acción de legitimidad y no como acción de reclamación de filiación no matrimonial, cuando ya se había efectuado la modificación legal respecto a la filiación (ley 19.585), que eliminaba la categoría de hijos legítimo-ilegítimos, implica a todas luces que se está ya no sólo efectuándose una distinción, una diferencia arbitraria, si no que además una ilegal, por parte del órgano público recurrido.

De su parte, estos derechos reciben reconocimiento constitucional, además, por la vía de tratados internacionales, como son el Pacto de San José de Costa Rica y la Declaración Universal de Derechos Humanos de 1948. Así el primero de ellos establece en su artículo 5 que toda persona tiene derecho a que se respete su integridad física, psíquica y moral. El numeral 11, que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad y que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

El segundo instrumento internacional mencionado, indica que todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona (artículo 3), además, su artículo 7 señala que todos son iguales ante la ley y tienen, sin distinción, derecho a igual protección de la ley. Finalmente, el artículo 12 nos señala que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección

de la ley contra tales injerencias o ataques.

Terminamos este comentario, señalando que el fallo en cuestión, asume una postura no garantística, con débiles fundamentos que evitan un análisis en mayor profundidad de la materia sometida a su conocimiento. Sospechamos que en el evento de haberse pronunciado acerca de la conculcación de las garantías invocadas, tal vez su contenido hubiese sido distinto.

Estando conscientes de la importancia y vastedad del tema, sólo esbozamos una posible solución a la problemática planteada a propósito de este caso. Pensamos que es necesario buscar una fórmula que realmente armonice el principio de publicidad de las actuaciones judiciales y el derecho a la información con el derecho a la intimidad y la protección de los datos personales en materia de tratamiento automatizado de datos judiciales y su publicación vía web. Así, se debe asumir un criterio defensor de la intimidad, pero que a su vez permita dar aplicación al ya tantas veces mencionado principio de publicidad, y al derecho que tienen las partes de conocer el estado de tramitación de sus causas judiciales; esto se puede lograr (como lo hace por ejemplo, el Poder Judicial Argentino www.ccc.pjn.gov.ar), distinguiendo entre los tipos de causas que resultan de un contenido más "sensible", como por ejemplo, las penales o las de menores, de aquellas con respecto a las cuales la ley no establece secreto o reserva, permitiendo el ingreso al contenido del expediente como un todo, pero sólo a través de su número de rol y con una clave para las primeras, y sólo a través del número de rol en las segundas.

10) Legislación extranjera y derecho comparado. Habeas data en Latinoamérica.

Como una forma de verificar el avance que existe en otros países en lo relativo a la protección de los datos personales por el uso de las nuevas Tecnologías de la Información, a continuación enumeramos las normas constitucionales relativas al habeas data y protección de datos personales en Latinoamérica.

1.- Argentina.

El Articulo 43 de la Constitución Nacional de 1994, tercer párrafo, establece que 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 aquellos. No podrá afectarse el secreto de las fuentes de información periodística.

La jurisprudencia argentina en materia de habeas data se ha desarrollado extensamente. Existen diversos fallos sobre el habeas data en Argentina. Existen asimismo otras normas vigentes que cumplen la función de leyes de protección de datos, y se están tratando actualmente varios proyectos de leyes sobre Protección de datos. Veamos algunas de estas normas positivas.

- Ley de Tarjetas de Crédito No. 25.065. La ley fue sancionada en el año 1998 y varios artículos fueron vetados. Pero el Congreso insistió y convirtió en ley también los artículos vetados en agosto de 1998. De especial importancia para la protección de datos es el art. 53 de la ley, que prohibe a los bancos expresamente informar a las centrales de riesgo privadas (las firmas que informan a los bancos sobre la conducta crediticia) si algún cliente de tarjeta está en situación de mora. La ley establece que los clientes morosos podrán informarse sólo al Banco Central. El articulo 53 (Prohibición de Informar) dice: "Las entidades emisoras de Tarjetas de Crédito, bancarias o crediticias tienen prohibido informar a las bases de datos de antecedentes financieros personales sobre los Titulares y beneficiarios de extensiones de Tarjetas de Crédito u opciones cuando el Titular no haya cancelado sus obligaciones, se encuentre en mora o en etapa de refinanciacion. Sin perjuicio de la obligación de informar lo que correspondiere al Banco Central de la República Argentina. Las entidades informantes serán solidaria e ilimitadamente responsables por los daños y perjuicios ocasionados a los beneficiarios de las extensiones u opciones de Tarjetas de Crédito por las consecuencias de la información provista". La norma aun no fue reglamentada.

- El Banco Central ofrece la posibilidad de consultar a través de Internet sus bases de datos con información de deudas financieras. Estas son (1) Central de Deudores Consulta de deudores: usando tipo y número de documento y denominación y la (2) Base de datos de Cuentacorrentistas Inhabilitados: aquí es posible consultar por

Personas Físicas, Tipo y número de documento, por Denominación Personas Jurídicas Tipo y número de documento Denominación. La consulta se realiza sobre las bases de información del Banco Central de la República Argentina conformadas por los datos recibidos de las Entidades Financieras. Un aviso en la pagina web del banco informa que "esta opción ha sido normada para consultas puntuales, no debiendo ser utilizada para descarga masiva de información. De constatarse tal situación, el B.C.R.A. se reserva el derecho de iniciar las acciones judiciales pertinentes más daños y gastos causídicos".

La jurisprudencia sobre Habeas Data se verifica en el caso "Urteaga" la Corte Suprema que estableció que el habeas data podía usarse para acceder a información publica. En el caso "Matimport" la Corte se refirió a las facultades del registro de juicios universales para tratar datos referidos a concursos y quiebras, manteniendo su validez por cumplir fines públicos. Finalmente en el caso "Scilingo" la Corte estableció limites al gobierno. En este caso la Corte Suprema de Justicia decidió que los ciudadanos pueden utilizar la acción de hábeas data para conocer los datos que poseen sobre ellos los organismos de seguridad, los que sólo podrán negarse a suministrar la información cuando se ponga en riesgo la seguridad del Estado.

En el caso "Cadaveira" un tribunal de apelaciones sostuvo que el Estado debe proveer información veraz en el mercado y que al no hacerlo afectada la privacidad de los individuos. Y agrego que el habeas data incluía la obligación de aclarar los datos erróneos que se han comunicado a terceros, no alcanzando solo con rectificarlos. Este caso permitió a un individuo no solo corregir información inexacta sino aclarar por el mismo medio (la base de datos del Banco Central) que nunca había estado inhabilitado y que se trato de un error del banco de datos estatal. Se trata de un claro establecimiento de limites a las facultades que tiene el Estado de almacenar y tratar datos personales.

El caso mas paradigmático en relación a las normas europeas en el sector privado es "Lascano Quintana c. Organización Veraz". Allí la Cámara Civil estableció como recaudo para el tratamiento de datos personales el consentimiento del registrado.

Por último, a fines de 1999 un fallo de un juzgado civil, a través de una sentencia correctamente fundada y de gran interés para los estudiosos de la privacidad, reconoció el "derecho al olvido", incluido dentro del habeas data pero con fundamentos también en el abuso de derecho del banco de datos privado.

2.- Brasil

La Constitución de Brasil de 1998 fue la primera en legislar el Habeas Data en Latinoamérica. Tiene varias normas referidas al habeas data. Estas normas son:

· concessão (art. 5.º, LXXII)
· gratuidade (art. 5.º, LXXVII)
· julgamento em recurso ordinário; competência do Supremo Tribunal Federal (art. 102, II, a)
· mandado de segurança; direito não amparado por (art. 5.º, LXIX)
· processo e julgamento; competênciado Superior Tribunal de Justiça (art. 105, I, b)
· processo e julgamento; competência do Supremo Tribunal Federal (art. 102, I, d)
· processo e julgamento; competência dos Tribunais Regionais Federais e seus juízes (art. 108 I, c e art. 109, VIII)

· Las normas mas importantes son:

· Art. LXXII Se concederá "habeas data":
· a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público;
b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo;

· Art. LXXVII son gratuitas las acciones de "habeas corpus" y "habeas data" y, en la forma de la ley, los actos necesarios al ejercicio de la ciudadanía.

· Art. 108. Es competencia de los Tribunales Regionales Federales: I procesar y juzgar, originariamente:.. c) los "mandados de seguranca" y los "habeas data" contra actos del propio Tribunal o de los jueces federales;

A fines de 1997 se dicto la Ley reglamentaria de Habeas Data. Ley nº 9.507, del 12.11.97. (Regula o direito de acesso a informações e disciplina o rito processual do

habeas data). Se refiere solo a los aspectos procesales y no trata cuestiones de protección de datos.

3.- Colombia

El art. 15 de la Constitución de Colombia establece que "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recog ido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley".

En Colombia se dictó una ley sobre habeas data que la Corte Constitucional declaró inconstitucional por cuestiones formales. También hay fallos muy importantes que establecen normas jurisprudenciales sobre protección de datos. Son las sentencias de unificación jurisprudencial que han establecido un derecho judicial relativo a la eliminación de los datos por el transcurso del tiempo y al consentimiento para el tratamiento de datos personales.

4. Nicaragua

El artículo 26 establece que toda persona tiene derecho a su vida privada y la de su familia, a la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo, a respeto de su honra y reputación. Y el art. 26 punto 4 crea un derecho similar al habeas data al establecer que tiene derecho a "A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información".

5. Perú

La constitución del Perú de 1994 establece en su artículo 2.- Toda persona tiene su derecho:

· 5. A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con le costo que suponga el pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional. El secreto bancario y la reserva tributaria puedan levantarse a pedido del juez, del Fiscal de la Nación, o de una comisión investigadora del Congreso con arreglo a ley y siempre que se refieran al caso investigado.

· 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afectan la intimidad personal y familiar.

· 7.Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, son perjuicio de las responsabilidades de ley. ...

· 9. A la inviolabilidad del domicilio. Nadie puede ingresar en él ni efectuar investigaciones o registros sin autorización de la persona que lo habita o sin mandato judicial, salvo flagrante delito o muy grave peligro de su perpetración. Las excepciones por motivos de sanidad o de grave riesgo son reguladas por la ley.

En la práctica el habeas data en Perú funciona tanto como un instrumento protector de la privacidad pero también como una norma de acceso a la información pública para el ciudadano. Existen varios casos relativos a ambas instancias. EL habeas Data esta reglamentado procesalmente.

6. Paraguay

La Carta Magna de Paraguay contiene una serie de interesantes normas sobre libertad de expresión y derecho a la privacidad. La Constitución de Paraguay de 1992 regula el habeas data en el art. 135: Toda persona puede acceder a la información y a los datos que sobre sí misma o sobre sus bienes obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos si fuesen erróneos o afectaran ilegítimamente sus derechos.

7.- Uruguay

En cuanto al Habeas Data, no existe en Uruguay previsión legal ni constitucional alguna que lo contemple. En un articulo publicado en REDI, titulado La protección jurídica de los "datos personales" y los servicios de información comercial y crediticia, Marcelo Bauzá Reilly da un panorama del habeas. Este autor sostiene que el país no tiene ... normas de carácter especial sobre esta cuestión de los "datos personales" y su regulación jurídica, aunque existen síntomas que permiten deducir que las tendrá en fecha no lejana. Y si bien un régimen en forma necesita mayores previsiones, no hemos seguido hasta el momento, siquiera, la reciente tendencia latinoamericana de incluir artículos constitucionales contemplativos del instituto de habeas data, siendo el único país del Mercosur que no lo ha hecho. Exceptuando unas pocas previsiones sectoriales ... la situación es de vacío -o prácticamente tal- en cuanto a la existencia de un régimen específico que regule la apropiación y uso de los datos personales por parte de Estado y los particulares terceros.

8. Venezuela

La reforma de la Constitución en 1999 incluyo una cláusula contemplando el habeas data.

11) Spam o correo no solicitado como violación de nuestra privacidad.

No existe una definición canónica de "spam." Ni siquiera existe demasiada claridad respecto al origen de la expresión.[80] Desde luego actualmente existe consenso en el hecho que la expresión incluye el correo electrónico no deseado; esta acepción es la que interesa examinar en las páginas siguientes.

Spam son mensajes electrónicos (habitualmente de tipo publicitario)[81] no solicitados enviados en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de spam incluyen mensajes, grupos de noticias usenet, motores de búsqueda y blogs. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.

Curiosamente para nosotros, el spam mediante el servicio de correo electrónico nació a patir del día 5 de Marzo de 1994. Este día Laurence Canter y Martha Siegel eran una pareja de abogados que comenzaron a ofrecer servicios legales relacionados con asesoría en materias de inmigración que consistían en asegurar a sus potenciales clientes –previo pago de US $100- su inclusión en las listas de lotería que seleccionan las solicitudes de visa que serán tramitadas. La oferta de la firma de abogados fue llevada a cabo poniendo un aviso en más de 6.000 grupos de discusión Usenet. La pequeña firma de abogados recibió un buen número de respuestas de clientes potenciales. Junto a esto, recibieron miles de respuestas airadas reclamando el envío de publicidad no solicitada. Esta avalancha de respuestas excedió la capacidad del proveedor de servicios de Internet de los abogados, de manera que, al corto andar, su cuenta fue cancelada.

---

[80] La expresión "spam" corresponde originariamente al nombre de un tipo de carne enlatada con especies -jamón con especias (spiced ham)- producida por Hormel Foods a partir de 1926, cuya principal característica era que no requería refrigeración. Esta característica la hizo extremadamente atractiva para el ejército y la popularizó durante la Segunda Guerra Mundial.

[81] LLANEZA GONZALEZ, Paloma; "Internet y Comunicaciones Digitales (Régimen legal de las tecnologías de la información y la comunicación)", página 272, realiza una distinción un poco más sutil, afirmando que *"...se denomina 'junk mail' o 'garbage mail', al correo basura, que por lo general, no tiene carácter comercial y que suele provenir de direcciones no anónimas. Los casos más frecuentes son las pesadísimas cartas cadenas ('chain letter') sobre la buena o mala suerte, virus informáticos inexistentes, niños gravemente enfermos que desean recibir correos electrónicos de todos los confines de la tierra*..", Editorial Bosch, Barcelona, España, 2000.-

Algo más tarde, la pareja de abogados publicó un libro llamado HOW TO MAKE A FORTUNE ON THE INFORMATION SUPERHIGHWAY dando noticia sobre técnicas de recolección de direcciones de correo electrónico desde grupos de discusión y sobre cómo enviar masivamente publicidad por medios electrónicos.

Los spammers (individuos o empresas que envían spam) utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de robots o programas automáticos que recorren internet en busca de direcciones. Algunas de las principales fuentes de direcciones para luego enviar el spam son:

- Las propias páginas web, que con frecuencia contienen la dirección de su creador, o de sus visitantes (en foros, weblogs, etc.).
- Los grupos de noticias de usenet, cuyos mensajes suelen incluir la dirección del remitente.
- Listas de correo: les basta con apuntarse e ir anotando las direcciones de sus usuarios.
- Correos electrónicos con chistes, cadenas, etc. que los usuarios de internet suelen reenviar sin ocultar las direcciones, y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje.
- Páginas en las que se solicita tu dirección de correo (o la de "tus amigos") para acceder a un determinado servicio o descarga.
- Compra de bases de datos de direcciones de correo a empresas o particulares (ilegal en la mayor parte de los países).
- Entrada ilegal en servidores.
- Por ensayo y error: se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes. Un método habitual es hacer una lista de dominios, y agregarles "prefijos" habituales. Por ejemplo, para el dominio microsoft.com, probar info@microsoft.com, webmaster@microsoft.com, staff@microsoft.com, etc.

Una vez tienen una gran cantidad de direcciones de correo válidas (en el sentido de que existen), los spammers utilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones. Esto supone un costo mínimo para ellos, pero perjudica al receptor (pérdidas económicas y de tiempo) y en general a internet, por

consumirse gran parte del ancho de banda en mensajes basura.

Además, es frecuente que el spammer controle qué direcciones funcionan y cuáles no por medio de web bugs o pequeñas imágenes o similares contenidas en el código HTML del mensaje. De esta forma, cada vez que alguien lee el mensaje, su ordenador solicita la imagen al servidor del spammer, que registra automáticamente el hecho. Son una forma más de spyware. Otro sistema es el de prometer en los mensajes que enviando un mail a una dirección se dejará de recibirlos: cuando alguien contesta, significa no sólo que lo ha abierto, sino que lo ha leído.

Recientemente, han empezado a utilizar una técnica mucho más perniciosa: la creación de virus troyanos que se expanden masivamente por ordenadores no protegidos (sin cortafuegos). Así, los ordenadores infectados son utilizados por el spammer como "ordenadores zombis", que envían spam a sus órdenes, pudiendo incluso rastrear los discos duros en busca de más direcciones. Esto puede causar perjuicios al usuario que ignora haber sido infectado (que no tiene porqué notar nada extraño), al ser identificado como spammer por los servidores a los que envía spam sin saberlo, lo que puede conducir a que no se le deje acceder a determinadas páginas o servicios.
Actualmente, el 40% de los mensajes de spam se envían de esta forma.

La ventaja de los mecanismos de marketing directo es que permiten llegar a los consumidores en términos que, al menos estadísticamente, llamarán su atención con mayor intensidad que mecanismos alternativos como publicidad en las calles o avisos en televisión. Lo anterior, sin embargo, posee costos. En el caso del envío de publicidad por correo regular, por ejemplo, es el avisador quien soporta la gran mayoría –sino todos- los costos del envío de la publicidad. De esta manera se invertirá en marketing directo en la medida que la ganancia proveniente de la respuesta de los consumidores supere a los costos de alcanzar a los consumidores. En el envío de publicidad masiva por correo electrónico, sin embargo, la ecuación entre costos y beneficios difiere.

En el caso del spam la mayoría de los costos del envío no son soportados por quien envía las comunicaciones. En general los costos que asume quien envía el spam son el de encontrar un proveedor de servicios de Internet suficientemente inocente, la composición del mensaje y el establecimiento de un sistema de procesamiento de pago por los bienes o servicios, en el caso que los provea el mismo, o bien la contratación de este servicio en caso contrario. El costo marginal de enviar un correo electrónico más es prácticamente inexistente, por lo tanto, los incentivos del emisor son enviar tantos

mensajes como sea posible.

Que los spammers no soporten la mayoría del costo de su actividad no significa que dicho costo no sea asumido por alguien. Como ya ha sido suficientemente acreditado, los costos siempre se radican en alguien, el problema es decidir en quién.34 En el caso del envío de spam los costos son soportados básicamente por los proveedores de servicios de Internet y los usuarios que reciben correo comercial masivo no solicitado.

El problema más serio suele ser de los proveedores de servicios. El spam representa una proporción significativa del tráfico de correos electrónicos, consumiendo de esta manera cantidades relevantes de ancho de banda, memoria, espacio de almacenamiento y otros recursos.

Junto a los proveedores de servicios, los segundos afectados son los usuarios de Internet. Quien recibe correos no deseados en su casilla electrónica utiliza su tiempo y dinero para procesarlos. [82]

Además de los proveedores de servicios y a los usuarios, el spam puede producir un daño más global a la Red. La proliferación incontrolada del spam podría tener un cierto efecto paralizante sobre Internet, ya sea porque el contenido de los mensajes de publicidad –buena parte de ellos sobre sitios pornográficos con lenguaje extraordinariamente explícito o imágenes suficientemente elocuentes [83]- disuada a los usuarios dejen de interactuar en la Red por temor a que sus datos sean recogidos por spammers o por que el número de correos electrónicos no solicitados simplemente sature la Red.

- El tratamiento del spam en la legislación chilena.

El envío de comunicaciones comerciales no deseadas se encuentra explícitamente tratado en la Ley 19.628 sobre protección de la vida privada. Conviene, examinar si protege a los titulares de datos de la recolección de sus direcciones de

[82] en Chile ya se ha determinado que esta práctica genera enormes perjuicios a los receptores de dichos correos. La Cámara de Comercio de Santiago los ha cuantificado en aproximadamente 36 millones de dólares al año. Ellos derivan del tiempo necesario para eliminarlos y de los costos de conexión que asume y debe pagar el receptor.

[83] Según información proporcionada por CISCO Systems Chile durante 1999, el 30,2% de los email no solicitados poseían contenido pornográfico, 29,6% consistía en ofertas para "hacerse rico", 23,5% buscaba vender otros productos o servicios, 9,9% ofrecía productos relacionados a la salud y 3,3% ofrecía entrada a sorteos o a juegos de azar.

correo electrónico y el posterior envío de comunicaciones no deseadas.

Recordando el análisis realizado a la ley, podemos señalar en primer lugar que la Ley establece dos tipos de datos relevantes, los de carácter personal (o datos personales) y los datos sensibles. Los datos personales refieren únicamente a las personas naturales y por la amplitud de su definición corresponden a cualquier información sobre una persona que pueda ser identificada. La Ley 19.628 no provee de criterios para determinar cuándo es identificable una persona. Se puede considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social. Respecto a los datos sensibles, a diferencia de otras normativas sobre privacidad, la Ley 19.628 establece una categoría de datos y luego ejemplos que la ilustran.

En segundo lugar, la Ley 19.628 consagra como principio general la obtención del consentimiento del titular de los datos para su tratamiento. De esta manera el artículo 4º prescribe en su inciso primero que: "el tratamiento de los datos personales con fines de publicidad, investigación o mercado sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello."

Las excepciones a la obligación de obtener el consentimiento del usuario se encuentran consagradas a partir del inciso 2º del artículo 4, algo más abajo de la regla general. La primera excepción queda constituida por la obtención de datos personales en fuentes accesibles al público. La accesibilidad al público de las fuentes quedará determinada según si estas se encuentran o no restringidas a los solicitantes ¿cuáles son entonces las fuentes accesibles al público? La interpretación más razonable parece ser que son aquellas en que por ley el acceso no se encuentra restringido por ley. Si esta es la interpretación es correcta, entonces la regla general es que todas las fuentes, salvo las exceptuadas explícitamente por ley, son accesibles al público y, por lo tanto puede llevarse el tratamiento de los datos personales contenidos en ellas sin autorización de sus titulares.

Según se ha advertido anteriormente, el problema del spam tiene que ver con dos cosas, la primera es la recolección de datos y, la segunda, con el envío masivo de correos. Se trata de examinar entonces ambas situaciones bajo el prisma de la Ley 19.628.

Aún cuando la expresión tratamiento de datos personales comprende, según la letra o) del artículo 2º de la Ley 19.628 la recolección de datos personales y, por lo

tanto, esta es regulada a partir del artículo 4º, el artículo 3º establece ciertas limitaciones a ella. La limitación, sin embargo, solo se aplicaría a aquella recolección de datos que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes. La limitación en cuestión exige que se informe a los titulares de dichos datos acerca del carácter obligatorio o facultativo de sus respuestas y el propósito para el cual se está solicitando la información. Además le asigna al titular la posibilidad de oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.

La actividad que parece estar reglando esta norma no es la recolección de direcciones de correos electrónicos con el fin de enviar publicidad, sino más bien la recolección de información sobre algún tipo de hábitos del sujeto para luego hacer públicos los resultados sin que sea posible identificar a las personas consultadas. No obstante lo anterior, aún cuando el fin inmediato de esta recolección no sea el marketing a través de correos electrónicos es perfectamente posible que estos se utilicen más adelante por quien los recolecta o bien por otra persona a quien sean transferidos, para campañas de spam. La protección de la Ley consiste en que el sujeto debe ser informado del carácter facultativo u obligatorio de sus respuestas y el propósito para el cual se está recolectando su información. En segundo lugar, el titular de los datos puede oponerse a su utilización con fines de publicidad. Cabe advertir que no se exige el consentimiento explícito del sujeto, sino nada más informar acerca del carácter de la respuesta.

En segundo lugar no se exige que la persona autorice que sus datos sean utilizados con fines de publicidad, sino que se le da el derecho a oponerse. Ahora bien, no es el artículo tercero la principal causa de preocupación. Como ya se ha advertido, en lo hechos, el artículo 4º autoriza el tratamiento de datos personales –incluida su recolección- sin necesidad que el titular lo autorice, siempre y cuando estos:

1. provengan de fuentes de acceso público
2. cuando sean de carácter económico, financiero, bancario o comercial
3. se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento
4. sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes y servicios.
5. sean tratados por personas jurídicas privadas para el uso de exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación

u otros de beneficio general de aquellos.

Una respuesta respecto a la situación legal del spam en Chile puede intentarse sintetizando el artículo 4º de la siguiente manera:

"No requiere autorización el tratamiento de datos personales cuando estos sean necesarios para las comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes y servicios."

Pues bien, se ha advertido ya que en Chile no existen limitaciones legales para recolectar direcciones de correo electrónico ¿qué sucede con el envío? La respuesta más sintética consiste en afirmar que el envío también queda cubierto por la expresión "tratamiento de datos" y por lo tanto no requiere autorización previa.

12) Ley de Protección a los Consumidores, últimas modificaciones.

La discusión sobre el spam en Chile tomó un nuevo cariz cuando a principios del año 2003 el Ministerio de Economía decidió incluir el tema dentro de la ley de derechos del consumidor.

En un primer momento se decidió por el "opt in", es decir, que sólo aquellos destinatarios que hubiesen solicitado los mensajes publicitarios los recibieran, tal como sucede en la Comunidad Europea.

Esta iniciativa pasó a la Cámara de Diputados, donde fue aprobada por unanimidad y posteriormente, a la Comisión de Economía del Senado, donde el tema volvió a ser discutido hasta que surgieron otras dos posturas frente al asunto. Una de estas fue la del "opt out", presentada por el senador UDI Jovino Novoa y que fue aprobada y ratificada por la Cámara de Diputados.

"Durante la discusión del proyecto en la Comisión de Economía, se evaluaron ambas posibilidades" explicó en ese momento el senador Novoa. "Entendiendo que ambos sistemas tienen sus ventajas y desventajas, decidimos aprobar el opt out, que permite un primer envío de publicidad para que el consumidor, posteriormente, decida si desea o no seguir recibiendo dicha información".

Esta elección, señala el parlamentario, favorecería en cierto modo a las empresas chilenas. "El opt in, o de autorización previa, perjudicaría a las empresas chilenas, ya

que las empresas extranjeras no tendrían problema alguno para enviar spam desde fuera" indica el senador , explicando que de este modo se consideró al spam como una manera de ayudar a las Pymes "ya que para ellas, éste es el medio más barato de dar a conocer sus productos o servicios"[84].

El parlamentario agrega que entiende que esta opción tiene el problema de la validación de la base de datos y el respeto a la privacidad de la información personal del usuario particular. "Por ello, en la sala, el Ejecutivo, con acuerdo nuestro, presentó una indicación para solucionarlo, en la medida posible, mediante la creación de un registro en el cual debían inscribirse las empresas que deseaban enviar información comercial" explica.

Este sistema, ya ha sido utilizado en Estados Unidos e implica que las firmas que deseen enviar spam deben individualizarse en un registro indicando su nombre o razón social, domicilio, rut, e-mail, representante legal y número de registro en el SERNAC. Así como también obliga a la empresa a consultar en su mensaje si la información personal entregada por el usuario podría ser utilizada para otras cosas, medida que hasta cierto punto frenaría el tráfico de bases de datos.

Pero para que esta indicación fuera aprobada, requería el voto unánime de los senadores, el que, por una persona, no se obtuvo finalmente. Con esto, se aprobó el opt out dejando fuera esta indicación específica de protección a los usuarios.

Aquella indicación especificaba que "la segunda comunicación que envíe la empresa y que no cuente con la autorización expresa del consumidor será considerada infracción a la Ley y habilitará a ésta o al Servicio Nacional del Consumidor a accionar. Asimismo, el consumidor o el Servicio Nacional del Consumidor podrá requerir al proveedor de servicios de Internet el bloqueo del emisor de las comunicaciones, sin que ello pueda ser considerada denegación de servicio por parte de éste". Sin embargo, esta

[84] Es común que este parlamentario de la UDI concentre sus ideas en protección de las empresas por sobre el de las personas. Una muestra tangible, además de su intervención en la modificación de la Ley del Consumidor se ve reflejada en el actual proyecto presentado por él ante el Congreso Nacional el 1º de marzo de 2005, que tiene como título "Modifica la ley Nº 19.628, sobre protección de la vida privada, con el fin de evitar el uso abusivo de datos personales o de empresas y de resguardar a los usuarios de correos electrónicos de la propaganda comercial no solicitada. " y que actualmente se encuentra en etapa de Primer Trámite Constitucional, subetapa de Primer Informe de Comisión de Constitución, Legislación, Justicia y Reglamento , y que en su artículo 1º reza: Artículo 1º:
1.) Sustitúyese el artículo 2º letra f) de la ley 19.628, por el siguiente:
"Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales o jurídicas, identificadas o identificables.".
Abre pues, la puerta para que todos los derechos referidos en la ley 19.628 y que se centra en las personas, puedan ser aplicados a las PERSONAS JURIDICAS que están compuestas, mayoritariamente, por empresas.

indicación no fue aprobada.

En este escenario poco auspicioso se aprueba el proyecto de ley 19.955, modificatoria de la ley 19.496 sobre Protección a los Derechos de los Consumidores, estableciendo una norma especial referente al spam, en el artículo 28 B, que indica: "Toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos."

Los spammers sólo serán sancionados con las multas relacionadas con publicidad engañosa que establece la ley del consumidor, por ejemplo contra quien "a sabiendas o debiendo saberlo y a través de cualquier tipo de mensaje publicitario induce a error o engaño", como reza el artículo 28 de esta normativa.

Pero, si existieran castigos específicos para los spammers en nuestro país ¿a quién se debería sancionar? ¿al que envía el spam? ¿a quien vende las bases de datos? ¿o a quien fabrica el producto promocionado?. "A todos los nombrados, porque coinciden en las calidades, pero con responsabilidades diversas", es la opinión del profesor chileno Renato Jijena, pues "El que lo envía directamente es el principal responsable, aun cuando alegue que lo hizo por encargo de otro, como el vendedor del producto".

En la práctica existen incluso situaciones que no son amparadas, existiendo un verdadero vacío legal, pues suele no darse entre el emisor del correo electrónico no deseado, invasivo y perjudicial y el receptor del mismo, una relación de aquellas "entre proveedores y consumidores" que se regulan en el contexto del derecho de los consumidores. Dicho de otra forma, los e-mails que saturan las casillas o buzones de correo electrónico pueden no contener ofertas, promociones comerciales o publicidad engañosa y no ser emitidos por proveedores que ofertan un bien a cambio de un precio.

El SERNAC o el Servicio Nacional del Consumidor se ha deslegitimado además, para abordar el tema del "spam" en el marco de la ley de derechos de los consumidores, porque, a esta fecha, se limita a entender que no se trata de prácticas de publicidad engañosa o de ofertas realizadas por proveedores o prestadores de servicios en el marco de una relación comercial directa con un consumidor.

Nuestra percepción es que los parlamentarios, al optar derechamente por facilitar el negocio de las promociones comerciales, no repararon en los detalles prácticos. Una muestra de que si uno solicita ser removido no se hace sino comprobar que tiene la

casilla activa: recibí un correo de "berlitz@tie.cl", y al solicitar ser removido apareció la dirección "hideagent@yahoo.com.ar" , lo que me llevaba a registrarme en una base de datos Argentina (por cierto, estadísticamente uno de los países "paraíso" de los "spammers") y en donde ninguna posibilidad tiene de ser aplicada la ley chilena.

¿Constituye un real incentivo para dejar de enviar correos electrónicos no solicitados la multa de hasta 50 UTM, que establece la ley?

La dificultad que presenta para el consumidor dirigir un reclamo o demanda en contra de un spamer, respecto del cual, no posee información básica como su nombre o dirección o, incluso, que se puede encontrar fuera de la jurisdicción nacional.

Dado el ámbito de aplicación de la Ley de Protección a los Consumidores, la norma sobre spam, no aplica a todos aquellos correos que tengan una naturaleza gratuita (invitaciones gratuitas a eventos, campañas políticas, etc.).

Tampoco aplica si los bienes o servicios que se ofrecen en el spam no van a ser adquiridos por los destinatarios finales de esos bienes o servicios, como por ejemplo, envío de spam a proveedores, distribuidores, importadores, etc.

Tampoco se aplica si en el correo electrónico se invita a la celebración de un acto jurídico que sea civil para ambas partes, lo que puede ser de frecuente ocurrencia.

No aplicará tampoco, si el spam no tiene fines promocionales o publicitarios, según la definición que de estas actividades realiza la ley.

Ni aplica a la oferta de servicios por profesionales independientes, así como tampoco a la oferta de bienes o servicios hacia la administración del Estado.

En conclusión, si bien, ha de reconocerse la buena voluntad del legislador al normar estas materias, tal espíritu no resulta suficiente, dado el restringido ámbito de aplicación de la Ley de Protección al Consumidor. Lo que se necesita es una normativa que sea de aplicación general y a cualquier tipo de spam, que permita la persecución de estas conductas a través, por ejemplo, de registros de spamers, iniciativa planteada por el ejecutivo por medio de una indicación al proyecto de modificación a la ley que, en definitiva, fue rechazado por el Congreso y por último que se establezcan sanciones acordes con el bien jurídico protegido en estas materias: la privacidad.

- Modificaciones y medidas sugeridas para evitar y sancionar el Spam

Como una manera de regular en forma mas precisa cuando estamos frente a un

mensaje spam, es que mencionamos una serie de medidas que se podrían aplicar perfectamente acorde a la legislación nacional.

- El receptor puede querer o no recibir el correo. Para evitar su perjuicio, siempre debe ser consultado previamente (opt in) sobre cuál es su intención. Esta consulta puede hacerse o en el sitio WEB del proveedor o mediante un correo destinado exclusivamente al efecto -mandado sólo previo registro y autorización del "spammer", de manera que el receptor pueda verificar en el sitio WEB del SERNAC (mientras no exista en Chile un órgano ad hoc) la realidad e idoneidad del que se lo manda antes de aceptar, rechazar o no hacer nada.

- La autorización debe ser expresa y quedar registrada. El silencio o el no envío de respuesta debe entenderse como rechazo y no como una aceptación tácita (quien calla no otorga). No se puede obligar a contestar, sea para autorizar el "spam" o para pedir ser borrado de la lista, porque lo que se logra es que el "spammer" sepa que la casilla está activa. Sólo debiera contestarse para decir que si a la futura recepción.

- Debiera establecerse expresamente un artículo que dijera que "carecerá de todo valor legal la cláusula que se contenga en los términos legales o condiciones de uso de los sitios WEB, y que establezca que el mero ingreso del usuario a dicho sitio importa la manifestación de un consentimiento tácito para recibir "spam"". Lo dicho, a la luz de la ley 19.995 del 14 de Julio del 2004, puede entenderse incluido en el nuevo artículo 12 A que se incorporó a la ley de los consumidores, el que establece que la sola "visita" -debiera decir ingreso- a un WEB site no impone a los consumidores -por regla general- obligación alguna.

- El opt out o el envío permitido a priori, sujetado a la obligación de ofrecer la posibilidad de ser borrado, no evita que se envíen correos anónimos, no evita que los costos del negocio (el franqueo del correo) lo sigan asumiendo los consumidores, y le sigue traspasando una carga injusta a los receptores de los correos, mismos que se encuentran con las vitrinas de las ofertas en su PC (invasión de la propiedad) sin que lo hayan querido.

- Existencia de un registro obligatorio previo (base de datos de "spammer"), para personas naturales o empresas nacionales o extranjeras que deseen operar y enviar correos a destinatarios domiciliados en Chile, sea desde servidores ubicados en Chile o en el extranjero. El envío de "spam" sin registro previo debe constituir infracción y ser sancionado expresamente. Se trata de poner barreras de entrada al negocio a los beneficiados, a los "spammer", obligándolos a funcionar previo registro obligatorio para evitar el anonimato.

- Si se acepta el envío de un primer correo de consulta obligatorio e igual para todos, este sólo puede tener este objetivo, sin promociones y ser enviado sólo por un spammer previamente registrado.

- No deben elaborarse listas de destinatarios de correos electrónicos, sea de los que quieran recibirlos, sea de los que no quieran. Sólo se logra entregar información sobre casillas activas.

- Los emisores registrados deberán identificarse al enviar sus correos, con indicación expresa del número de registro asignado.

- Los emisores registrados sólo debieran poder enviar correos a quienes a su vez están registrados como receptores interesados en recibir "spam", sea porque se anotan en el sitio WEB del proveedor, sea porque consienten expresamente ante una consulta.

- Si ante una petición de eliminación el spammer no borra la dirección del destinatario, contravención (multas) e incluso delito (sanciones penales).

Estas serían, pues medidas constructivas para regular en forma correcta este mal que es llamado SPAM.

Capitulo V Protección Penal

"Si lo entiendes, está obsoleto"

Anónimo

1) Concepto y características de un Derecho Penal Informático

El impacto de la informática en la sociedad, inevitablemente acarrea la transformación del orden jurídico tradicional. La revolución que han significado las innovaciones tecnológicas recientes han revelado la incapacidad experimentada por las normas establecidas por el Derecho Penal tradicional. Este conjunto de normas punitivas han visto superada su capacidad para enfrentar la aparición de numerosas conductas disvaliosas impensadas en otras épocas.

La informática si bien ha servido de puente comunicador entre los avances tecnológicos y el acceso masivo a las diversas fuentes de información, trajo aparejada la aparición de nuevas formas de delinquir y, a su vez, ha permitido el perfeccionamiento de las ya existentes. Los sujetos activos de esta modalidad de delincuencia se han caracterizado por recurrir al uso instrumental de ordenadores para cometer sus fechorías y actualmente han diversificado sus medios de comisión a través de las redes telemáticas,que interconectan estos dispositivos.[85]

El fenómeno descrito dejó al descubierto la necesidad de realizar un proceso de adaptación de los sistemas normativos, los que han debido crear las correspondientes figuras típicas para incriminar las conductas de reciente aparición.La respuesta de algunos juristas origina el derecho informático, cuyo contenido en parte comprende dos ámbitos interrelacionados que aquí queremos destacar:

1º La problemática respecto de la privacidad, que requiere la estructuración de una

[85] Red Telemática: se refiere a la aplicación de la informática en redes de telecomunicaciones. Las redes de conexión pueden ser locales, metropolitanas, nacionales o internacionales.

normativa específica, fundamentalmente por la existencia de grandes bancos de datos nominativos y la posibilidad de su interconexión telemática, y

2º La problemática de los delitos informáticos, ya sea ubicando a la informática como medio utilizado para consumar el delito o como objeto de comisión del mismo, constituye un factor criminológico de creciente importancia que va requiriendo la estructuración de tipologías y regulaciones específicas.

Considerando los radicales cambios ocasionados por los progresos tecnológicos el delito no siempre puede ser analizado con las perspectivas tradicionales de la criminología, casi en forma natural entramos en una nueva perspectiva para el análisis jurídico penal: el denominado derecho penal informático.

Para Jijeva Leiva[86] no se trata de pensar en un nuevo Derecho Penal sino de adaptar el vigente a las nuevas exigencias, configurando y considerando nuevos bienes jurídicos, analizando las modalidades de atentar contra los mismos y, en definitiva, tipificando nuevas figuras criminales. Hablar y referirse a una necesidad de legislación penal nueva (entiéndase adaptada) lleva envuelta la necesidad de demostrar la forma en que se atenta en contra de algo o alguien y cómo ese atentado produce un daño.

El pretender justificar la existencia de un derecho penal que pueda comprender y abracar las tecnologías de la información hace necesario el tratar de involucrar los ámbitos de la ciencia y explicar su interrelación a fin de poder justificar en realidad la existencia del derecho penal informático o aún de un derecho que pueda contener a las tecnologías de la información sin perder su esencia de ciencia social y sin subvertir los principios que le han mantenido vivo desde la época romana que es la que hoy nos funge de base.

Por ende, no creemos para nada aconsejable crear un nuevo Derecho Penal ex novo, desligado del que actualmente se estudia en las Escuelas de Derecho, pero sí consideramos imprescindible que aquél sea revalorizado y adaptado.

Esto último nos sirve de fundamento para reclamar la autonomía del Derecho Penal Informático, por lo menos a nivel metodológico, a nivel de la cátedra, debiendo ser estudiado, ciertamente, como parte importante de un curso de derecho informático.[87]

---

[86] Jijena Leiva, Renato Javier, Chile, la protección penal de la intimidad y el delito informático, Santiago, Ed. Jurídica de Chile, 1992

[87] Esta necesidad se ve reflejada en que la Universidad de Valparaíso NO cuenta con NINGUNA cátedra que aborde temas referidos al Derecho y las nuevas Tecnologías de la Información, tal como ocurre en otras Universidades nacionales, tanto las tradicionales como la Universidad de Chile como las privadas en el caso de la Universidad Diego Portales, donde incluso funciona a su alero la Fundación Fernando Fueyo

Hay que entender que independientemente de los progresos económicos, sociales y culturales inducidos por la informática, las nuevas tecnologías engendran nuevos tipos de delincuencia, a los que los practicantes del Derecho Penal deben aportar una respuesta. Tal es el caso de la ley francesa del 6 de enero de 1978, la que indudablemente contribuyó a la definición de un derecho penal especial de la informática en la medida en que los principios esenciales de su texto fueron combinados con sanciones penales. Es el conjunto de las disposiciones el que apunta a sancionar los atentados a las personas, realizados a través de la manipulación de datos personales que les conciernan: La loi du 6 janvier 1978 crée un droit pénal spécifique qui sanctionne les atteintes aux droits fondamentaux de personnes au travers des manipulations de données permettant leur identification.[88]

Es evidente que los ilícitos y los abusos informáticos en cierta forma han sorprendido a los penalistas, situación que en parte se debe —y no nos cansamos de repetirlo— a que el Derecho Penal anterior al desarrollo de la informática no pudo prever sus implicancias criminales y, además, a que por ser novedoso el tratamiento de esta materia, de esta temática, se caracteriza por una notable falta de precisión. En nuestra opinión, tanto para ilustrar a los iuspenalistas como para encontrar la necesaria claridad conceptual, no basta con modificar el Derecho Penal tradicional: es necesario investigar y desarrollar un derecho penal de la informática.

En un principio, se observa una reacción a nivel privado frente a las primeras manifestaciones de invasión no autorizada por los sujetos agentes de las conductas descritas, procediéndose al fortalecimiento de los mecanismos de seguridad de los sistemas que se vieron afectados, pero simultáneamente se producía de parte de los transgresores un perfeccionamiento en sus técnicas de intromisión lo que, se tradujo en una rápida superación de estas nuevas defensas.

Posteriormente, ante esta realidad se consideró muy necesaria la participación del Estado y sus organismos, para consolidar la adecuada complementación de los mecanismos de seguridad privados con normativas que establecieran una clara regulación y sanción de estas conductas.

---

en la cual de desarrolla un Programa de Derecho, Tecnologías de la Información y Propiedad Intelectual, donde se abordan temas mencionados y relativos a derecho informático.

[88] El alcance es formulado por Pierre A. WEILL, en su trabajo intitulado *EME de la Législation et Tendances de la Jurisprudence relatives á la Protection des Données Personnelles en Droit Pénal Franois,* publicado en la *Revue I nternationale de Droit Comparé* (julio-septiembre, 1987), pp. 655 ss

Fruto de este esfuerzo mancomunado, se comenzó a observar el nacimiento en distintas partes del mundo de legislación referida a estos tópicos, incorporando las correspondientes figuras típicas introduciéndolas en el Ordenamiento Jurídico respectivo a través de la modificación del Código Penal o creando Leyes Penales Especiales. En este sentido particular trascendencia tendrían en su oportunidad las normativas de Estados Unidos contenidas en la Federal Computer Crime Act (1984) y la Computer Fraud and Abuse Act (1986), y la correspondiente a Gran Bretaña conocida como Computer Misuse Act (1990).

La legislación norteamericana contemplaba expresamente los siguientes comportamientos:

- abuso que afecte a cuestiones de seguridad nacional,
- utilización no autorizada de los sistemas informáticos del Gobierno,
- abuso informático sobre instituciones financieras,
- acceso informático con intención de defraudar, mediante el cual se obtenga cualquier cosa de valor (que no sea el uso del computador),
- acceso que se realice con la intención de alterar, dañar o destruir información contenida en un sistema de información, o para impedir su uso por quien está autorizado para ello, y
- traficar con cualquier código secreto o información similar que afecte al comercio interestatal o a los computadores del Gobierno Federal.

En esta legislación se contemplaban sanciones de multa hasta los US$ 250.000, penas privativas o restrictivas de libertad de hasta 5 años y decomiso del material utilizado en la comisión del delito.

Por su parte, la Ley de Gran Bretaña sancionaba cualquier intento, con éxito o no, de alterar datos informáticos con intención criminal. Estas actuaciones podrían ser penalizadas con hasta 5 años de cárcel, multas y decomiso.

2) Delito Informático en la doctrina

Existen diferentes términos para definir este tipo de delitos entre los que podemos destacar y diferenciar, entre la opinión de los autores y de instituciones jurídicas:

- **LOS AUTORES**

a) Delincuencia informática

La define Gómez Perals[89] como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

b) Criminalidad informática

Alestuey[90] prefiere hablar de "delincuencia o criminalidad informática".

Baón Ramirez[91] define la criminalidad informática como la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).

Tiedemann[92] considera que con la expresión "criminalidad mediante computadoras", se alude a todos los actos, antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos.

c) Delitos informáticos

Romeo Casabona[93] se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual Delito Informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución.

Para Davara Rodriguez[94] define el Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada

---

[89] **GÓMEZ PERALS, Miguel.** *"Los Delitos Informáticos en el Derecho Español"*, Informática y Derecho nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi, págs. 481 a 496.

[90] **ALESTUEY DOBÓN, María del Carmen.** *"Apuntes sobre la perspectiva criminológica de los delitos informáticos"*, Informática y Derecho nº 4, UNED, Centro Regional de Extremadura, III Congreso Iberoamericano de Informática y Derecho 21-25 septiembre 1992, Mérida, 1994, Editorial Aranzadi, págs. 453 a 463.

[91] **BAÓN RAMÍREZ, Rogelio.** *"Visión general de la informática en el nuevo Código Penal"*, en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, 1996, págs. 77 a 100.

[92] **TIEDEMANN, Klauss.** *"Poder económico y delito"*, Barcelona, 1985.

[93] **ROMEO CASABONA, Carlos María.** "Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la información" ,FUNDESCO, Colección impactos, Madrid, 1987, págs. 25 a 34

[94] DAVARA RODRÍGUEZ, Miguel Ángel. *"Manual de Derecho Informático"*, Editorial Aranzadi, Pamplona, 1997, págs. 285 a 326.

a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.
Determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo con los ordenadores.
Parker define los delitos informáticos como todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio.

d) Computer crimen
En el ámbito anglosajón se ha popularizado la denominación de "*Computer Crime"* y en el germano la expresión "*Computerkriminalität"*

e) Delincuencia de cuello blanco
La doctrina, casi unánimemente, la considera inscribible en la criminalidad "de cuello blanco" y es la violación de la ley penal por una persona de alto nivel socio-económico en el desarrollo de su actividad profesional.

f) Abuso informático
es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos.

- Clasificación

En todo delito de los llamados informáticos, hay que distinguir el medio y el fin. Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad de la informática y la telemática, y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito; una finalidad deseada que causa un perjuicio a otro, o a un tercero.

Según BARRIUSO RUIZ[95] los podemos clasificar en :

[95] BARRIUSO RUIZ, Carlos. *"Interacción del Derecho y la informática"*, Dykinson, Madrid, 1996, págs. 245 a 252.

1. Delitos contra la intimidad
1. De los robos
1. De las estafas
1. De las defraudaciones
1. De los daños
1. Relativo a la protección de la propiedad industrial
1. Relativos al mercado y a los consumidores

De acuerdo con Pérez Luño[96] podemos hacer la siguiente clasificación:

a) Desde el punto de vista subjetivo

Ponen el énfasis en la pretendida peculiaridad de los delincuentes que realizan estos supuestos de criminalidad

b) Desde el punto de vista objetivo

Considerando los daños económicos perpetrados por las conductas criminalistas sobre los bienes informáticos:

- Los fraudes

Manipulaciones contra los sistemas de procesamiento de datos. Podemos citar:

- los daños engañosos (*Data diddling)*
- los "Caballos de Troya" *(Troya Horses)*
- la técnica del salami *(Salami Technique/Rounching Down)*

- El sabotaje informático:

- bombas lógicas *(Logic Bombs)*
- Virus informáticos

- El espionaje informático y el robo o hurto de software:

- Fuga de datos *(Data Leakage)*

- El robo de servicios:

- Hurto del tiempo del ordenador.
- Apropiación de informaciones residuales *(Scavenging)*
- Parasitismo informático *(Piggybacking)*
- Suplantación de personalidad *(impersonation)*

- El acceso no autorizado a servicios informáticos:

[96] PÉREZ LUÑO, Antonio-Enrique. "*Ensayos de informática jurídica*", Biblioteca de Ética, Filosofía del Derecho y Política, México, 1996, págs. 17 a 23

- Las puertas falsas *(Trap Doors)*
- La llave maestra *(Superzapping)*
- Pinchado de líneas *(Wiretapping)*

c) Funcionales

La insuficiencia de los planteamientos subjetivos y objetivos han aconsejado primar otros aspectos que puedan resultar más decisivos para delimitar la criminalidad informática.

Atentados contra la fase de entrada *(input)* o de salida *(output)* del sistema, a su programación, elaboración, procesamiento de datos y comunicación telemática.

Para Jover Padró[97] se entendían comprendidos dentro de los delitos informáticos:

a) El fraude informático, ilícitos patrimoniales que Jurisprudencia y Doctrina han calificado como hurto, apropiación indebida o estafa.

b) Los documentos informáticos y sus falsedades.

c) Del sabotaje informático, tipificado como delito de daños y estragos.

d) Los ataques contra la intimidad de las personas.

e) Las defraudaciones a la propiedad intelectual.

f) Las faltas informáticas.

Para Baón Ramirez dentro de la criminalidad informática podemos distinguir dos grandes grupos de delitos:

- Un primer grupo se refiere a los delitos que recaen sobre objetivos pertenecientes al mundo de la informática. Así distinguiremos los delitos:

- relativos a la destrucción o sustracción de programas o de material,
- relativos a la alteración, destrucción o reproducción de datos almacenados,
- los que se refieren a la utilización indebida de ordenadores,

- En un segundo grupo se encuadraría la comisión de los delitos más tradicionales como los delitos contra:

[97] JOVER PADRÓ, Josep. *"El Código Penal de la informática"*, X Años de Encuentros sobre Informática y Derecho 1996-1997, Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE), Aranzadi Editorial, Pamplona, 1997, págs. 349 a 370

- la intimidad,
- la propiedad,
- la propiedad industrial o intelectual,
- la fe pública,
- el buen funcionamiento de la Administración,
- la seguridad exterior e interior del Estado.

Romeo Casabona analiza las distintas facetas de lo que llama "las repercusiones de las Nuevas Tecnologías de la Información en el Derecho Penal", y de esta forma, divide su análisis en diferentes apartados bajo los títulos de:
- La protección penal de la intimidad e informática,
- La informática como factor criminógeno en el tráfico económico,
- El fraude informático,
- Implicaciones penales de las manipulaciones en cajeros automáticos mediante tarjetas provistas de banda magnética,
- Agresiones a los sistemas o elementos informáticos.

Correa, siguiendo a Uhlrich, clasifica los delitos informáticos de la siguiente manera:
a) fraude por manipulaciones de un ordenador contra un sistema de procesamiento de datos,
b) espionaje informático y robo de software,
c) sabotaje informático,
d) robo de servicios,
e) acceso no autorizado a sistemas de procesamiento de datos,
f) ofensas tradicionales en los negocios asistidos por ordenador.

Tellez Valdés[98] clasifica estas acciones en atención a dos criterios:
1. Como instrumento o medios, categoría en la que encuadra a las conductas que él llama "criminógenas que se valen de los ordenadores como método, medio o símbolo en la comisión del ilícito",

[98] TELLEZ VALDÉS, Julio. *"Los Delitos informáticos. Situación en México"*, Informática y Derecho nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996, págs. 461 474.

2. Como fin u objetivo, encuadrando en esta categoría a las "conductas criminógenenas que van dirigidas en contra del ordenador, accesorios o programas como entidad física".

Sieber hace una clasificación que responde no sólo a un criterio sistematizador vinculado a las características del procesamiento automático de datos, sino al mismo tiempo a una separación de diversos tipos criminológicos de conducta. Las conductas más significativas desde esta perspectiva podrían agruparse en estas cinco modalidades principales:

a) manipulaciones de datos y/o programas, o "fraude informático",

b) copia ilegal de programas,

c) obtención y utilización ilícita de datos, o "espionaje informático",

d) destrucción o inutilización de datos y/o programas, o "daños o sabotaje informático" y

e) agresiones en el hardware o soporte material informático, principalmente "hurto de tiempo del ordenador".

Siguiendo a Davara Rodriguez dentro de un apartado en el que incluye "La informática como instrumento en la comisión de un delito", distingue dentro de la manipulación mediante la informática dos vertientes diferentes:

a) Acceso y manipulación de datos y

b) Manipulación de los programas.

Atendiendo a ello, considera que determinadas acciones que se podrían encuadrar dentro de lo que hemos llamado el delito informático, y que para su estudio, las clasifica, de acuerdo con el fin que persiguen, en seis apartados:

1. Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos,
1. Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello,
1. Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas,
1. Utilización del ordenador y/o los programas de otras persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro,
1. Utilización del ordenador con fines fraudulentos y
1. Agresión a la "privacidad" mediante la utilización y procesamiento de datos

personales con fin distinto al autorizado, que será objeto de éste trabajo.

Para Claudio Ossa Rojas, existen diversos grupos de sujetos activos, los que se delimitan de acuerdo a los medios y las formas utilizadas por estos para su ejecución. Así, podemos distinguir las siguientes conductas

1.- Phreaking.

Consiste en el acceso no autorizado a sistemas telefónicos para obtener gratuidad en el uso de las líneas, con el objeto de lograr conexión mantenida por esta vía a las redes informáticas, ya sean nacionales o internacionales.

Esta conducta, se relaciona con los delitos informáticos a través del ataque de los phreakers hacia sistemas de telefonía, los que si son considerados en su conjunto, pueden fácilmente llegar a comprometer la funcionalidad de los más grandes sistemas de telecomunicaciones coordinados a través de redes de ordenadores, los que, a través de la utilización de softwares especializados manejan las comunicaciones que se desarrollan por esta vía. Sin embargo, esta conducta no es nueva, ya que fue practicada desde los inicios de la telefonía, pero el ataque en ese entonces, apuntaba al quebrantamiento de sistemas de carácter analógico y no digital, y por consiguiente no podría relacionarse con delitos informáticos.

Dentro de las actuales manifestaciones de phreaking podríamos distinguir:

a) Shoulder-surfing: esta conducta se realiza por el agente mediante la observación del código secreto de acceso telefónico que pertenece a su potencial víctima, el cual lo obtiene al momento en que ella lo utiliza, sin que la víctima pueda percatarse de que está siendo observada por este sujeto quien, posteriormente, aprovechará esa información para beneficiarse con el uso del servicio telefónico ajeno.

b) Call-sell operations: el accionar del sujeto activo consiste en presentar un código identificador de usuario que no le pertenece y carga el costo de la llamada a la cuenta de la víctima. Esta acción aprovecha la especial vulnerabilidad de los teléfonos celulares y principalmente ha sido aprovechada a nivel internacional por los traficantes de drogas[99]

c) Diverting: consiste en la penetración ilícita a centrales telefónicas privadas, utilizando éstas para la realización de llamadas de larga distancia que se cargan posteriormente al dueño de la central a la que se ingresó clandestinamente. La conducta se realiza atacando a empresas que registren un alto volumen de tráfico de llamadas telefónicas,

[99] Falcon, Enrique.¿Qué es la Informática Jurídica?. Del Ábaco al Derecho Informático. Editorial Abeledo-Perrot. Bs. Aires, Argentina.1992.

con el fin de hacer más difícil su detección.

d) Acceso no autorizado a sistemas de correos de voz: el agente ataca por esta vía las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos destinados al conocimiento exclusivo de los usuarios suscriptores del servicio. A través de esta conducta el sujeto activo puede perseguir diversos objetivos:

d.1) Utilizar los códigos de transferencia de mensajería automática manejados por el sistema.

d.2) Lograr el conocimiento ilícito de la información recibida y grabada por el sistema.

e) Monitoreo pasivo: por medio de esta conducta el agente intercepta ondas radiales para tener acceso a información transmitida por las frecuencias utilizadas por los teléfonos inalámbricos y los celulares.

2.- Hacking.

Esta conducta se refiere al acceso no autorizado que realiza el sujeto activo a un sistema de información atentando contra el sistema de seguridad que este tenga establecido. La finalidad del actuar del agente (Hacker) puede ser diversa, ya que buscará a través de ella conocer, alterar o destruir la información contenida en el sistema ya sea parcial o totalmente.

Frente a este grupo de sujetos, la doctrina ha postulado dos posiciones:

- Posición mítica: considera a estos sujetos como individuos de corta edad, por lo general adolescentes de posición social media, aparentemente inofensivos, ausentes de toda conciencia de estar obrando mal, a menudo sugestionados por el síndrome de "*Robin Hood*" y con un coeficiente intelectual muy alto. Su personalidad presenta la característica particular de ser inestable. Su figura cobró importancia a raíz del intrusismo en sistemas de información que en un comienzo realizaron adolescentes norteamericanos y europeos, los que, en un afán lúdico ingresaban a sistemas de información para luego huir sin causar mayores daños. Lamentablemente, las conductas observadas por estos sujetos fueron convirtiéndose paulatinamente en actividades muy riesgosas, tanto para los sistemas como para la seguridad interna y externa de los países en que actuaban, ya que muchas veces sus jugarretas pusieron en graves aprietos a sistemas altamente sofisticados, produciendo efectos negativos en distintos lugares del planeta, debido a la posibilidad de desplazamiento con que contaban a través de las redes informáticas.

- Posición realista: incorpora a los sujetos considerados por la posición mítica, pero

agrega a otros sujetos que, si bien no poseen avanzados conocimientos tecnológicos relativos a la informática, pueden realizar conductas propias de la delincuencia informática. Esta apreciación vino a poner de manifiesto que, los casos más serios de delincuencia informática, podían ser llevados a cabo por sujetos que trabajan en el mundo de la informática, de edades superiores a los míticos hackers inicialmente descubiertos y que no presentan ni la mitad de inteligencia que se les atribuía a estos. Entre estos sujetos se ha incluido además a aquellos que no necesariamente desempeñan sus labores en entidades relacionadas con sistemas informáticos, pero que ingresan a ellos de un modo irregular.

El resultado de las consideraciones aportadas por quienes sustentan esta posición realista ha permitido la inclusión dentro de los hackers de los sujetos conocidos como insiders, que son aquellos individuos que acceden sin autorización a un sistema de información que les es muy cercano debido a una relación laboral, actual o reciente, que les ha permitido el conocimiento de las formas posibles para realizar los ataques que estimen convenientes logrando el ingreso libremente, con la finalidad de utilizar la información contenida por el sistema para fines propios.

3.- Trashing.

Esta conducta tiene la particularidad de haber sido considerada recientemente en relación a los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Estas acciones corresponden a una desviación del procedimiento conocido como reingeniería social.

Estas actividades pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada.

4.- Atentados contra la propiedad intelectual.

En una primera aproximación, se debe aclarar que bajo el concepto de propiedad intelectual se deben considerar dos aspectos que algunos ordenamientos jurídicos tratan en forma separada. El primero de ellos se regula bajo los conceptos que comprende la Propiedad Industrial, así estas actividades delictivas podrían afectar a la información relativa a la obtención de la protección de derechos de propiedad industrial (marcas,

patentes de invención o de procedimientos, diseños industriales y modelos de utilidad), a la manejada durante el correspondiente procedimiento de reconocimiento de estos derechos y a la que tenga relación con estos una vez adquiridos. El segundo aspecto, comprendido en estas conductas, se refiere al atentado en contra de los derechos autorales, tanto en sus aspectos morales, patrimoniales o mixtos.

- **INSTITUCIONES JURIDICAS**

- La Convención de Delitos Informáticos del Consejo de Europa de 2001, clasifica las conductas lesivas a la información en cuatro tipos:

a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.-
Sanciona el acceso y la intercepción ilegal, interferencia de datos y sistemas y el mal uso de dispositivos.
b) Delitos de fraude informático.- Falsificación y fraude computacional
c) Delitos por su contenido.- Producción diseminación y posesión de pornografía infantil.
d) Delitos relacionados con la infracción de la propiedad intelectual y derechos afines.-
La amplia gama de reproducciones ilícitas por medios informáticos de obras protegidas por el derecho de autor.

- La Unión Europea, en la Propuesta de Decisión-Marco del Consejo Relativa a los Ataques de los que son Objeto los Sistemas de Información, de agosto de 2002, identifica las siguientes amenazas:

a) Acceso no autorizado a sistemas de información, que incluye la "piratería" informática;
b) Perturbación de los sistemas de información, como la "denegación de servicio";
c) Ejecución de programas perjudiciales que modifican o destruyen datos, incluye virus, bombas lógicas y gusanos;
d) Interceptación de las comunicaciones, denominada intromisión (sniffing);
e) Declaraciones falsas, se trata de la usurpación de la identidad de una persona en Internet, se llama "spoofing" (modificación de datos).

- Las Naciones Unidas, reconoce los siguientes tipos de delitos informáticos.

1. Fraudes cometidos mediante manipulación de computadoras:
a) Manipulación de datos de entrada;
b) manipulación de programas;
c) manipulación de datos de salida;
d) fraude efectuado por manipulación informática.

2. Falsificaciones informáticas:
a) como objeto, se alteran datos de los documentos almacenados;
b) como instrumentos.

3. Daños o modificaciones de programas o datos computarizados:
a) Sabotaje informático;
b) virus;
c) gusanos:
d) bomba lógica o cronológica.

4. Falsificaciones informáticas:
a) Acceso no autorizado a sistemas o servicios;
b) piratas informáticos o hackers;
c) reproducción no autorizada de programas informáticos.

3) Protección penal de la privacidad y el delito informático

Las leyes de protección de datos personales amparan la privacidad. Y desde esta particular perspectiva, ¿qué principios deberían, en concreto, inspirarlas?

Entre nosotros, la formulación más clara ha sido elaborada por el profesor

Muñoz Navarro.[100] Siguiendo sus planteamientos, podemos consignar los siguientes:

a) Se hace necesario regular la recolección de datos nominativos, determinándose cuáles tienen el carácter de públicos (porque relacionan a la persona con el resto de los individuos o con el grupo social) y cuáles el de privados (ya que afectan a la persona en su relación consigo misma o con su núcleo básico).

b) Debe establecerse y garantizarse el derecho de toda persona natural o jurídica para utilizar esta herramienta que le provee la tecnología, por cierto con limitantes.

Estas últimas serían:

i) Que tratándose de datos nominativos, la actividad debe sujetarse a la ley, y

ii) Que debe establecerse algún tipo de procedimiento previo de autorización o registro en la constitución de archivos de datos de tal carácter. En vez de una libertad informática absoluta se está optando por el principio del control y registro, en cuya virtud es el Estado el que debe tener el derecho de autorizar los archivos que se creen y llevar la supervigilancia administrativa de los mismos.

c) En aras de garantizar la calidad y confiabilidad de los datos, la normativa debe consagrar el derecho de acceso de los sujetos de la información.

d) En cuanto al uso que pueda darse ala información nominativa, habrá que definir claramente el objeto de la recolección de datos y establecer —por ley o contractualmente— el uso que de ella pueda hacerse.

e) Para garantizar la seguridad de la información, habrá que adoptar tanto medidas técnicas como jurídicas de tutela. Las segundas se traducen en la creación de herramientas legales que impidan el acceso no autorizado a los sistemas y que, de producirse, lo sancionen.

f) Se hace preciso definir las responsabilidades de los administradores de la información por el manejo indebido de datos nominativos, como también las medidas que ellos deberán adoptar para obtener la seguridad del sistema.

g) Cuando la seguridad sea vulnerada por actos ilícitos, nacerá la obligación de reparar el daño para quien lo haya ocasionado dolosa o culpablemente. Así se estará respondiendo por perturbaciones a la intimidad causadas por indiscreción, impertinencia, codicia o insensatez. Para efectos del resarcimiento por la intromisión en la intimidad de una persona, se requiere que el hecho sea constitutivo de delito o

[100] MUÑOZ N., Patricio, *Bases para una Legislación Informática sobre la Privacidad de los Datos, en* revista *Trilogía Ciencia-Técnica-Espíritu,* publicada por el Instituto Profesional de Santiago 13 (1987) 7, pp. 56 ss

cuasidelito. Considera Muñoz Navarro[101] que «la configuración del delito informático como una figura punible distinta, es la única solución que permitirá resolver el problema desde el punto de vista del hecho ilícito».

En general, se denominan atentados contra la vida privada diversos supuestos en que la intimidad puede ser lesionada o desconocida. En caso de estar tipificados penalmente por la ley constituyen delitos criminalmente sancionados. No es difícil constatar que aquéllos son cuantitativamente cada vez más numerosos y cualitativamente cada vez más diversos.

En el ámbito del derecho penal reviste mayor importancia la construcción de una teoría jurídica de la intimidad, ya que el concepto material de todo bien jurídico tutelado desempeña el papel de límite del *ius puniendi,* esa facultad del Estado para definir cuáles merecen ser amparados y, en consecuencia, establecer las conductas que les son atentatorias.

La regulación y resguardo de la privacidad es un tema que deben asumir los penalistas, sobre todo frente a los nuevos ataques por medios informáticos, porque estamos convencidos de que la mejor y la principal respuesta es el tipo de tutela que brinda el Derecho Penal. Lo anterior es consecuencia lógica de concebirlo como el sector del ordenamiento jurídico cuya finalidad es la protección de los bienes vitales y fundamentales del individuo y de la sociedad toda, los que son elevados a la categoría de bienes jurídicos o intereses sociales más relevantes.

Es necesario también reconocer que el carácter fragmentario del derecho penal[102] (El profesor Novoa alude al carácter fragmentario del Derecho Penal calificando a éste como «un sistema discontinuo de ilicitudes», porque no se produce «un ilícito penal que sea un campo continuo comprensivo de todos los hechos punibles y susceptible de ser parcelado en los distintos delitos, sino que se presenta como un verdadero archipiélago de hechos punibles, constituido por multitud de islas —representativas de los hechos punibles—, cada una de las cuales está separada de las otras por un espacio que corresponde a hechos no punibles».) se hace especialmente patente en materia de protección de la privacidad, por la obligada selección de conductas a tipificar, de entre la amplia variedad de acciones atentatorias contra este bien jurídico.

Entendemos, pues, a la privacidad como el más relevante de los bienes jurídicos

[101] Muñoz Navarro, ob cit.
[102] NOVOA MONREAL, Eduardo, *Curso* de *Derecho Penal* (Santiago, 1966) 1, p. 28.

afectados por el delito informático y, en consecuencia, requiere de la tutela brindada por el derecho penal.

Por cierto que a esta especial protección debe recurrirse en última instancia, ante la propia naturaleza de las sanciones que articula, especialmente restrictivas de los derechos y libertades fundamentales. De aquí que se sostenga que el resguardo penal de la intimidad requiere además la institucionalización de mecanismos orientados a la protección extrapenal, por ejemplo administrativos, ya que sólo de cumplirse esta premisa político-criminal, la intervención penal en el terreno informático podrá ajustarse al principio de ultima ratio del ordenamiento punitivo.'" A no dudar, la existencia de una normativa que consagre mecanismos de tutela o de control administrativos permitirá que sólo sean sancionadas penalmente las infracciones más graves. En definitiva, permitirá respetar el carácter fragmentario que es inherente al Derecho Penal.

4) Delitos informáticos en la legislación chilena. Mención a la protección de la privacidad.

En Chile, con la entrada en vigencia de la ley N°19.223, Chile se convierte en país pionero en Latinoamérica en dictar una legislación especifica relativa a los Delitos Informáticos. La Ley N° 19.223 de fecha 7 de junio de 1993, que tipifica figuras penales relativas a la informática[103], tiene su origen en la moción presentada ante la Cámara de Diputados por el diputado señor José Antonio Viera-Gallo, con fecha 16 de julio de 1991. La Ley tiene como antecedente directo la legislación francesa, en particular la Ley N° 88-19, de 5 de enero de 1988, Relativa al Fraude Informático.

e trata de figuras pluriofensivas, que junto con proteger el bien jurídico mencionado en la historia de la Ley, esto es, "la calidad, pureza e idoneidad de la información en cuanto tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan", protegen otros bienes jurídicos como la propiedad, la privacidad y la confianza en el correcto funcionamiento de los sistemas y redes computacionales.

Son figuras dolosas en las cuales se exige además un elemento subjetivo

[103] El texto de la ley se encuentra en el anexo de la presente memoria.

adicional, como la comisión de las acciones "maliciosamente" (artículos 1°, 3° y 4°) o con "el ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma" (artículo 2°). En este sentido, creemos que la función del término "maliciosamente" consiste en dejar sin aplicación la presunción de dolo del artículo 1° inciso segundo[104] del Código Penal, ya que según la historia de la Ley serán reiteradas las situaciones en que, por ejemplo, se alteren los datos contenidos en un computador sin la intención de haber provocado ese resultado. Aún falta mucho camino por recorrer respecto a la cultura informática. Estos sistemas, a pesar de su gran capacidad y utilidad, siguen siendo sumamente sensibles. Basta un poco de café, humo de cigarrillo o fijador de pelo, para que éstos fallen. De hecho, la medida de seguridad básica consiste en la creación de las denominadas copias de seguridad, debido a la posibilidad de perder la información. Por su parte, "el ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma", exige para la perfección del tipo la concurrencia en el sujeto activo de un determinado motivo o ánimo que debe ir encaminado a apoderarse, usar o conocer información de la cual no tiene derecho a apoderarse, usar o conocer. En el ánimo del sujeto se encuentra el conocimiento de que la información de la cual desea apoderarse, usar o conocer está restringida para él.

Su artículo 1° inciso primero contempla la figura del denominado "sabotaje informático", esto es, la destrucción (deshacer o arruinar una cosa material) o inutilización (pérdida de utilidad o utilidad limitada para el fin que el sistema esta determinado, sin la destrucción del mismo) de un sistema de tratamiento de información (hardware y/o software) o sus partes o componentes, o el impedimento (imposibilidad total para que el sistema ejecute sus funciones propias), obstaculización (el sistema no puede cumplir su función de tratar la información, o si puede, que lo hace de manera dificultosa) o modificación (el sistema sigue funcionando y prestando utilidad, pero no funciona de la forma prevista por el titular del sistema, ni le da a éste la utilidad que había previsto) de su funcionamiento.

Como ejemplo, podríamos señalar la introducción de un virus computacional para que el sistema funcione más lento, o funcione imperfectamente, o que finalmente no pueda funcionar.

El inciso 2° del artículo 1° contempla una figura agravada. Si como

[104] Art. 1 inciso 2° Código Penal: "Las acciones u omisiones penadas por la ley se reputan siempre voluntarias, a no ser que conste lo contrario"

consecuencia de las acciones descritas en el inciso primero, se afectaren los datos contenidos en el sistema, la penalidad se agravará. El fundamento se encuentra en que es posible prever que si se realizan las acciones del inciso primero, producto de éstas los datos contenidos en el sistema pueden resultar alterados, dañados o destruidos.

El artículo 2° sanciona el denominado "espionaje informático", esto es, el interceptar (evitar que la información llegue a su destino), interferir (introducir en la recepción de una señal otra extraña y perturbadora) o acceder a un sistema de tratamiento de información con ánimo de apoderarse, usar o conocer indebidamente la información contenida en el mismo. Se incluye en este tipo la intercepción de datos en transmisión y la sustracción o copia de datos.

Recordemos que un sistema automatizado de tratamiento de la información es mucho más que un computador. Las líneas a través de las cuales se envía la información de computador a computador son, por ejemplo, integrantes del sistema. Por lo tanto las acciones pueden recaer tanto en los computadores como en las líneas a través de las cuales se envía una comunicación.

El artículo 3° sanciona el denominado delito de "alteración de datos", que consiste en alterar (introducción de datos erróneos, transformación y desfiguración de datos, y el suprimir datos correctos), dañar (borrado parcial de datos o oscurecimiento de datos) o destruir (borrado de datos, que los hace desaparecer de modo completo e irrecuperable) los datos contenidos en un sistema de tratamiento de información. La ley 19.223 distingue entre el delito de sabotaje informático y la alteración de datos. El sabotaje informático hace referencia a las acciones contra el sistema de tratamiento de información o contra su funcionamiento. En cambio, el delito de alteración de datos se refiere a las acciones contra los datos.

El artículo 4° sanciona la revelación o difusión de datos contenidos en un sistema de tratamiento de información. Cuando se ocupa el verbo revelar, el dato debe ser secreto. Si se ocupa el verbo difundir, no es necesario que el dato sea secreto, pero creemos que sólo deberían protegerse por este artículo aquellos datos que realmente sean de interés para el sujeto pasivo.

El inciso segundo del artículo 4° contempla una agravante de responsabilidad, cuando el que incurre en las acciones de revelación y difusión es el responsable del sistema de tratamiento de información. Este es el único caso en que la ley exige la concurrencia de un sujeto calificado.

Sin lugar a dudas el texto de la Ley N° 19.223 es actualmente insuficiente para

combatir la delincuencia informática en Chile. La Ley fue creada en 1993, año en que el fenómeno Internet aún no lograba desarrollarse en el país. Por lo cual, el legislador al momento de tipificar las conductas, no pudo dimensionar el cambio que produciría Internet en nuestra sociedad, y en el comportamiento de los delincuentes. A lo menos, creemos que debe estudiarse

i)la sanción de los delitos de fraude informático, acceso no autorizado, creación y distribución de virus o programas dañinos, y falsificación informática;

ii)la reformulación de los tipos de sabotaje informático, alteración de datos y apoderamiento de información; y

iii)la incorporación de conceptos esenciales para una correcta aplicación de la ley .

Junto con lo anterior, debe hacerse un esfuerzo para incorporar al país a las iniciativas internacionales que se están realizando con el objeto de sancionar la delincuencia informática de manera global, mediante la cooperación internacional de todos los países. Internet permite realizar un delito en Chile desde cualquier país del mundo. Es por ello, que la única forma de protegerse frente a delincuencia informática, es la cooperación internacional.

Debemos entender además, que todos estos delitos se relacionan en mayor o menor grado con la vulneración, directa o indirecta, del bien jurídico privacidad, al existir una manipulación de nuestros datos en forma ilícita y no permitida por la víctima.

- Fraude informático.

Dentro del fenómeno de la delincuencia informática, reviste particular importancia el denominado fraude informático, debido al creciente aumento de manipulaciones fraudulentas de elementos informáticos. La diversidad de modalidades de comportamientos constitutivos de fraude informático no tiene límites.

Esta figura vino a absorber todas aquellas conductas defraudatorias que, por tener incorporada la informática como herramienta de comisión, no podían ser subsumidas en el tipo clásico de la estafa del derecho comparado. Esta vinculación con la estafa desde sus inicios determinó además que el concepto, estructura y contenido del fraude informático fueran construidos a partir de los elementos del delito de estafa.

Las manipulaciones fraudulentas de elementos informáticos se dirigen a obtener un lucro en perjuicio económico de otro. En este sentido, el perjuicio económico debe

entenderse tanto en su carácter individual como macrosocial. Esto nos permite afirmar que las defraudaciones por medios informáticos lesionan algo más que el patrimonio, hay un interés social valioso y digno de protección, como lo es la confianza en el correcto funcionamiento de los sistemas automatizados de tratamiento de la información.

Mucho se ha discutido si las conductas sancionadas mediante el fraude informático pueden ser sancionadas al amparo del delito de estafa[105] tipificado en el Art. 468 de nuestro Código Penal. En este sentido, creemos que el delito de estafa de nuestro Código Penal presenta dificultades para comprender a aquellas conductas defraudatorias realizadas por medios informáticos, en sistemas de tratamiento automatizado de la información en que no intervienen personas en su control, e incluso en aquellos en que existe la presencia de personas, pero cuyas intervenciones están limitadas a accesos meramente mecánicos.

El delito de estafa presupone que una persona sea engañada, y que se la induzca como consecuencia de esa conducta a un error que la lleva a realizar un acto de disposición patrimonial lesivo, pero en las manipulaciones defraudatorias, este engaño no ocurre. No se puede engañar a una máquina (computador), el engaño supone una relación psicológica entre el agente y el sujeto engañado.

Es por lo anterior, que el fraude informático comprende todas las conductas de manipulaciones defraudatorias, abusos o interferencias en el funcionamiento de un sistema de tratamiento automatizado de datos, con la intención de obtener un provecho, para producir un perjuicio económico. Eso si, el fraude informático debe tener siempre las notas configuradoras de una defraudación. Defraudación entendida como la causación de un perjuicio económico, irrogado mediante un medio engañoso, fraudulento (que aquí es la manipulación de los elementos informáticos).

Cabe hacer presente, que durante el proceso de formación de la Ley N° 19.223, el Gobierno, presentó indicación al proyecto en cuanto a incorporar el fraude informático mediante el siguiente artículo: "Artículo 2°, Intercálese, a continuación del artículo 468 del Código Penal, el siguiente artículo 468 bis, nuevo: Art. 468 bis. Incurrirán asimismo en las penas establecidas en el artículo 467, los que, con ánimo de lucro, defraudasen a otro mediante una manipulación informática que interfiera en la

[105] Art. 468 Código Penal: "Incurrirá en las penas del artículo anterior el que defraudare a otro usando de nombre fingido, atribuyéndose poder, influencia o créditos supuestos, aparentando bienes, crédito, comisión, empresa o negocios imaginarios, o valiéndose de cualquier otro engaño semejante."

recepción, procesamiento o transmisión de datos, causando con ello un perjuicio económico".[106] Esta indicación junto con las demás propuestas por el Gobierno fueron rechazadas por la Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados.

Por todo lo anterior, es que creemos debe incorporarse a nuestra legislación el fraude informático, como una figura dolosa, en la cual se exija como elemento subjetivo del tipo el ánimo de lucro, y como elemento objetivo la obtención mediante una manipulación informática de una transferencia indebida de cualquier activo patrimonial en perjuicio de tercero.

Las manipulaciones informáticas pueden efectuarse sobre los datos (al momento de ser ingresados al sistema mediante el suministro de datos falsos, cuando salen del sistema o cuando son transmitidos a través de Internet y otras redes), o sobre el programa del sistema (en este caso los datos suministrados no son falsos pero se manipula el programa para que el procesamiento de los datos conduzca a resultados falsos).

Es así como estaríamos frente a casos de manipulaciones informáticas, por ejemplo, en la utilización de datos en forma incorrecta o de una manera incompleta, o bien al utilizarlos sin estar autorizado, no olvidando en todo caso que estas manipulaciones deben ser fraudulentas, es decir, no basta con la sola manipulación de elementos informáticos, sino que es necesario que concurran las notas configuradoras de una defraudación (causación de un perjuicio económico, por un medio astuto, engañoso). Ejemplo de la utilización de datos incorrectos podemos observar en el caso del uso fraudulento de tarjetas falsificadas u otros instrumentos (como detectores de clave) para obtener dinero metálico de un cajero automático. En cuanto a la utilización de datos no autorizados, sería el caso, por ejemplo, de aquel sujeto que ocupe en forma fraudulenta una tarjeta u otro instrumento destinado a la obtención de dinero de un cajero automático, sin ser su titular (la tarjeta no ha sido falsificada en este supuesto, sino que ésta no estaría siendo utilizada por su verdadero titular). Como otros ejemplos de manipulaciones informáticas, podemos citar el caso de aquel empleado de una entidad bancaria que seleccione cuentas de ahorro que no hayan registrado movimiento alguno durante un largo periodo de tiempo, y transfiera sus fondos a otras cuentas abiertas por él, o bien el caso de aquel empleado de una empresa que con la ayuda de un

[106] BOLETÍN OFICIAL N°412-07, de la Honorable Cámara de Diputados y Senado de la República de Chile, p. 1972.

programa especialmente elaborado logre intercalar en la base de datos de los sueldos de la empresa, los datos de sueldos de personas ficticias, e indica su propia cuenta para que le depositen los sueldos de dichas personas. La manipulación informática sería el equivalente al engaño y al error del delito de estafa.

La transferencia del activo patrimonial se produce como consecuencia de las manipulaciones informáticas fraudulentas. Esta transferencia puede producirse directamente a través de las manipulaciones de los elementos informáticos, o bien puede obtenerse a través de un tercero en el caso que no concurran en éste los elementos constitutivos de la estafa, como lo son el engaño, en cuanto relación directa entre dos seres humanos, o un error psicológico en una persona). El agente de la acción accede a una transferencia de un activo, al cual no tiene derecho, y la expresión cualquier activo tiene por finalidad no restringir el objeto transferido a una cosa corporal, incluyendo así tanto el dinero metálico, como el dinero contable o giral (el cual la opinión generalizada no constituye una cosa corporal). Finalmente, producto de la transferencia indebida de un activo patrimonial se produce el perjuicio de tercero, esto es, un desequilibrio patrimonial sin fundamento legal.

Día a día podemos observar como el comercio electrónico y las transacciones bancarias aumentan en Internet. Este tipo de operaciones vía computador, en que una persona puede realizar desde su hogar transacciones comerciales o movimientos bancarios, si bien forman parte de las estrategias de mejoramiento de servicio al cliente, pueden constituir a su vez focos de criminalidad, específicamente de manipulaciones informáticas fraudulentas. Estos supuestos en los cuales no concurre la existencia de una persona engañada, que sufra un error psicológico y que como consecuencia de ello realice la disposición patrimonial (elementos exigidos por el tipo de estafa del Código Penal), en virtud de esta norma que proponemos quedarían cubiertos, y por lo tanto podrían ser sancionados.

- Acceso no autorizado.

El artículo N° 2 de la Ley N° 19.223 tipifica el acceso a un sistema de tratamiento de la información, pero tal como lo vimos en el numeral 3 anterior de este artículo, se exige la concurrencia de un elemento subjetivo como lo es “el ánimo de apoderarse, usar o conocer indebidamente la información.”

Sin perjuicio de lo anterior, la figura de acceder sin autorización a un sistema de

tratamiento de información, constituye delito individualmente considerada, en muchas legislaciones. En este sentido, creemos que junto a las conductas sancionadas por el artículo N° 2 de la Ley N° 19.223, se debe tipificar la figura de acceso no autorizado sin la concurrencia de un elemento subjetivo. Debe bastar con el acceso sin autorización o sin derecho a un sistema de tratamiento de información, concepto que comprende a los sitios web en Internet.

Esta acción de acceder a un sistema, mediante la violación de las medidas seguridad, por más mínimas que sean, evidentemente significa una puesta en peligro del bien jurídico protegido, ya sea éste la calidad, pureza e idoneidad de la información, la propiedad o la privacidad. Nadie tiene que estar tratando de superar las medidas de seguridad de un sistema de tratamiento de información o un sitio web. Para que el tipo se perfeccione, no se debe exigir ningún ánimo del agente, bastando el acceso al sistema al cual el sujeto activo no tiene derecho a acceder o la realización de actos tendientes a acceder a un sistema.

Esta figura de acceso no autorizado o indebido a un sistema de tratamiento de información formaba parte del proyecto original chileno sobre "Delitos Informáticos", que presentó el diputado señor José Antonio Viera-Gallo a la Cámara de Diputados, en la sesión 19ª, de fecha 16 de julio de 1991. En el proyecto original el artículo 2° señalaba: "el que sin derecho intercepte, interfiera, o acceda a un sistema automatizado de tratamiento de información será castigado con presidio menor en su grado medio."

Desafortunadamente, durante los trámites constitucionales posteriores a que dio lugar la Ley N° 19.223, el legislador fue desnaturalizando esta figura hasta el punto de hacerla desaparecer del texto legal. La situación no deja de ser grave. En el delito de violación de correspondencia, artículo 146 del Código Penal[107] se sanciona, como primera acción "el abrir", no exigiendo ningún elemento subjetivo, sin perjuicio de sancionar con una mayor penalidad a quien divulgare o se aprovechare de los secretos que la correspondencia o los papeles de otro contienen. Se sanciona la conducta de abrir porque ya existe una lesión al bien jurídico protegido a través de su modalidad de puesta en peligro. No se exige que se tome conocimiento del contenido de la correspondencia ni que divulgue su contenido.

Una vez que un sujeto se encuentra en conocimiento por medios ilícitos de las

[107] Art. 146 inciso 1° Código Penal: "El que abriere o registrare la correspondencia o los papeles de otro sin su voluntad, sufrirá la pena de reclusión menor en su grado medio si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en su grado mínimo.

claves secretas para ingresar a un sistema de tratamiento de información, éstas, pueden llegar a las manos de un delincuente. Por todo lo anterior, para nosotros el verbo "acceder" significa penetrar o ingresar a un sistema de tratamiento de la información, permaneciendo o no en él. Bastaría el hecho de entrar en un sistema por un segundo, luego de descifrada la clave de acceso o de violentada sus medidas de seguridad, para que el verbo acceder esté satisfecho.

Esta acción es equivalente a copiar la llave de un escritorio o de una casa, abrir el cajón o la puerta, probar que se tiene la capacidad de abrir y luego cerrar y marcharse, llevándose la llave. Esta es una acción potencialmente delictiva, que debe ser penalizada, lógicamente con una pena menor.

Parte de la doctrina y derecho comparado exigen en el tipo que el sistema se encuentre protegido contra accesos no autorizados, por que ello sería prueba de que la información que se protege es valiosa. No estamos de acuerdo con la inclusión de ese elemento, ya que con el mismo, la protección penal se estaría haciendo aplicable sólo a aquellos que pueden costear medidas de seguridad. Junto con lo anterior, parece ser que existe la creencia que cuando un sitio web es objeto de un acceso no autorizado, son los responsables del sitio los culpables por no haber adoptado las medidas de seguridad adecuadas. A menudo escuchamos las declaraciones de jóvenes que han accedido "ilegalmente" a sitios, que justifican su actividad en que el sitio correspondiente no tenía medidas de seguridad. Con esto, finalmente el sitio que ha sido objeto de un acceso no autorizado termina siendo criticado públicamente, cuando ha sido el objeto de una acción ilícita.

Los accesos no autorizados son una realidad, desconocerlos sólo hará más fácil la labor de los delincuentes. Las empresas no deben tener temor a denunciar que han sido objeto de accesos no autorizados por perdida de la imagen corporativa.

La autoprotección es importante, pero no todos las empresas pueden destinar grandes cantidades de dinero para protegerse. Es la ley la que debe proteger a las personas.

- Creación y distribución de virus y programas dañinos.

El estudiante de la República de Filipinas creador del famoso virus denominado "I Love You", luego de ser investigado es dejado libre, ya que la creación de virus y programas dañinos para los sistemas informáticos no se encuentra penada en dicho país.

Poco tiempo más tarde, con el objeto de evitar la repetición de hechos como estos, se dicta en la República de Filipinas la ley N° 8.792, de fecha 14 de junio de 2000, que regula la validez y uso de transacciones y documentos electrónicos comerciales y no comerciales, y las penas por sus usos ilegales. La Parte V y final de dicho texto legal sanciona en la sección 33 la introducción de virus computacionales y otros, que provoquen la destrucción, alteración, robo o pérdida de mensajes de datos electrónicos o documentos electrónicos con pena privativa de libertad y multa

En México, el creador y distribuidor del virus W32/SirCam (hola cómo estás? Te mando este archivo para que me des tu punto de vista) no podría ser demandado por la figura de creación y distribución de virus por no encontrarse tipificada. Sin perjuicio de lo anterior, a contar de 1999 existen en el Código Penal Federal mexicano disposiciones que sancionan la modificación, destrucción o la provocación de pérdida de información contenida en sistemas o equipos informáticos con pena privativa de libertad de hasta 2 años, tipo que podría ser aplicado. Sin perjuicio de lo anterior, no parece lógico que una persona creadora de un virus que causa millones de dólares en pérdidas sea procesada por el delito de alteración de datos o sabotaje informático, y no por una figura que sancione conductas que pueden tener repercusiones mundiales.
Países como Canadá y los Estados Unidos de América ya han tipificado las figuras de creación y distribución virus.

Perseguir a esta clase de conductas se hace sumamente complicado si esto se hace a través de los tradicionales tipos de sabotaje informático y alteración de datos. En muchas ocasiones, el virus no viene directamente del delincuente, sino que por el contrario viene del computador de alguien que conocemos, quien hasta desconoce que su computador ha sido infectado, y que él mismo está infectando otros sistemas de tratamiento de información. ¿A quién debemos culpar, al dueño del computador de donde se envió el virus o al creador del mismo? ¿y qué sucede cuando el creador del virus no se encuentra en la jurisdicción donde se cometió el daño? ¿y si esa conducta no se encuentra penalizada en el lugar donde se creó el virus?

Los autores de los variados y originales virus[108] a los cuales nuestros computadores se ven expuestos cada día, con los perjuicios que eso significa a nivel individual como global, deben ser sancionados. El peligro y daño de dichas conductas son demasiado grave para permitir la evasión de la pena.

[108] Jerusalem, Concept, Melissa, I Love You, W32/SirCam, W32/CodeRed, W32/Nimda@MM, etc

Por todo lo anterior, es que creemos que la sanción de la creación y distribución de programas destinados a dañar los sistemas de tratamiento de la información y las redes debe ser cubierta a través de un nuevo tipo, y no a través de las figuras de sabotaje informático y alteración de datos, las que no fueron creadas para reprimir esta nueva clase de conductas ilícitas, que producen daños a nivel mundial.

Sólo la tipificación de estas conductas por los ordenamientos penales de los países, permitirá hacer frente a la delincuencia informática desde una perspectiva global y mundial.

- Falsificación informática.

La Ley N°19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma, publicada en el Diario Oficial de fecha 12 de abril de 2002 viene a reconocer el denominado documento electrónico. De acuerdo a la ley, se entiende por documento electrónico: toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior. En este sentido, no cabe duda que el uso del documento electrónico en el tráfico comercial y jurídico logrará un gran desarrollo.

Si bien, la ley regula los efectos procesales del documento electrónico, creemos que a fin de precaver la falsificación de los mismos, y la sanción de dicha conducta, es que debe incorporarse el delito de falsificación informática a nuestra ley.

Muchos podrán creer que a través de una interpretación extensiva de la ley es posible sancionar la falsificación informática a través de los artículos 193 a 198 de nuestro Código Penal, pero dicho ejercicio no es propio en materia penal, donde debe primar una interpretación restrictiva. El legislador de nuestro Código Penal jamas tuvo en mente sancionar la falsificación de un documento electrónico, lo que al momento de aplicar la pena, podría inhibir a nuestros tribunales de aplicar el tipo clásico de falsificación a los documentos electrónicos.

Por todo lo anterior, es que recomendamos la creación del tipo de falsificación de documento electrónico, a fin de mantener el principio de tipicidad y legalidad en materia penal.

- Reformulación de los tipos de sabotaje informático, alteración de datos y

apoderamiento de información.

Como pilares de un legislación sancionadora de la delincuencia informática, recomendamos efectuar cambios menores en los tipos de sabotaje informático (art. 1° Ley N°19.223), alteración de datos (art. 3° Ley N°19.223) y apoderamiento de información (art. 2° Ley 19.223), principalmente debido a los cambios en la ley que produciría la tipificación del acceso indebido.

En este sentido, se recomienda eliminar el ánimo del tipo de apoderamiento de datos a fin de facilitar la prueba de su comisión, y complementar el tipo de alteración de datos incorporando el verbo rector "interceptar", a fin de sancionar también la alteración de datos que se encuentran en proceso de transmisión.

La comisión de las conductas anteriormente sancionadas sin dolo sería sancionada como una figura agravada del acceso indebido. De esta manera, aquel que ejecute actos tendientes a acceder a un sistema informático o acceda al mismo sin estar autorizado, debe responder por las consecuencias que su actuar antijurídico produzca.

- La incorporación de conceptos esenciales para una correcta aplicación de la ley .

Se recomienda reemplazar "sistema de tratamiento de información" por "sistema informático", definiendo dicho concepto en la ley a fin de volver a la idea original de esta ley, en el sentido de proteger objetos que por su naturaleza no se encontraban protegidos por la normativa clásica. Podrá discutirse si es propio de una legislación sobre delincuencia informática sancionar junto con el software el harware, pero jamas se podrá pretender como consta en la historia de la Ley N°19.223, que a través de una ley de delitos informáticos se sancionen las acciones sobre registros manuales o sistemas manuales de tratamiento de la información.[109]

Se recomienda incorporar el concepto de documento electrónico que contiene La Ley N°19.799 Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma, en su artículo 2°.- Letra d), a fin de facilitar la sanción de la falsificación informática.

[109] Para una mayor profundización sobre esta materia, se recomienda ver "Delincuencia y Fraude Informático Derecho Comparado y Ley N°19.223", Editorial Jurídica de Chile, 1999, pág. 139.

5) Análisis de una jurisprudencia chilena relativa al delito informático.

Entre los días 28 de diciembre de 2001 y 8 de enero de 2002, un ex empleado de la empresa ATI Chile, realizó diversas intromisiones ilegales al servidor de ésta, alterando, dañando y conociendo indebidamente información contenida en éste. Los sitios Web afectados fueron: www.guestbook.cl y www.metabuscador.cl

El imputado era un joven de 19 años, conocido en el Chat IRC con el seudónimo «P0key», el cual habría actuado por «venganza» en contra de la empresa, pues había sido despedido de ésta.

El «cracker»[110] al ingresar ilegalmente a estos sitios, alteró el contenido de éstos, creando una nueva página Web (index.html) en reemplazo de la existente, que mostraba mensajes ofensivos[111] hacia la empresa e indicaba que el sitio había sido hackeado.

El administrador del sistema informático procedió a efectuar una inmediata auditoría de todos los archivos «LOG» del servidor y pudo comprobar que dichos sitios habían sido víctima de una serie de ataques e intromisiones, además, la eliminación de algunos archivos de auditoría de transacciones de cuentas de FTP, para borrar rastros desde dónde se efectuaban los ataques. Incluso, mientras se realizaban las auditorías, se pudo comprobar que el «cracker» intentaba ingresar al correo electrónico del gerente general de la empresa, hecho que pudo ser controlado a tiempo.

Se pudo comprobar que el 90% de los ataques provenía desde una IP fija, que correspondía a un Ciber Café en el cual el imputado trabajaba como administrador. El resto de los ataques provenía desde cuentas conmutadas de acceso a Internet, fundamentalmente desde el domicilio del imputado.

Una vez iniciada la investigación y presentada la querella criminal por delitos informáticos, el caso tomó especial importancia en la prensa de la ciudad de Talca y entre los usuarios del Chat IRC. Aprovechando este momento, el imputado concurrió en forma voluntaria al diario El Centro de Talca y entregó una entrevista, siendo portada, bajo el título: «Yo soy el ciber pirata». De esta manera lograba la fama y reconocimiento por sus pares, hecho buscado comúnmente entre los «crackers». Incluso

[110] Persona que «quiebra» un sistema de seguridad informática.
[111] «Sí, soy un criminal …, mi crimen es ser mejor que todos ustedes, algo que jamás me perdonarán …».

ofrecía sus servicios para reparar las fallas de seguridad del sistema.

- Juicio Abreviado

El día fijado para la audiencia de preparación del juicio oral, los intervinientes: Ministerio Público, Defensor Penal Público y Querellante, acordaron proceder conforme al Procedimiento Abreviado[112]. Para ello el querellante tuvo que desistirse de otros dos delitos a fin de cumplir con los requisitos establecidos en el Código Procesal Penal. Una vez realizadas las preguntas de rigor al acusado, la Juez de Garantía señora Marta Asiaín Madariaga, autoriza la realización del juicio abreviado y da la palabra al fiscal para que exponga el caso.

El fiscal jefe de la ciudad de Talca don Carlos Olivos Muñoz, realizó una clara exposición respecto de los hechos, la investigación realizada, todos los medios de prueba reunidos durante ocho meses de investigación y solicitó la aplicación de una pena de 3 años y un día de presidio, por tres delitos informáticos: artículos 1, 2 y 3 de la Ley 19.223.

El querellante, abogado Alberto Contreras Clunes, ratifica todo lo señalado por el fiscal y recalca la gravedad de los delitos imputados, los perjuicios ocasionados a la empresa y el actuar malicioso del acusado. También resalta el hecho que el acusado confiesa su participación en su declaración policial y el jactarse de ello en la entrevista del diario El Centro.

Importante resulta la inclusión de un peritaje informático realizado por la Brigada del Ciber Crimen de la Policía de Investigaciones de Chile. En efecto, se realizó un peritaje a la computadora que ocupaba el acusado en el Ciber Café, como a su computadora personal. Por medio de un sofisticado programa, inaugurado en esta ocasión, se logra recuperar diversos archivos borrados del disco duro de la CPU del Ciber Café. Merece especial atención uno, consistente en un correo electrónico enviado por el acusado a su pareja en el cual le cuenta: «estoy borrando unas («weas») que me pueden comprometer en los asuntos judiciales …», enviado precisamente en la tarde del día anterior al que prestó declaración policial.

En sus conclusiones el peritaje señala que: «El computador en cuestión cuenta con las capacidades técnicas necesarias y los programas adecuados tanto para navegar

[112] Artículo 406 del Código Procesal Penal.

por Internet como para efectuar daños a sistemas informáticos». En efecto, se pudo determinar que el disco duro contenía 24 programas: «… de uso frecuente por los Hackers, Crackers o Criminales Informáticos».

Finaliza el querellante señalando la importancia que tiene la informática en la actualidad, las potenciales víctimas de este tipo de delitos y los graves perjuicios que se causan a las empresas, pudiendo éstas llegar a quebrar económicamente por el desprestigio que estos delitos le provocan, solicitando la imposición de una pena de cinco años de presidio, en atención a tratarse de reiteración de delitos, contemplados en los artículos 1, 2 y 3 de la Ley 19.223.

Por su parte el defensor penal público don Joaquín Lagos León, alegó indicando que no se encontraba acreditada la participación de su defendido en los hechos, negándole valor a la declaración policial.

Introdujo una novedosa jurisprudencia del derecho norte americano, en la cual se penaliza a las empresas que ofrecen servicios de seguridad informática y son víctimas de «hackers», puesto que no dan cumplimiento a los servicios ofrecidos[113].

Trata en detalle las circunstancias personales del acusado, indicando que se trata de un joven autodidacta en computación, de esfuerzo, padre de familia, casado. Solicita la absolución de su representado y en caso de condena, se aplique el mínimo de la escala, esto es, la pena de 541 días de presidio, con el beneficio de libertad vigilada, al no registrar antecedentes penales.

- El Fallo

Al finalizar la audiencia, la Juez de Garantía dicta su veredicto: Culpable por los delitos N°1, 2 y 3 de la Ley 19.223, fijando la fecha de la lectura del fallo para el día 11 de abril de 2003.

El fallo consta de 13 fojas en las que pormenorizadamente se analizan todos los medios de prueba, describiendo en forma precisa el actuar delictivo y la forma en que éste se encontraba acreditado.

Al fijar la pena, la Juez advierte que tratándose de reiteración de delitos resulta más beneficioso aplicar una pena única conforme al artículo 351 del Código Procesal Penal. Señala también que lo dispuesto en el inciso cuarto de dicho artículo, es: «una

[113] La empresa víctima se dedica sólo a «Web hosting», es decir, alberga páginas Web, las diseña y mantiene

facultad para el Tribunal» en consideración a que el querellante solicitó una pena superior a la del fiscal.

Por otra parte, afirma que: «la entidad de las atenuantes[114] no nos convence, teniendo presente que según quedó establecido se trata de delitos reiterados, por lo que la pena que se impondrá en el grado señalado se considera más condigna con el actuar ilícito del acusado».

En atención a ello aplica la pena de tres años y un día de presidio, que es el mínimo de la escala penal de presidio menor en su grado máximo.

- Comentarios de Juriprudencia

Tratar los Delitos Informáticos es en sí un tema complejo. Sin embargo, la claridad del fallo nos deja plenamente satisfechos que se ha comprendido en toda su dimensión el tipo penal y las consecuencias que de él derivan.

Siendo muchas veces la prueba pericial esencial en el esclarecimiento de los hechos y la participación del autor de estos ilícitos, ella fue cabalmente comprendida y acreditó, más allá de toda duda razonable, la participación culpable del acusado.

La oportuna incautación de la CPU del acusado y del servidor del Ciber Café, además, del análisis exhaustivo dichos equipos; logró precisar con fecha, hora, minuto y segundo cuando se cometieron los ataques, como también el lugar de origen de éstos y el usuario que los realizó.

La oportuna detección de los ataques y las rigurosas medidas de seguridad aplicadas por la empresa, evitaron que los daños y perjuicios fuesen mayores.

La adecuada colaboración entre el fiscal jefe del Misterio Público de la ciudad de Talca señor Carlos Olivos con el abogado querellante y la víctima, lograron diseñar una investigación que a lo largo de ocho meses obtuvo abundantes medios probatorios que incriminaron al imputado.

Siendo éste el primer caso sobre Delito Informático dentro de la reforma procesal penal y la meridiana claridad de los fundamentos en la sentencia condenatoria, se convertirá necesariamente en un obligado precedente.

Es necesario destacar que, más allá del éxito en la resolución del caso, existió una empresa que se atrevió a denunciar el delito, con todas las consecuencias que trajo

[114] Artículo 11 Nº6 y Nº9 del Código Pena

para con sus clientes y prestigio, algo que por lo general no hacen las víctimas de estos delitos.

Como conclusión final simplemente cabe señalar que en la actualidad existe suficiente tecnología para investigar este tipo de delitos y, mejor aún, es posible sancionar a los autores de éstos, erróneamente denominados «hackers», siendo en rigor, simples delincuentes informáticos.

Por último, y en lo relativo a la privacidad, podemos mencionar que no se aplicó la ley 19.628 sobre Protección de la vida privada, pues aunque hay un acceso a información sensible, existiendo una base de datos y coincidiendo con una protección legal, no se aplica esta ley a personas jurídicas, como es en este caso.

6) Privacidad y tutela penal en la legislación extranjera

A continuación veremos algunas normas del derecho comparado que dicen relación a los delitos informáticos específicamente con el derecho y protección de la privacidad

1) España:

Se ha tratado de defender la intimidad como un valor en sí, es decir, con independencia de la finalidad perseguida por las conductas criminales.

Este derecho fundamental ha sido reconocido con carácter universal en el artículo 12 de la Declaración Universal de Derecho Humanos de las Naciones Unidas de 1948, en el artículo 8.1 de la Convención Europea para la protección de los Derechos Humanos y de las Libertades fundamentales de 195O, y en el artículo 17.1 del Pacto Internacional de Derecho Civiles y Políticos de 1966.

Su reconocimiento y garantía se lleva a cabo, en primer lugar, en la Constitución Española cuyo artículo 18.1 dispone que "se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

En el apartado 4 del artículo 18 se establece que "La ley limitará el uso de la informática

para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

El artículo 18 acoge un contenido amplio de intimidad. Junto a la declaración general de positivación del derecho a la intimidad, se reconoce el derecho a la intimidad domiciliaria y a la libertad y confidencialidad de comunicaciones privadas, para acabar con la constitucionalización del "habeas data" o faceta informática de la intimidad que la "privacy" adopta frente a los peligros de la informática. El artículo 18.4 CE. reconoce la dimensión positiva de la intimidad, convertida en "libertad informática", que básicamente constituye un derecho de control sobre los datos personales que circulan en la sociedad informatizada.

El mandato constitucional se cumplió mediante la promulgación de la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (B.O.E. nº 262, de 31 de octubre de 1992). Tuvieron gran importancia en el nacimiento de esta ley el Convenio 108 del Consejo de Europa de 1981, el Acuerdo de Schengen de 1985, sobre supresión gradual de los controles entre las fronteras comunes y la Propuesta de Directiva del Consejo de la Comunidad Económica Europea de 24 de septiembre de 1990, sobre protección de las personas en lo referente al tratamiento de los datos personales (modificada el 15 de octubre de 1992), que dio lugar a la Directiva 95/46/CE de 24 de octubre.

- DE LOS ATAQUES CONTRA EL DERECHO A LA INTIMIDAD

En estos ataques, la informática es un medio idóneo de comisión de estos delitos de descubrimiento y revelación de secretos y otras agresiones a la intimidad. Los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio se encuentran tipificados en el Capítulo I del Título X del CP.

- LA TUTELA PENAL DE LAS COMUNICACIONES ELECTRÓNICAS Y TELECOMUNICACIONES EN EL ART. 197.1 CP.

DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS DOCUMENTALES

Se castiga en este artículo al " que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico, o cualquiera otros documentos o efectos personales"

Pena: Prisión de uno a cuatro años y multa de doce a veinticuatro meses.

El tipo penal protege gran cantidad de soportes que contengan secretos de una persona.

El bien jurídico protegido no es el derecho de propiedad sobre el documento sino el secreto de la correspondencia, como atentado contra la intimidad de las personas.

Este delito consta de los siguientes elementos esenciales:

1º) Un hecho de apoderamiento -no de simple apertura- de los documentos.

2º) Que se realice con animo de descubrir o conocer los secretos de otro

3º) Que existan tales secretos. Por secreto hay que entender el hecho que sólo conoce una persona, o un círculo reducido de ellas, respecto al cual el afectado no desea, de acuerdo con sus intereses, que sea conocido por terceros.

4º) Que sean secretos de la persona a quien pertenezca la titularidad del documento.

5º) Que el apoderamiento además del móvil inicial de conocer los secretos de otro tenga el ulterior móvil de divulgación , aunque no es indispensable para la consumación del delito. El presente artículo no hace referencia a la divulgación que si recogían los artículos 497 y 497 bis del anterior CP.

El precepto amplía el secreto que antes era de "papeles o cartas y comunicaciones telefónicas" a "mensajes de correo electrónico" en clara referencia a la informática y "cualquier otro documento o efectos personales", expresión esta última que creemos configura el tipo de forma abierta y que permitirá entender tipificados otros soportes que se puedan llegar a crear en un futuro, sin tener que modificar el precepto penal por englobarlos.

Sujeto activo y pasivo puede ser cualquier persona, incluso los menores e incapaces pueden ser sujetos pasivos.

- SECRETO DE LAS TELECOMUNICACIONES

En el art. 18.3 de la Constitución "se garantiza el secreto de las comunicaciones y, especialmente...de las telefónicas, salvo resolución judicial".

Se castiga en el artículo 197.1 párrafo segundo, a quien intercepte a otro "sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación".

Pena: Prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Este precepto está en línea con los artículos 497 y 497 bis del anterior CP

(introducido por L.O. 7/1984, de 15 de octubre). Este artículo disponía de dos tipos de delitos: en primer lugar las interceptaciones de las comunicaciones en los términos descritos por el tipo penal. En segundo término, la revelación y divulgación de lo ilegalmente descubierto. La primera modalidad constituía el tipo básico y la segunda, el tipo cualificado del delito.

En relación al medio consistente en interceptar las comunicaciones telefónicas o utilizar instrumentos o artificios técnicos de escucha, transmisión, grabación o reproducción del sonido del anterior artículo 497, en el artículo 197.1 se incluye la imagen y cualquier otra señal de comunicación. La ampliación del objeto material del delito parece acertada, pues parece conveniente la inclusión de todos aquellos objetos en los que puede quedar plasmada o proyectada la intimidad del sujeto.

- LA TUTELA PENAL DE LOS DATOS PERSONALES. EL ART. 197.2 CP.

El artículo 197.2 supone una novedad "Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado". Iguales penas se impondrán a quien sin estar autorizados, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero".

Pena: Prisión de una a cuatro años y multa de doce a veinticuatro meses.

La penas previstas en este apartado son las mismas que las establecidas para el apoderamiento de documentos o efectos personales, lo cual merece la misma crítica que se hizo en el artículo 197.1 que debería haberse atendido a la insidiosidad de los medios para estratificar la gravedad de las penas.

En este precepto se convierten en delito actividades que antes sólo tenían sanción administrativa, al tipificar un elenco de conductas que implican abusos informáticos contra la "privacy" o libertad informática. Al marco legal extrapenal que informa y preside las conductas típicas del artículo 197.2 hicimos referencia en el apartado 3.1.

Todas las acciones típicas previstas en el artículo 1972. CP se producen sobre datos personales ya registrados en el fichero, por tanto las conductas de recogida ilícita

de datos personales con fines informáticos y la creación clandestina de ficheros o bancos de datos personales con fines de automatización deben encontrar respuesta sancionadora fuera del Derecho penal, como infracciones administrativas.

La referencia de "reservados" utilizado para calificar los datos de carácter personal no puede hacer referencia a los datos "sensibles", pues a ellos se refiere el artículo 197.5, por tanto carece de sentido este término utilizado en la redacción.

Se extiende el ámbito de incriminación de tipo a los datos personales que obren en registros o archivos públicos o privados de tipo convencional, es decir, no automatizados. El CP. va más allá de lo dispuesto en la La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de carácter personal (en adelante LORTAD), pero en sintonía con la Directiva 95/46/CE.

- TIPO AGRAVADO DE REVELACIÓN, DIFUSIÓN O CESIÓN DE DATOS. ART. 197.3 CP

Se castiga en el párrafo primero del artículo 197.3 a los que habiendo realizado alguna de las conductas previstas en los números 1 y 2 "difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas".
Pena: Prisión de dos a cinco años.

El fundamento del tipo agravado es el merecimiento de menoscabo a la intimidad que comporta la revelación, difusión o cesión de datos, hechos o imágenes.

Cuando opera la cláusula de los tipos agravados el delito contra la intimidad se comporta como un tipo penal compuesto (estructura típica doble) que requiere que, previamente se haya llevado a cabo el acto de intromisión ilícita en la intimidad ajena (tipo básico).

El hecho de divulgar o revelar lo descubierto ya se encontraba más penado en los artículos 497 y 497 bis del anterior CP.

Dispone el artículo 197.3, en su párrafo segundo :"el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizar la conducta descrita en el párrafo anterior"
Pena: Prisión de uno a tres años y multa de doce a veinticuatro meses.

Se contempla el supuesto en el que el sujeto lleva a cabo un acto de difusión, revelación o cesión de datos, hechos o imágenes, concernientes a la intimidad de otro, sin haber tomado parte en la conducta típica básica de acceso ilícito a la intimidad,

conforme a los apartados 1 y 2 del artículo 197. El tipo exige como elemento típico delimitador de la conducta incriminada que el sujeto tuviere conocimiento del origen ilícito de los datos.

Se trata de un delito de indiscreción, que presenta una autonomía con respecto a las restantes tipicidades presentes en el Título X del CP.

- TIPO AGRAVADO DE DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS POR PERSONAS ENCARGADAS O RESPONSABLES DE SU CUSTODIA MATERIAL. ART. 197.4 CP.

Se castiga en este apartado cuando "los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros".
Pena: Prisión de tres a cinco años.
Y continua "Si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior".

Este tipo agravado se proyecta sobre las personas encargas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos y registros (delito especial). El tipo básico es el contemplado en el artículo 197.2 (atentados al habeas data).
La LORTAD en su artículo 3.d entiende por responsable del fichero a toda "persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento".

- EL TIPO AGRAVADO DE ACCESO ILÍCITO A LOS DATOS PERSONALES "SENSIBLES" O DE ACCESO ILÍCITO A LA INTIMIDAD DE MENORES E INCAPACES. EL ART. 197.5 CP.

En el apartado 5 del artículo 197 se establecen dos supuestos diferentes:

En el primer supuesto se castigan "los hechos descritos en los apartados anteriores" cuando "afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual"
Penas: Las que correspondan en cada caso en su mitad superior.

Se contempla un tipo agravado, referido a que el acceso ilícito a la intimidad

ajena se produce sobre la esfera más sensible de la misma, lo que la doctrina anglosajona denomina el núcleo duro de la privacy.

Guarda el derecho protegido en éste primer supuesto (a la autodeterminación informativa) un estrecho nexo con valores, como la dignidad humana y el libre desarrollo de la personalidad, recogidos en el artículo 10.1 CE., así como con otras libertades públicas como la libertad ideológica (artículo 16.1 CE.) o la de expresión (artículo 20 CE.) .

La protección jurídica de los datos personales representa, en el marco de la evolución del derecho penal comparado, uno de los aspectos más recientes y significativos del esfuerzo por tutelar y garantizar la esfera de los derechos y libertades fundamentales.

En la misma dirección, la LORTAD somete a un régimen jurídico reforzado de garantías la automatización de los datos personales del artículo 7, al considerarlos datos "especialmente protegidos".

En el segundo supuesto, se establece otra cláusula de especialidad de los delitos tipificados en los apartados anteriores en función de que la víctima fuere un menor de edad o un incapaz. Se trata de una novedad importante en el Código Penal.

Penas: Las que correspondan en cada caso en su mitad superior.

Menor de edad es el que no ha cumplido 18 años e incapaz es "toda persona, haya sido o no declarada su incapacitación, que padezca una enfermedad de carácter persistente que le impida gobernar su persona o bienes por sí misma".

- EL TIPO AGRAVADO EN ATENCIÓN A LOS FINES LUCRATIVOS. ART. 197.6 CP.

Contempla un tipo agravado, que atiende a los fines lucrativos que presiden el atentado a la intimidad.

Penas: Las previstas en los números 1 al 4 del artículo 197 CP. en su mitad superior y en el caso de que el acceso ilícito a la intimidad ajena , llevado a cabo con fines lucrativos, afectase a los datos del núcleo duro de la privacidad (supuesto del apartado 5 del artículo 197 CP), se impondrá la pena de prisión hipergravada de cuatro a siete años de prisión.

No es necesario que se haya conseguido ningún beneficio económico, es suficiente con que la conducta se realice con esa finalidad.

- EL TIPO AGRAVADO DE AUTORIDADES Y FUNCIONARIOS PÚBLICOS. ART. 198.

Se castiga en este artículo, a "la autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior"
Pena: Las respectivamente previstas en el artículo anterior, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

El tipo exige que el sujeto activo actúe con prevalimiento de cargo y que el acceso ilícito a la intimidad se produzca en una situación en la que no medie una causa o investigación judicial por delito.

Sería importante delimitar este tipo con los tipos penales de funcionarios públicos o autoridades contra la intimidad de los ciudadanos contemplados en el capítulo de delitos contra las garantías constitucionales (Cap. V. Secc. 2, Tít. XXI) y sobre todo con los artículos 535 y 536 del CP.

El artículo 535 incrimina los atentados contra la inviolabilidad de correspondencia y de comunicaciones y el 536 contempla los atentados contra la inviolabilidad de comunicaciones telefónicas, de las telecomunicaciones, así como contra el derecho a la propia imagen.

El artículo 536 prevé una pena menor cuando la autoridad o funcionario público que realice esas conductas delictivas lo haga mediando causa por delito. Mientras que en el artículo 199 se castigan las difusiones de datos personales conocidos por motivos profesionales.

Sí la intromisión ilícita contra la intimidad se produce mediando una investigación judicial por delito, de forma ilegal, y conforme a las exigencias típicas subjetivas, vendrá en aplicación el artículo 536 CP.. Igual acontece con los atentados contra la inviolabilidad de correspondencia o postal, mediando causa penal se aplicará el art. 535 CP.

El criterio adoptado por el CP de 1995 para delimitar la aplicación de los delitos contra la intimidad, se ciñe al dato objetivo de que el acceso ilícito a la intimidad se produzca, mediando una causa penal, en el seno por tanto de una investigación pública de carácter penal. De todas formas los artículos 535 y 536 no vendrán en aplicación por el mero dato objetivo de que medie una causa penal. Pues deberá establecerse además

que el atentado contra la intimidad, perpetrado por funcionario público, constituye un exceso en la actividad investigadora del delito que comporta la violación de garantías del ciudadano. Por consiguiente, si media una causa penal sobre el sujeto y , totalmente al margen de la investigación penal se verifica una injerencia en su intimidad, por parte de funcionarios públicos, con prevalimiento de funciones públicas, vendrá en aplicación el artículo 198 CP.

- LA VIOLACIÓN DE SECRETO PROFESIONAL. ART. 199 CP.

En el art. 199 se tipifica la violación del secreto profesional. La formulación que hace el apartado dos del artículo es lo suficientemente genérica como para entender que el precepto penal comprende todo secreto profesional, si bien debe ser excluido de este grupo, por su propia naturaleza, el secreto profesional delos periodistas, que se configura más como derecho, desde una perspectiva estrictamente jurídica, que como deber u obligación.

El secreto profesional general consiste en el deber jurídico a veces reconocido como derecho, de guardar silencio sobre las informaciones que puedan ser calificadas como secretas o confidenciales , conocidas a través del ejercicio de una profesión, cargo u oficio.

- REVELACIÓN DE SECRETOS POR RAZÓN DE OFICIO O RELACIONES LABORALES. ART. 199.1.

Se castiga en el artículo 199.1 al "que revelare secretos ajenos de los que tengan conocimiento por razón de su oficio o sus relaciones laborales".
Pena: Prisión de uno a tres años y multa de seis a doce meses.
Los profesionales de la informática, que en el ciclo operativo del fichero automatizado efectúan el tratamiento automatizado de los datos personales, acceden lícitamente a los mismos.. En este contexto se genera un deber de sigilo o confidencialidad similar al de otra profesiones u oficios. El referido deber de sigilo o discreción también recae sobre el responsable y el encargado de los ficheros automatizados.

Se trata de auténticos deberes jurídicos (por tanto, no son sólo ético-deontológicos de tipo profesional) pues se hallan instituidos por el artículo 10 de la LORTAD.

- SECRETO PROFESIONAL. ART. 199.2 CP.

Se castiga al "profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona"
Pena: Prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

La acción consiste en divulgar los secretos que se conozcan de una persona como consecuencia de la relación profesional con la misma. Con respecto a la acción de divulgar podría cuestionarse la subsunción de los actos electrónicos de cesión o transmisión ilícita de datos. Desde una perspectiva estrictamente gramatical, la objeción puede tener fundamento. Pero, la interpretación gramatical de la acción de divulgar, que dese esa perspectiva puede llegar a sugerir un acto de mayor difusión que las acciones de revelar, ceder o transmitir los datos, debe ser desechada. Si se observa que en los artículos 197 y 199 del CP. el legislador se refiere, en las diversas modalidades típicas, indistintamente, a los actos de difundir, divulgar, ceder o revelar, deberá concluirse que se impone el sentido de la interpretación teleológica, que en este caso no aparece como vulneradora del sentido objetivo de la ley. En esta medida, los actos de cesión o transmisión electrónica ilícita de los datos personales, a los que se accedió lícitamente , por parte del responsable o del encargado del fichero o bien por parte de los profesionales del banco de datos, deben quedar subsumidos en el artículo 199.2 CP.
La perduración del deber de sigilo o discreción sobre los profesionales que operan en el banco de datos, una vez finalizada la relación laboral o profesional, puede llegar a suscitar problemas. Debe postularse la perduración del deber de secreto profesional, una vez verificada la ruptura del vínculo entre el sujeto y el fichero automatizado. Estas cautelas han estado presente en la LORTAD, dado que su artículo 10 instaura el deber de secreto :"El responsable del fichero automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo".

- EXTENSIÓN DE LA TUTELA PENAL DE LA INTIMIDAD A LOS DATOS RESERVADOS DE LAS PERSONAS JURÍDICAS. ART. 200 CP.

Dispone el artículo 200 que: "lo dispuesto en este capítulo, será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código."

Pena: La que corresponda de las previstas en el Capítulo.

Es preciso efectuar una delimitación de este precepto en atención al bien jurídico protegido, la intimidad de las personas físicas. A juicio de MORALES PRATS debe interpretarse que la tutela de datos o informaciones de tipo societario o empresarial stricto sensu no entran prima facie en la ratio de tutela del precepto. Este tipo de información ya encuentra tutela en otros contextos del CP. y, muy especialmente, en el ámbito de los delitos relativos al mercado (artículos 278 y siguientes del CP.). Por lo tanto, el artículo 200 CP. debe interpretarse en sentido restrictivo, de forma que la alusión a datos reservados de las personas jurídicas, se proyecta sobre datos, en principio de personas jurídicas, pero con trascendencia en la intimidad de las personas físicas (por ejemplo de los socios, directivos o empleados de la misma).

El legislador ha generado en el contexto del artículo 278 CP. una grave laguna. En efecto, el precepto no prevé atentados a la información empresarial reservada mediante abuso informático, puesto que no alude a los medios comisivos del artículo 197.2 CP. . Ante este vacío normativo sólo cabe interpretar que el artículo 200 CP cumple una función subsidiaria, de recogida de conductas no abarcadas por el artículo 278 CP. Así, el artículo 200 CP. acogería conductas ilícitas de descubrimiento y de revelación o cesión de datos automatizados de personas jurídicas (en relación a los números 2 y 3 del artículo 197 CP.) pero al precio de desconocer su ubicación sistemática entre los delitos contra la intimidad de la persona física.

En cambio, PÉREZ LUÑO opina que el artículo 200 extiende a las personas jurídicas la tutela penal de la intimidad, cuando se descubren o revelan datos reservados de personas jurídicas sin el consentimiento de sus representantes legales. En este punto, el nuevo Código Penal corrige uno de los aspectos más insatisfactorios de la LORTAD. A medida que el proceso de datos se proyecta a las empresas, a las instituciones y asociaciones, se hace cada vez más evidente la conveniencia de no excluir a las personas jurídicas del régimen de protección que impida o repare los daños causados por la utilización indebida de informaciones que les conciernen. En efecto, la defensa de la intimidad y los demás derechos fundamentales no es privativa de los individuos, sino

que debe proyectarse a las formaciones sociales en las que los seres humanos desarrollan plenamente su personalidad.

- CONDICIONES OBJETIVAS DE PERSEGUIBILIDAD. ART. 201.1 y 201.2 CP.

Dispone el artículo 201.1 que "Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquella sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal".

El artículo 202.1 del CP. prevé la privatización del ius persiquendi en los delitos contra la intimidad regulados en el Capítulo I del Título X CP.

La persecución de los delitos hasta ahora analizados, requería la previa interposición de denuncia de las persona agraviada o de su representante legal. No obstante, cuando la víctima fuere un menor de edad, un incapaz o una persona desvalida la denuncia podrá correr a cargo del Ministerio Fiscal.

El sometimiento de la persecución a la previa denuncia del particular puede plantear problemas, si se repara en que los delitos contra la intimidad perpetrados por medios sofisticados pasan inadvertidos para la víctima, que no percibe las injerencias más penetrantes, certeras y sistemáticas sobre su intimidad. Por este motivo, en muchos casos en los que se empleen estos medios para atacar el bien jurídico, el descubrimiento del delito se producirá generalmente en el seno de actuaciones inspectoras o de investigación al margen de la propia víctima del delito.

El artículo 201.2 indica que "no será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas".

Este apartado libera la persecución del delito del requisito de la previa denuncia de la víctima, en los supuestos de delito contra la intimidad por parte de funcionarios públicos, con prevalimiento de cargo y en los supuestos en los que el delito contra la intimidad afecte a los intereses generales o a una pluralidad de personas, que puede albergar, por ejemplo, supuestos de fuga de datos personales masiva a "paraísos informáticos".

- EL PERDÓN DEL OFENDIDO. ART. 201.3 CP.

Este artículo prevé, como singular forma de extinción de la responsabilidad

criminal en los delitos contra la intimidad, el perdón del ofendido o de su representante legal. Esta medida se adopta, sin perjuicio de lo dispuesto en el artículo 130.4 CP., apartado segundo, con respecto a las garantías previstas para los casos en los que la víctima fuere un menor o un incapaz.

A la vista del artículo 130.4 CP. se observa que el perdón del ofendido puede operar una vez dictada sentencia condenatoria, antes de que se hubiere iniciado la ejecución de la pena impuesta. Debe postularse pues la limitación del perdón al momento anterior de emisión de sentencia.

Con demasiada frecuencia se prestará al chantaje, exigiendo una compensación que estará relacionada con las posibilidades económicas del autor. En principio, esto animará a denunciar hechos con la esperanza de conseguir una indemnización.

2) FRANCIA.

Con la Ley de Modificación del Código Penal, número 88-19, de 5 de enero de 1988, relativa al fraude informático, también conocida como "*loi Godfrain*", el legislador recogió en un nuevo Capítulo del Código Penal, bajo la rúbrica "Sobre ciertas infracciones en materia informática" (especialmente los delitos vinculados a la piratería, intrusión, traba al funcionamiento, esto es virus y ciertas asociaciones que pueden ser de hackers) toda la nueva realidad criminal compleja vinculada a las nuevas tecnologías de la información, pero siempre y cuando no tuvieran ya una adecuada inclusión bajo figuras clásicas existentes. En este sentido, la utilización frecuente del término "informatisé" (informatizado) sobre el de "informatique" (informático), ha hecho pensar a la doctrina que el legislador se ha preocupado de proteger la información en su conjunto y no sólo aquella en soporte informático, es decir, que su preocupación se ha centrado en las conductas fraudulentas de acceso y uso ilícito de los sistemas de tratamiento automatizado de datos, absteniéndose de regular las manipulaciones informáticas con ánimo de lucro y en perjuicio patrimonial de tercero, núcleo principal del fraude informático.

Es así como, el título genérico de la ley hace referencia al fraude informático, en el enunciado, en su texto no aparece ninguna referencia específica al mismo. Es más, la ley sanciona específicamente la falsedad informática, sólo cuando el dato alterado se encuentre sobre un soporte informático.

Por lo tanto, las defraudaciones patrimoniales por medios informáticos quedan

sin regulación especial, porque de acuerdo con las decisiones y jurisprudencia de la Corte de Casación Francesa y de los Tribunales de Apelación, aquellas venían siempre subsumidas en la figura clásica de estafa del Art. 405 del Código Penal, que sanciona al que "*haciendo uso de falsos nombres o de falsas cualidades, bien empleando maniobras fraudulentas para simular la existencia de falsas empresas, de un poder o crédito imaginario, o por hacer nacer la esperanza o la creencia de un suceso, de un accidente o de cualquier otro acontecimiento imaginario, se haya hecho reintegrar o traspasar, o hubiera intentado hacerse reintegrar o traspasar fondos, muebles, obligaciones, disposiciones, billetes, promesas, deducciones o desgravaciones, y hubiera por uno de estos medios, defraudado o intentado defraudar la totalidad o parte de la fortuna de otro".*

La subsumisión es posible al recogerse en la descripción de la conducta típica la cláusula "maniobras fraudulentas" y el "perjuicio", debiéndose entender éstas como formas de engaño, siendo las manipulaciones informáticas integrables en aquéllas, y la omisión del texto a referencias genéricas sobre el "engaño", el "error" y al "acto de disposición". Al respecto, según la doctrina, la ley de reforma francesa se concibe materialmente como una vía para reprimir accesos abusivos a los sistemas informáticos y actuaciones ilícitas sobre datos informatizados y su tratamiento, se produzca o no perjuicio, habiéndose rechazado de forma expresa en el proceso de tramitación parlamentaria las propuestas de subsumir las agresiones patrimoniales por medios informáticos en los tipos recogidos por esta ley.

La reforma penal de 1992, Ley 92-683, vigente a partir de marzo de 1994, introdujo cambios en el texto legal de las disposiciones informáticas y las trasladó a otra parte del Código, esto es, al Libro III, Título II, Capítulo III: De los atentados contra los sistemas de tratamiento automatizado de datos. La falsificación informática que estaba regulada en los artículos 462-5 y 462-6, sobre la falsificación y uso de documentos electrónicos falsificados, actualmente en el nuevo Art. 441-1, que se refiere a todas las posibles formas de un documento, incluyendo el electrónico. El acceso fraudulento en sistemas informáticos en el actual 323-1, sabotaje informático en el artículo 323-2.

- Acceso fraudulento a un sistema de elaboración de datos.

Artículo 323-1. "El hecho de acceder en forma fraudulenta a la totalidad o parte de un sistema de tratamiento automatizado de datos, o de mantenerse en él, será castigado con

un año de prisión y multa de 15.000 euros.

Si de ello resultare, bien la supresión o la modificación de datos contenidos en el sistema, o una alteración del funcionamiento de este sistema, la pena será de dos años de prisión y de 30.000 euros de multa".

Para que se entienda consumado este delito, no se requiere la alteración, daño o destrucción de los datos contenidos en el sistema, ni el apoderamiento, uso o conocimiento de la información contenida en él, y tampoco la revelación o difusión de los datos contenidos en ese sistema. La mención a "mantenerse en él", se refiere al acceso que ocurre en forma accidental o casual.

- Sabotaje informático

Artículo 323-2. "El hecho de obstaculizar o alterar el funcionamiento de un sistema de tratamiento automatizado de datos será castigado con tres años de prisión y multa de 45.000 euros".

La legislación francesa, al igual que la alemana distingue entre el delito de sabotaje informático y la alteración de datos.

- Destrucción de datos.

Artículo 323-3. "El hecho de introducir de manera fraudulenta datos en un sistema de tratamiento automatizado o de suprimir o modificar fraudulentamente los datos que contengan será castigado con tres años de prisión y multa de 45.000 euros".

El objeto del delito son los datos contenidos en un sistema de tratamiento de los mismos.

- Asociaciones para cometer delitos informáticos.

Artículo 323-4. "La participación en un grupo formado o en un acuerdo establecido para la preparación, caracterizada por uno o varios hechos materiales, de una o varias de las infracciones previstas en los artículos 323-1 a 323-3 será castigada con las penas previstas para la misma infracción o para la infracción castigada más severamente ".
Se trata de los llamados Clubs de Hackers.

Artículo 323-5. “Las personas físicas culpables de los delitos previstos en el presente capítulo incurrirán igualmente en las penas accesorias siguientes:
1º La prohibición, por un período hasta de cinco años, del ejercicio de derechos cívicos, civiles y de familia, según las modalidades del artículo 131-26;
2º La prohibición, por un período de hasta cinco años, de ejercer una función pública o de ejercer la actividad profesional o social en el ejercicio de la cual o con ocasión de la cual se haya cometido la infracción;
3º El comiso de la cosa que haya servido o estaba destinada a cometer la infracción o de la cosa producto de la misma, con excepción de los objetos susceptibles de restitución;
4º La clausura, por un período de hasta cinco años, de los establecimientos o de uno o varios de los establecimientos de la empresa que hayan servido para cometer los hechos incriminados;
5º La exclusión, por un período de hasta cinco años de los contratos públicos;
6º La prohibición, por un período de hasta cinco años, de emitir cheques, salvo los que permitan la retirada de fondos por el librador contra el librado o los que estén conformados;
7º La publicación o la difusión de la resolución adoptada en las condiciones previstas en el artículo 131-35”.

Artículo 323-6. “Las personas jurídicas podrán ser declaradas penalmente responsables de las infracciones definidas en el presente capítulo en las condiciones previstas en el artículo 121-2.

Las penas aplicables a las personas jurídicas serán:
1º La multa, conforme a lo previsto en el artículo 131-38;
2º Las penas mencionadas en el artículo 131-39.

La prohibición mencionadas en el apartado 2º del artículo 131-39 se aplicará a la actividad en cuyo ejercicio o con ocasión de la cual se haya cometido la infracción”.
Artículo 323-7. “La tentativa de los delitos previstos en los artículos 323-1 a 323-3 será castigada con las mismas penas ”.

- Falsificación y uso de documentos electrónicos falsificados.

Artículo 44 1-1. “Constituye una falsedad toda alteración fraudulenta de la verdad, susceptible de causar un perjuicio y realizada por cualquier medio, en un escrito o en cualquier otro medio de expresión de pensamiento que tenga por objeto o que pueda tener como efecto constituir la prueba de un hecho con consecuencias jurídicas o de un derecho ”.

El legislador francés suprimió los artículos 462-5 y 462-6, sobre falsificación y uso de documento electrónico falsificado, y amplió el concepto de documento de manera de incluir los electrónicos.

3) ALEMANIA.

La reforma penal en materia de delitos informáticos, vino como consecuencia de la insuficiencia y deficiencias de las normas tradicionales y los tipos clásicos en ellas previstas. Un largo debate, iniciado a mediados de la década de los setenta, dio como resultado la “Segunda Ley de Lucha contra la Criminalidad Económica” de 1986.

Las modificaciones introducidas por esta Ley en el Código Penal Alemán, respecto de las conductas delictuales relacionadas con los medios informáticos, no sólo consistieron en la modificación de alguna disposición ya existente, sino que en algunos casos se introdujeron nuevas figuras o tipos penales.

Entre las nuevas figuras que regula Ley se encuentran: el espionaje de datos (párrafo 202.a), estafa mediante ordenador o fraude informático (párrafo 263.a), falsificación de datos probatorios (párrafo 269), modificaciones complementarias del resto de las falsedades documentales (párrafo 270, 271, 273, 274 y 348), engaño en el tráfico jurídico mediante sistemas de procesamiento de datos (párrafo 270), modificación de datos (párrafo 303.a) y sabotaje informático (párrafo 303 .b).

- Espionaje de datos.

Párrafo 202.a

“I. Quien consiga sin autorización, para sí o para otro, datos que no le competan y que estén especialmente protegidos contra el acceso ilegítimo será castigado con pena privativa de la libertad de hasta tres años o con multa.

II. Datos, a efectos del apartado I, serán sólo aquellos que sean almacenados, transmitido electrónica, magnéticamente, o de forma no inmediatamente accesible ”.

El tipo protege el interés formal en el mantenimiento del secreto por parte del titular para disponer del almacenamiento y transmisión de datos no directamente perceptibles, el que a través de su protección manifiesta su interés en el mantenimiento del secreto.

Sujeto activo sólo puede ser aquel para el cual no están previstos los datos, de manera que no contempla el supuesto del empleado que sin autorización utiliza datos para el accesibles. La punibilidad está limitada a los datos que están especialmente protegidos contra el acceso no autorizado (ejemplos, contenedores cerrados, contraseñas, encriptados, etc.).

Del concepto de datos del inciso segundo del párrafo 202.a, se desprende que es necesario que el acto de espionaje recaiga sobre datos no perceptibles directamente.

- Estafa informática.

Párrafo 263.a "I. Quien, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro influyendo en el resultado de un proceso de elaboración de datos por medio de una errónea configuración del pro grama, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso, será castigado con pena de privación de libertad de hasta cinco años o con multa.
II. Procede aplicar el 263, apartados II a V.

El párrafo 263.a contempla la conceptuación de la figura como tipo básico en el inciso primero, y la sanción de la forma imperfecta de ejecución (tentativa) y un supuesto de agravación del tipo en razón de la gravedad del hecho (privación de libertad de uno a 10 años) por la remisión que efectúa al párrafo 263.

El proyecto del gobierno entendió por "proceso de datos" todos aquellos procesos técnicos en los que se alcanzan determinadas conclusiones de trabajo a partir de la toma de datos y de su puesta en relación según determinados programas. Se contempla aquí únicamente el proceso automático de datos. Según las reglas alemanas un programa es una instrucción completa para la resolución de una tarea junto con todos los ajustes precisos para ello, los programas informáticos son instrucciones de trabajo para el ordenador.

En cuanto a la situación que se refiere al empleo de datos incorrectos o

incompletos comprende la manipulación en el input o entradas, no sólo por el operador o usuario del terminal que suministra de modo inmediato datos falsos a la instalación del proceso electrónico de datos, sino también por quienes los proporcionan de modo inmediato, como el personal de clasificación de datos (perforadores, mecanógrafos, etc.). Se incluyen los casos de determinación a través de terceros ajenos (ej. clasificación de datos primarios), como los casos de suministro inmediato, en que intercalan terceros que no practican ninguna comprobación material de los datos.

De acuerdo con la doctrina alemana, el que utiliza una tarjeta falsificada de acceso al ordenador emplea datos incorrectos del mismo modo de quien falsifica estados de cuenta.

En cuanto a la influencia en el resultado de un proceso de elaboración de datos a través de un uso no autorizado de datos, la doctrina alemana, considera que de este modo se ha cubierto el supuesto del que mediante uso ilegítimo de tarjeta (las de cajero) y de códigos ajenos consiga acceder a sistemas informáticos con efectos patrimoniales de relevancia.

Respecto de la influencia en el resultado de un proceso de elaboración de datos a través de intervención no autorizada en el proceso, la misma doctrina, la considera una fórmula amplia que pretende evitar posibles lagunas legales, abarcando supuestos no subsumibles en las alternativas anteriores, o de dudosa subsunción.

Ahora bien, al no recoger expresamente, la fórmula alemana, el término ordenador o informático tienen cabida en el precepto las manipulaciones fraudulentas de tipo patrimonial sobre cualquier tipo de sistemas automatizado de toma de decisiones, y no únicamente informático, consistiendo la acción típica en interferir en el resultado de un proceso de tratamiento de datos, de lo que se deriva una interferencia en una disposición patrimonial.

- Falsificación de datos probatorios.

Párrafo 269.

I. Quien, para engañar en el tráfico jurídico, almacene o altere datos probatorios relevantes de manera que en el momento de su recepción existiría un documento no auténtico o falsificado, o utilice datos almacenados o alterados de ese modo será castigado con pena de privación de libertad de hasta cinco años o con multa.

II. La tentativa es punible.

Deberá aplicarse el 267, apartado III".

La doctrina alemana, ha señalado que en ese país, el tipo de falsedad documental no es aplicable a la llamada falsificación de datos probatorios, debido a la imposibilidad de percibir directamente la declaración y la identidad del otorgante.

La acción consiste en modificar datos ya almacenados o almacenar otros nuevos con el mismo fin, o en utilizarlos en esas condiciones. Es necesario que la visualización de los datos sea equiparable a la existencia de un documento no auténtico o falsificado, es decir, que si fueran impresos o transcritos esos datos constituirían falsedad documental al tenor del párrafo 267.

En cuanto a los elementos del tipo subjetivo, además del dolo (basta que sea eventual), debe concurrir la intención de engañar en el tráfico jurídico. Según la doctrina alemana este requisito se cumple cuando el autor sólo quiere producir la manipulación en el proceso de datos, por lo tanto, no se exige el contacto personal entre el autor y la víctima (a diferencia de cómo es interpretado el engaño en el tipo de estafa). El artículo 270 aclara las dudas sobre el contenido de este elemento, con la innovación de equiparar el engaño a las manipulaciones informáticas, al disponer "La falsificación de una elaboración de datos en el tráfico jurídico equivaldrá al engaño en el tráfico jurídico ". Esta norma es aplicable a todos los tipos legales en los que se exige "el engaño en el tráfico jurídico", teniendo gran importancia al considerar que la manipulación fraudulenta del proceso de datos produce un efecto similar al engaño.

- Alteración de datos.

Párrafo 303.a.

"I. Quien borre, elimine, inutilice o altere ilícitamente datos (202.a, apartado II) será castigado con pena de privación de libertad de hasta dos años o con multa

II. La tentativa será punible ".

La disposición protege tanto al que almacena los datos, como a la persona afectada por el contenido de éstos. Objeto de la acción, son todos los datos no inmediatamente perceptibles en el sentido del párrafo 202.a.II.

Se mencionan cuatro acciones típicas:

a) el borrado, los hace desparecer de modo completo e irrecuperable (Ej. la destrucción de soportes, borrar los enlaces necesarios y perder la interpretabilidad, etc.);

b) ocultar, privando del acceso a los mismos a la persona autorizada;
c) inutilizar, cuando se dañan de manera tal que no puedan cumplir su fin;
d) alterar, se trata de perturbaciones funcionales, como la transformación de su valor informativo, puede tener lugar a través del añadido de datos, el borrado parcial o la puesta en relación con otros datos. Lo decisivo es que los datos posean un nuevo contenido una información alterada.

- Sabotaje informático

Párrafo 303b. "Quien destruya una elaboración de datos que sea de esencial importancia para una industria ajena, una empresa ajena o una autoridad, cometiendo el hecho de acuerdo al párrafo 303 .a.II, o destruyendo, dañando, inutilizando, eliminando o alterando una instalación de elaboración de datos o un soporte de datos, será castigado con pena de privación de libertad de hasta cinco años o con multa. II. la tentativa será punible ".

La finalidad perseguida por la legislación alemana, al crear el tipo de sabotaje informático diferenciado del tipo de alteración de datos, fue sancionar con mayor severidad las acciones que atentan contra procesos de datos que sean de importancia esencial para una empresa o establecimiento industrial ajenos o para la administración. Estas acciones pueden recaer en los equipos de procesamiento de datos, en los soportes y en los datos mismos. La doctrina entiende que es sancionado penalmente el que arremete a equipos o soportes de datos suyos en los que otras personas tengan un interés jurídicamente protegido o si borra datos que el mismo hubiera almacenado y que fueran procesados para terceros cuyo interés en su existencia se perjudica.

4) ITALIA.

El Código Penal italiano tipifica los siguientes delitos informáticos:

- Acceso abusivo a un sistema informático o telemático (artículo 615 tercero)

Se configura exclusivamente en caso de sistemas informáticos o telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de

reservar el acceso al mismo sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes.

- Difusión de programas dirigidos a producir daños o interrumpir un sistema informático o telemático (artículo 615 quinto)

El que difunda un programa informático que tenga por objeto el daño a un sistema informático o telemático, datos, o programas, o la interrupción total o parcial de funcionamiento puede ser condenado hasta dos años de prisión.

- Atentado contra un sistema informático o telemático de utilidad pública (artículo 420)

Se sanciona con pena de prisión a quien dañe o destruya un sistema informático de utilidad pública.

- Abuso de la calidad de operador de sistema.

Este delito es una agravante del delito de acceso abusivo y lo comete quien tiene la posibilidad de acceder y usar un sistema informático o telemático de manera libre por la facilidad de comisión del delito.

- Detentación y difusión abusiva de códigos de acceso a sistemas informáticos o telemáticos (Artículo 615 cuarto)

Castiga al que con el fin de obtener para sí o para otro un beneficio o causando un daño a otro, abusivamente se apodera, reproduce, difunde, comunica códigos, palabras claves u otro medio idóneo que permita el acceso a un sistema informático o telemático.

a. Difusión de programas dirigidos a dañar o interrumpir un sistema informático (Artículo 615 quinto).
b. Violación de la correspondencia electrónica (articulo 616)
c. Intercepción abusiva. (Artículo 617, cuarto, quinto)

Está tratado junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. La intercepción fraudulenta, el impedimento

o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, de todo o parte, por cualquier medio del contenido de la comunicación se castiga con reclusión de seis meses a cuatro años. Se castiga también la instalación de aparatos para interceptar, impedir o interrumpir las comunicaciones informáticas o telemáticas.

- Falsificación informática (617 sexto)

Es la alteración, modificación o borrado del contenido de documentos o comunicaciones informáticas o telemáticas. Documento informático está definido por la doctrina italiana como cualquier soporte informático que contenga datos, informaciones o programas específicamente destinados a elaborarlos.

- Espionaje informático.

- Fraude informático (Artículo 640 tercero)

La disposición establece que cualquiera que procure un beneficio para sí o para otro alterando de cualquier modo el funcionamiento de un sistema informático, sobre los datos, las informaciones o los programas comete delito de fraude informático. La pena se agrava si el sujeto activo es operador del sistema informático.

- Ejercicio arbitrario de la propia razón con violencia sobre programas informáticos (Artículo 392)

Los virus informáticos pueden ser usados como una excelente herramienta para la protección de los derechos intelectuales y los negocios contractuales. Pero estas conductas pueden no ajustarse a Derecho. Si un programador inserta un virus en un programa a fin de que, en caso de copia, el mismo se active y destruya la información existente en el ordenador es posible considerar la situación como abuso de Derecho. Si bien el titular de la obra de software está en su derecho de proteger sus intereses como autor o dueño, dicha facultad no debe extenderse más allá de lo que razonablemente expliciten las leyes, o el contrato que lo relacione con el usuario. El Código Penal italiano en el artículo 392, sanciona el ejercicio arbitrario, con violencia, sobre un

programa, mediante la total o parcial alteración, modificación o cancelación del mismo o sobre un sistema telemático, impidiendo o perturbando su funcionamiento.

CAPITULO VI: Protección Administrativa

"Todo lo que puede ser inventado ha sido inventado."
Charles H. Duell, Comisario de la Oficina de Patentes de EEUU, 1899

1) Rol del Estado y las Tecnologías de la Información.

La organización política de la sociedad es una construcción histórica que evoluciona de manera diferente, dependiendo de realidades globales y particulares de cada lugar y tiempo. El Estado es probablemente la construcción política más relevante de la modernidad. No obstante, hacia fines del siglo XX, aparte de las duras críticas de los más diferentes sectores políticos e ideológicos, respecto de sus capacidades para enfrentar los mas diversos desafíos, constituye una realidad plenamente vigente. En los últimos años diferentes enfoques han propuesto abordar la problemática del Estado, o de sus componentes, con la intención de adecuarlo a los requerimientos de los nuevos tiempos. Así han surgido respuestas para Reformar el Estado, para resustancializarlo, para reducirlo, o para reinventar el Gobierno, entre otras.

Algunos autores, como Castells, nos dicen que la tecnología no determina la sociedad. Sin embargo el impactante cambio -entendido como revolución de la tecnología de la información- se expresa en diferentes ámbitos del quehacer humano y particularmente en las comunicaciones (entre personas, organizaciones, instituciones) y en la captura, procesamiento y utilización de la información (para optimizar procesos productivos de bienes y servicios). Se debe considerar además el prodigioso avance en el mapeo del genoma humano que tiene claras implicancias en el futuro desarrollo de la

biotecnología, incorporando nuevas interrogantes, dudas y posibilidades en la vida de las personas, a partir de las múltiples aplicaciones posibles que se pueden derivar en el desarrollo de la informática y las comunicaciones, además de la medicina y los sistemas productivos y de investigación.

La tecnología ha provocado entre muchos de sus impactos uno de la mayor relevancia, esto es la transformación que ha tenido en nuestras sociedades el concepto del tiempo. "Este tiempo lineal, irreversible, medible, predecible se está haciendo pedazos en la sociedad red, en un movimiento de significado histórico extraordinario...es la mezcla de tiempos para crear un universo eterno, no autoexpansivo, sino autosostenido y no cíclico, sino aleatorio, no recurrente, sino incurrente: el tiempo atemporal".[115] ¿Cómo entonces definir políticas, hacer leyes, tomar decisiones, definir el interés público, establecer acuerdos, firmar tratados, en suma gobernar y llevar el timón de la nave sociedad hacia el futuro?.

En el contexto de la llamada nueva economía, el grado de interdependencia e interconexión en la economía mundial se ha incrementado dramáticamente y eso mismo puede ser también observado en el sistema político internacional, el cual puede ser mirado como una web de interdependencia. .[116]

Algunas funciones del estado, que son prioritarias desde el punto de vista económico: Como "contenedor" de prácticas e instituciones únicas y distintivas, como regulador de las actividades, como competidor con otros estados tal como puede competir una firma con otra. Al decir de Porter, las diferencias en las estructuras económicas nacionales valores, cultura, instituciones, historia contribuyen intensamente a generar diferencias competitivas. De allí la importancia del Estado en el papel que pueda jugar la actividad comercial, la inversión extranjera y las políticas de desarrollo.

Es en ese contexto que resulta particularmente interesante analizar el papel del Estado ante el efecto de la sociedad de la información en la organización del trabajo como actividad humana, y en el proceso educativo.

Por el proceso de la globalización y partiendo de la premisa que el proceso de globalización es un fenómeno también comunicacional, pero a la vez económico y cultural y que muy probablemente se habría visto demorado, sin contar con las tecnologías de la comunicación disponibles hoy día.

[115] Dicken, P. Global Shift. PCP ed. London., pág 467, 1999
[116] Dicken, P opcit, pag. 79

La globalización puede ser pensada al inicio de su estudio como un proceso amplio, profundo y veloz de interconexión a nivel de todo el mundo en todos los aspectos de la vida social, [117] que va desde las expresiones mas elevadas del ser humano hasta las mas repugnantes. Puede ser concebida como un procesos altamente diferenciado el cual encuentra expresión en todos los aspectos claves de la actividad social y, podemos agregar, con influencia en todos los aspectos de la vida humana.

Las Tecnologías de la Información y las Comunicaciones han cambiado radicalmente la naturaleza de las relaciones humanas al disponer de la capacidad de procesar enormes volúmenes de datos, trasformarlos en conocimiento y transmitirlos a cualquier parte en tiempo real; esto es, capacidad de generar y transmitir conocimiento acelerando el ritmo y la calidad en la interacción en prácticamente todas las áreas de la actividad humana. Este es el paradigma de la Sociedad de la Información.

Este paradigma ha permitido acelerar el proceso de convergencia tecnológica dentro del cual, las tecnologías se retroalimentan para ser más eficaces y eficientes, y a su vez permiten generar más conocimiento para crear mayor sinergia. La convergencia tecnológica actúa como mediador entre actores dentro de las estructuras sociales cada actividad de agregación, transmisión, recepción, análisis, y actuación, derivada de la información y conocimiento implícitos en esta cadena.

El impacto social de las TIC se ha acentuado porque éstas han sido progresivamente más accesibles a cada Ciudadano, ampliando la red de intercambio de conocimiento y por ello añadiéndole valor. La expresión concreta de esta red ha sido Internet, inicialmente posible por una tecnología previa como es la telefónica, al disponer de su infraestructura, además del desarrollo y aceptación de protocolos que empaquetan la información y permiten intercambio dentro de márgenes aceptables de error.

La Sociedad de la Información está así sujeta a diversas lecturas por la enorme variedad y profundidad de la convergencia tecnológica[118]. Así, podemos analizarla desde una perspectiva básicamente técnica (TICs, desarrollo de hardware y software); cultural y social (contenidos masivamente intercambiados, comunidades virtuales con impactos en la cultura y la política); económica: eCommence, eBusiness (B2B, B2C, P2P,G2B,G2C,G2G) y las nuevas realidades laborales y el efecto en el Estado de

[117] Held, D.; Mac Grew, A.; Goldvlatt, D.; Perraton, J.,Global Transformation. Polity Press, Cambridge, 1999.
[118] Castells, M. (2000). "The New Economy: Informationalism, Globalization, Networking". The Rise of the Network Society (Second Edition). Malden: Backwell Publishers Ltd.

Bienestar[119]; o filosófica, mediante la comprensión de la nueva vivencia espacio-temporal de cada Ciudadano.

Todas las aproximaciones para comprender la Sociedad de la Información, suponen elementos reales, si bien muchos de ellos además son virtuales , que pueden expresarse por diversos canales, siendo el dúo Internet/PC el más conspicuo, además de la TV interactiva, móviles, dispositivos inalámbricos, etc.

Internet es actualmente el canal principal de expresión de la Sociedad de la Información compuesto por navegadores en metalenguaje, hipervínculos, y convergencia de contenido escrito y audiovisual.

Estos componentes de Internet, han sido producto de una combinación de iniciativas de desclasificación y masificación del Estado (como expresión Civil y/o Militar) y del Mercado respectivamente. Ejemplo de ello ha sido la evolución desde el Proyecto ARPANET hasta la Web actual, o de la tecnología de satélites hasta las comunicaciones planetarias actuales.

La evolución de la Nueva Economía ha creado una realidad en la cual existen empresas privadas como actores globales en todos los tipos de actividad, tanto primaria, como intermedia o de servicios. Para coordinar estas actividades y ser competitivos, se ha dispuesto de sistemas de gestión mucho más eficientes para lograr sus respectivos objetivos particulares en comparación con la gestión del Sector Público: el sector privado se ha convertido en el actor principal dentro de la Nueva Economía, y ha adquirido la iniciativa con relación al Estado y los organismos internacionales de regulación y financiamiento, para seguir configurando la Sociedad Informacional. Esto pone en peligro la gobernabilidad como concepto integrador y articulador y pone el mercado como elemento rector principal. La evolución de la asimetría en el reparto de recursos y la degradación ambiental son dos ejemplos claros de la crisis de gobernabilidad, en cuya acción prevalece la visión unidimensional de la economía.

Rescatar el rol activo de los Estados y de los organismos internacionales de cogobierno o regulación pasa por superar la Brecha Digital, permitiendo el acceso masivo a los canales de expresión que ofrecen las TIC, profundizando la relación Ciudadano-Gobernante, acercando al Ciudadano a su respectiva administración local o nacional, y reforzando así la representatividad del Estado para redimensionar el rol de cada actor.

[119] Carnoy, M. (2000). "New Technology and Job Markets". Sustaining the New Economy. Russell Sage Foundation: New York.

Ello obliga a cada estado a formular un plan de desarrollo de superación de la Brecha Digital en el cual la visión del proyecto de país debe contener metas muy concretas en materia de infraestructura, capacitación, descentralización, e iniciativas legislativas.

Un ejemplo de la importancia de la presencia del Estado se halla en las resoluciones de la Unión Europea, reconociendo la importancia de la economía digital para el crecimiento, productividad y empleo, la importancia de ofrecer a los ciudadanos todas las posibilidades de acceso y capacitación necesarias para desempeñarse y trabajar en la Sociedad de la Información, y la necesidad de realizar progresos para mantener el desarrollo de la economía digital como una prioridad en la agenda Europea.[120]

Otro ejemplo lo ofrece el Gobierno de Irlanda, que insiste en tres aspectos estratégicos, como son el desarrollo de ancha banda para la conectividad, la promoción de un clima propicio para la innovación y la inversión en la capacitación[121]. Por otra parte, el Gobierno de Australia considera que los estados deben asumir un nuevo papel que supere el rol de meros reguladores, para ser factores activos de capital, conocimiento, innovación e inversiones[122]. Opiniones similares se hallan en los documentos oficiales de gobiernos del Reino Unido, Nueva Zelanda, Italia, Chile, Canada, Sur Africa, etc.

Así mismo, el rol de las instituciones supranacionales es progresivamente destacado para compensar una característica que define la forma actual de globalización, que tiende a neutralizar los intentos de los estados para manejar sus asuntos con autonomía, y para hacer realidad la intención de muchos países de abordar colectivamente determinadas políticas por medio de lo que se define sistema internacional.[123]

Las iniciativas de los estados y sus acciones concretas han constituido factores clave de éxito en su aumento de competitividad, ya que los programas relativos a la Brecha Digital y de Gobierno Digital han obligado a repensar en detalle la estructura, el funcionamiento, los procedimientos y las métricas del Sector Público, y a realizar la adecuada capacitación para sus funcionarios, incrementando así su productividad y

[120] COUNCIL RESOLUTION OF THE EUROPEAN UNION on the implementation of the eEurope. 2005 Action Plan. 5197/03. Brussels, 28 January 2003

[121] Building the Knowledge Society. Report to Government, December 2002. Information Society Commission. www.isc.ie

[122] Drivers and Shapers of Economic Development in Western Australia in the 21st Century. http://www.wa.gov.au/tiac/index.html

[123] Held, D. and McGrew, A., Goldblatt, D. and Perraton, J. (1999), Global Transformations : Politics,Economics and Culture, Polity Press, Cambridge. Chapter 1.

satisfacción general. Todo ello dentro de un marco metodológico que integra datos acerca de la realidad digital, los grupos poblacionales que ameritan intervención estatal en esta materia, los principales actores de este proceso, y las prácticas establecidas y exitosas en otros países. Este cambio cualitativo del Sector Público, unido a canales de comercio electrónico que le permiten interactuar con el Ciudadano y las empresas, ha trasladado a éstos el crecimiento del factor productividad, permitiendo que, en conjunto, cada país sea más competitivo.

- ¿Cuál es el panorama en Chile?

Este desarrollo de las TIC no es un dato menor, de hecho en Chile y el mundo se habla de la asistencia del planeta a una nueva revolución; la revolución tecnológica. Esta revolución tecnológica es equiparable, y algunos prevén que superará en importancia, a la revolución industrial y al desarrollo de la imprenta y el libro.

Ya en el informe elaborado por la Comisión Presidencial "Nuevas Tecnologías de Información y Comunicación", titulado "Chile: hacia la Sociedad de la Información", presentado el 26 de enero de 1999 al Presidente Eduardo Frei Ruiz-Tagle, se señala:
"Esta revolución tecnológica resulta de la convergencia de diversos fenómenos, entre los que destacan la difusión mundial de redes de información y comunicaciones (como Internet), la informatización de bienes y procesos, la digitalización de la información y la creciente importancia del aspecto inmaterial de la riqueza producida. Emerge un nuevo paradigma económico y social caracterizado por la confluencia de cinco procesos:

- La integración digital de sonido, datos e imagen, así como la convergencia entretelecomunicaciones, computación y televisión. De esta forma, las distinciones tradicionales entre telefonía, televisión, ondas radiales y TVcable tienden a desaparecer. Se tornará cada vez más irrelevante la diferencia entre medios de acceso (computador, televisión u otros artefactos) a las redes digitales, de información, mientras éstas ofrecerán nuevos servicios cada vez más interactivos.

- La maximización de la eficiencia y eficacia social de las nuevas tecnologías cuando operan en redes. Es decir, no sólo se trata de redes físicas con computadores y cables de fibra óptica, sino redes sociales y comerciales de

información y conocimiento, que aumentarán su utilidad para los usuarios y para la sociedad en la medida que más personas y empresas estén conectadas a ellas.

- La aceleración de la producción y difusión global del conocimiento y la información. Las nuevas tecnologías potencian la sinergia entre conocimiento e innovación. Esto implica que mientras más invierta el país en recursos humanos, mayor será su dominio sobre estas nuevas tecnologías y mayor será su capacidad de innovar, generando nuevas bases de competitividad y bienestar social.

- El desarrollo de una nueva infraestructura de información. Su rol será tan vital para el crecimiento y el bienestar como actualmente lo es la infraestructura física. La multiplicación de las redes digitales, y el enriquecimiento del contenido que viaja por ellas, facilitará el desarrollo de empresas y mercados, el funcionamiento eficiente y descentralizado del sector público, así como el tránsito hacia una sociedad civil cada vez más abierta y comunicativa".

Actualmente, durante el gobierno del actual Presidente de la República, don Ricardo Lagos Escobar, se envió el 11 de mayo de 2001 un texto instructivo Presidencial en lo referido al llamado Gobierno Electrónico, donde hace referencia a todas las características relativas a la introducción y uso de las Tecnologías de la Información y las Comunicaciones y cual sería el Rol del Gobierno (en este sentido del Estado):

El texto reza:

I. En los últimos años, las tecnologías de información y comunicación han tenido un significativo desarrollo.

Ello ha generado un fuerte impacto en los distintos ámbitos del quehacer de las personas y de la actividad económica, pues ha facilitado la vida cotidiana y ha logrado mayor eficiencia y eficacia en el desarrollo de variados tipos de procesos.

El desarrollo de estas tecnologías abre nuevos e interesantes canales, tanto para la provisión de servicios a la sociedad, como para mejorar la calidad y oportunidad de la información a la que los ciudadanos pueden acceder.

Hoy se habla del "Gobierno Electrónico". Este es el uso de las tecnologías de información y comunicaciones que realizan los órganos de la administración para

mejorar los servicios e información ofrecidos a los ciudadanos, aumentar la eficiencia y la eficacia de la gestión pública e incrementar sustantivamente la transparencia del sector público y la participación de los ciudadanos.

El Gobierno ha definido diversas acciones para desarrollar una mejor relación Estado-ciudadano, apoyándose en tecnologías de información. En tal sentido, en octubre pasado, fue aprobada una Agenda de Gobierno Electrónico por el Comité de Ministros de las Nuevas Tecnologías de Información y Comunicaciones.

Actualmente se encuentran en fase de desarrollo, un conjunto de iniciativas e instrumentos que van en la dirección indicada.

II. En mérito de lo anterior y con el objeto de definir claramente los componentes esenciales del Gobierno Electrónico, he resuelto instruir lo que indico a continuación.

1. En primer lugar, los ámbitos en los cuales se desarrollará el Gobierno Electrónico serán los siguientes:

a. Atención al ciudadano. En esta materia, se considera el establecimiento de nuevas formas de relación Gobierno/ciudadano-empresa-inversionista, mediante el uso de las tecnologías de información y comunicaciones , que permitan al Estado brindar sus servicios en forma eficiente, eficaz y con independencia del lugar físico.

b. Buen Gobierno. Se busca el establecimiento e introducción de nuevas formas y procesos internos en la Administración del Estado, que permitan la integración de los sistemas de los diferentes servicios, compartir recursos y mejorar la gestión interna de los mismos.

c. Desarrollo de la democracia. Se considera la creación de mecanismos que, usando las tecnologías de información y comunicaciones, permitan al ciudadano jugar un rol activo en el quehacer del país, permitiendo abrir nuevos espacios y formas de participación.

2. En segundo lugar, los principios orientadores que deberán regir todos los proyectos de Gobierno Electrónico, serán los siguientes:

a. Transformador. Promueve el establecimiento, en la Administración del Estado, de una nueva forma de operar, creando y modificando sustantivamente los actuales procedimientos de funcionamiento y de relación con el ciudadano, mediante la introducción de tecnologías de información y comunicaciones.

b. Al alcance de todos. Se traduce en asegurar a todos los ciudadanos el acceso a los servicios provistos en forma electrónica por el Estado, considerando una dimensión geográfica (dónde se accede), una social (quién accede) y una horaria (cuándo se accede), y asegurando que dichas dimensiones sean equitativas.

c. Fácil de usar. Tiene por propósito que las tecnologías de información utilizadas por el Estado, sean simples y sencillas para los ciudadanos.

d. Mayor beneficio. Implica que el beneficio que signifique para los ciudadanos demandar un servicio a través de tecnologías de la información y comunicaciones, sea superior al que recibirán de obtenerlo en forma presencial en las dependencias del órgano público.

e. Seguridad, privacidad y registro. Su finalidad es disponer de adecuados niveles de seguridad y de estándares, respecto a la privacidad de las personas en el acceso a la información y de las transacciones que se efectúen.

f. Rol del sector privado. Postula que la implementación de servicios, así como la formación y capacitación de funcionarios y ciudadanos, se apoye en el sector privado. Esto se hará mediante procesos competitivos. Sin embargo, la propiedad y uso de la información estará siempre reservada al Estado y al ciudadano al cual pertenezca.

g. Desconcentración. Indica que la administración, mantención y actualización de las tecnologías de información y comunicaciones, será de responsabilidad de cada Servicio, salvo aquellas situaciones que involucren la participación de varios Servicios. En todo caso, se debe asegurar la interoperabilidad al interior del sector público.

h. Competencia electrónica. Señala que las transacciones podrán efectuarse desde cualquier punto del territorio, por lo que las competencias de los Servicios deberán adaptarse para contemplar esta posibilidad.

3. En tercer lugar, el desarrollo del Gobierno Electrónico deberá asumirse, por los órganos de la administración, como un proceso evolutivo que comprende cuatro fases:

a. Presencia. En esta fase se provee básicamente información del Servicio al ciudadano.

b. Interacción. Considera comunicaciones simples entre el Servicio y el ciudadano y la incorporación de esquemas de búsqueda básicas.

c. Transacción. Incluye provisión de transacciones electrónicas al ciudadano por parte del Servicio, en forma alternativa a la atención presencial en las dependencias del órgano.

d. Transformación. Considera cambios en los Servicios para proveer aquellas prestaciones que componen su misión crítica en forma electrónica, y la introducción de aplicaciones que administran la entrega de prestaciones a los ciudadanos.

4. En cuarto lugar, los Jefes de Servicio, tanto en los procesos de modernización que ejecuten, así como en los proyectos que utilicen tecnologías de información y comunicaciones, para concretar el desarrollo del Gobierno Electrónico en el Estado, deberán seguir las siguientes pautas, centradas en tres áreas.

5. La primera área es la relación de los Servicios con los ciudadanos. En este aspecto, deberán:

a. Introducir progresivamente el uso de tecnologías de información y comunicaciones en todos los procesos asociados a brindar prestaciones a los ciudadanos, debiendo considerar la interrelación que tengan con otras reparticiones públicas.

b. Fomentar y promover el acceso de los ciudadanos a los servicios e informaciones gubernamentales, mediante las tecnologías de información. Como medida para alcanzar este fin, deberán crear incentivos a los ciudadanos para el uso de estos medios, sin que esto se traduzca en una disminución de la calidad del servicio existente.

c. Proveer a los ciudadanos un servicio completo en función de sus necesidades, de modo que tengan un rol de atención directa al ciudadano. Para ello, deberán lograr su integración con aquellos que tengan un rol de trabajo y provisión interna de antecedentes.

d. Atender a los ciudadanos mediante ventanillas únicas, prefiriendo que, de ser posible, éstas sean desarrolladas y operadas por empresas privadas. Los proyectos que se diseñen y los procesos de licitación que se convoquen con motivo de lo anterior, deberán establecer exigencias en cuanto a fiabilidad, seguridad y velocidad; así como indicadores de calidad de servicio al ciudadano, utilización de estándares que aseguren compatibilidad, protección de bases de datos, privacidad en línea; y sistemas de monitoreo de la gestión a los ciudadanos.

e. Procurar que el uso de autorizaciones electrónicas en la relación entre el ciudadano y los Servicios, guarde relación directa con el nivel de seguridad que cada ciudadano aspira obtener o con aquél que la ley establezca para el caso.

6. La segunda área de trabajo del Gobierno Electrónico es el mejoramiento de la gestión y procesos internos y de la relación entre los Servicios. En esta área, los Jefes de Servicio deberán:

a. Mejorar la eficiencia operacional dentro de los Servicios, mediante el uso de las tecnologías de información y comunicación, simplificando y rediseñando los procesos que implementen.

b. Desarrollar programas continuos de enseñanza de las tecnologías de información a nivel de todas las plantas del Servicio. Estos programas deberán incluir metodologías de enseñanza provistos por medio del uso de tecnologías de información.

c. Contar con un sistema de información diseñado para apoyar las funciones internas y la atención a los ciudadanos, además de atender directamente a los sistemas de información de otras reparticiones públicas.

d. Propender a que los Servicios que tienen un rol de trabajo y provisión interna de antecedentes, puedan hacerlos accesibles en línea a todas las reparticiones de Gobierno que tengan un rol de atención directa al ciudadano, en aquello que sea pertinente de acuerdo a las respectivas competencias y responsabilidades.

Sin perjuicio de las redes propias que utilicen los Servicios, éstos deberán conectarse progresivamente con las otras instituciones mediante la red que administra el Ministerio del Interior. Aquellas instituciones que están directamente enlazadas, deberán estar en pleno funcionamiento en los próximos seis meses. El resto de los Servicios deberá estar enlazado en los próximos doce meses.

e. Instaurar, como una medida de gestión destinada a medir el avance del Gobierno Electrónico en cada Servicio, un indicador de periodicidad trimestral, que mida los porcentajes de trámites presenciales y electrónicos que han brindado los Servicios a los ciudadanos y a otras reparticiones públicas.

f. Mantener licenciados todos los productos de software que se utilicen en la Institución. Los Servicios serán autónomos para seleccionar y utilizar los productos de software que resuelvan más apropiadamente sus necesidades y que se ajusten a la realidad.

g. Desarrollar mecanismos que permitan, faciliten y promuevan al interior de su repartición, que las comunicaciones se efectúen preferentemente mediante tecnologías de información. De igual forma, las instituciones del Estado deberán ser las primeras en utilizar los servicios electrónicos que provea otra repartición pública.

h. Considerar, en el desarrollo de proyectos que utilicen tecnologías de información, el impacto en la organización y en el personal que podría producir dicho desarrollo. Para

ello, deberán incluir como parte de dichos proyectos, la detección y resolución de los efectos que provoca su aplicación. Especial énfasis deberán efectuar cuando dicho impacto involucre a los funcionarios de la institución.

i. Adoptar, progresivamente, estándares de la industria de tecnologías de información y comunicación, que permitan relacionar e interconectar distintos sistemas y diversas plataformas, de modo que sean abiertos y no propietarios.

j. Tender a presentar una imagen común en Internet. Para ello deberán, en un plazo no superior a los seis meses, adscribirse también a la utilización de los dominios gov.cl y gob.cl, en adición de aquellos que actualmente posean.

k. Promover la agregación de demanda para obtener mejores precios y condiciones de compra, como manera de hacer más eficiente el uso de los recursos financieros disponibles. Esta estrategia también será válida en la concreción de proyectos que utilicen tecnologías de información cuyo desarrollo no resulte factible para un único Servicio.

7. La tercera área de trabajo del Gobierno Electrónico es la profundización de la participación de los ciudadanos en los procesos políticos. En esta área, los Jefes de Servicio deberán:

a. Considerar y adoptar medidas tendientes a proporcionar a la ciudadanía la información pertinente, a la consideración de sus opiniones y sugerencias, así como a facilitar instancias de participación ciudadana y la transparencia.

b. Velar por el desarrollo de páginas web informativas de fácil acceso y comprensivas. Asimismo, deberán vincular esta información a portales de búsqueda generales, tanto del Gobierno como de privados, de manera de facilitar el acceso a la información.

8. En quinto lugar, corresponderá al Ministerio Secretaría General de Gobierno velar por los estándares de contenido de las páginas web de los diversos Ministerios y Servicios, asegurando el acceso de los ciudadanos a la información general y específica sobre la acción del gobierno.

9. En sexto lugar, el Ministerio de Hacienda deberá generar los antecedentes que permitan conocer el presupuesto de gasto e inversión en nuevas tecnologías de información y comunicaciones, que efectúe anualmente el Gobierno.

10. En séptimo lugar, el Ministerio Secretaría General de la Presidencia efectuará la coordinación y seguimiento del cumplimiento de las Instrucciones precedentes y de todas aquellas que se establezcan en el futuro en relación al desarrollo del Gobierno Electrónico.

11. Finalmente, los Servicios deberán presentar al Ministerio Secretaría General de la Presidencia, a más tardar el día 15 de Agosto del 2001, un plan que señale como aplicará el presente Instructivo en su Institución.
Saluda atentamente a Ud.,

Ricardo Lagos Escobar
Presidente de la República.

2) Régimen de los Bancos de Datos de Organismos Públicos.

La verdadera incidencia de la manipulación de datos por parte de entidades públicas o privadas, al parecer, no fue correctamente dimensionada sino hasta el advenimiento de la llamada "era de la información", donde la tecnología permitió que pudiera almacenarse toda clase de datos y, más aún, hizo posible que éstos se mantuvieran siempre conectados con la persona respecto de la cual provienen, sin importar el registro o base de datos en la cual se encuentren y el titular de la misma.

Ante esta tecnología y posibilidades que ella brinda, la informática ante el derecho presenta una variedad de enfoques, todos de gran trascendencia. Desde luego, un elemento que trae a colación es su directa relación con el poder, puesto que quien es dueño de la información es precisamente quien la controlará, usará según sus propias finalidades y, por ello, se encontrará en inmejorables condiciones de imponer su voluntad; y otro elemento que resulta por lo demás ser correlativo al ejercicio del poder descrito es aquel referido a los derechos de los individuos y los roces que surgen en la relación existente entre la protección de sus derechos, la privacidad de los datos que a aquél se refieren (se trata de la creación de un sistema de protección de datos) y el

derecho de los demás, de ser informados respecto de los datos registrados acerca de las personas.

Como vemos, en este tema poder y derechos fundamentales se encuentran en íntima imbricación, lo que al menos permite aventurar, a modo conclusivo, que cuando son los órganos del Estado los que detentan la información es el Derecho Público el instrumento adecuado para lograr de esta estrecha unión una articulación legítima en miras de propender al bien común y, por ende, al servicio a la persona humana. Este es el fin que justifica la acción del Estado, y que además, siendo su deber alcanzarlo, no le es posible excusar su ejercicio en cuanto existan los presupuestos para su actuación, lo que en este caso se da a todas luces.

De esta forma se advierte cómo ha sido posible que en el derecho de la Administración se encuentren temas cada vez más modernos o tecnológicos. En efecto, al menos en las fronteras del tema que ahora trataremos, normativamente se han implementado varias novedades, desde el uso de la firma digital y los documentos electrónicos por los órganos del Estado[124], la instalación de un portal de compras del Estado, hasta la definitiva protección legal de los datos de carácter personal, por la nueva Ley N° 19.628, sin omitir, desde luego, las importantes imposiciones de transparencia documental que, ahora como principio, se encarga de contemplar la Ley de Bases, luego de las modificaciones que le introdujera la llamada Ley de Probidad Administrativa[125]

En esta ley confluyen muchos aspectos relacionados con la protección de la persona, y es esta perspectiva desde la cual deben ser interpretadas sus normas; así también deben serlo aquellas otras contenidas en cuerpos legales o normativos distintos que afecten esta protección; es lo que sucede, por ejemplo, con el actual artículo 13 (antiguo 11 bis de la Ley 18.575), de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, precepto que faculta a los órganos del

[124] Al efecto, ver D.S. N° 81 (Segpres), de 10 de junio de 1999, pub. en Diario Oficial de 26 de junio de 1999, que regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado. De interés también D.S. N°5.996 (Interior), de 24 de septiembre de 1999, pub. en Diario Oficial de 12 de noviembre de 1999.

[125] Se trata de la Ley 19.653, de 14 de diciembre de 2000. Su Reglamento sobre el Secreto o Reserva de los Actos y documentos de la Administración del Estado, en D.S. N° 26 (Segpres), de 28 de enero de 2001, pub. en Diario Oficial de 7 de mayo del mismo año. En España, numerosa bibliografía sobre la materia ha sido desarrollada últimamente. De utilidad, El derecho a la intimidad y a la privacidad y las Administraciones Públicas, obra colectiva, director Domingo Bello Janeiro, Manuel Heredero, coordinador, Santiago de Compostela, 1999. En especial, Los derechos de la persona en el ámbito de las tecnologías de la información, de Eduardo Vilariño Pintos, pp. 17-0; La relación jurídica de disposición de datos de carácter personal, Francisco González Navarro, pp. 31-80, entre otros.

Estado para declarar ciertos actos bajo la condición o calidad de secretos, cuestión que pugna claramente con el derecho que asiste a los particulares en razón de la Ley 19.628 (sobre protección de datos personales), para conocer y requerir de la Administración los datos contenidos en registros públicos ya sean propios o de terceros en cuanto por su naturaleza y finalidad interesen para el desarrollo de ciertas actividades.

Sabido es que el legislador no puede ejercer su potestad en todas las materias. La actual Constitución innovó en la materia y restringió la dictación de leyes estableciendo el llamado dominio legal máximo, dicen algunos; es decir, se fija un límite al legislador, y se especifica en su texto cuándo es posible dictar leyes. En tal sentido, su artículo 60 dispone que sólo son materias de ley las siguientes. Con este imperativo se pretendió prohibir al legislador inmiscuirse en ámbitos respecto de los cuales no estaba expresamente autorizado por la misma Constitución.

Ante este enunciado, lo primero que cabe preguntarse es si las materias que contiene la Ley 19.628, sobre protección de datos personales, son, propiamente, materias de ley o, lo que es lo mismo, de dónde arranca la competencia del legislador para la presente regulación.

Desde luego, es evidente que esta competencia no se desprende explícitamente del mencionado artículo 60 de la Constitución, cuestión que pudiera llevar a la conclusión apresurada de que la materia no es propia de la ley; suerte que este postulado, bajo esta sola reflexión, no podría ser real, ello debido a que el pretendido propósito del dominio máximo que estatuye en su enunciado el artículo 60 de la Constitución, ya citado, tampoco lo es. El mismo artículo en su numeral 20 abrió la potestad legislativa de modo general a toda otra norma general y obligatoria que estatuya las bases esenciales de un ordenamiento jurídico y, además, porque la Constitución en muchas materias encarga directamente al legislador que las regule, en forma exclusiva y excluyente, como es el caso del ejercicio de los derechos fundamentales que se reconocen en el artículo 19, entre otros.

Debemos detenernos entonces en otras materias de ley que están y se cruzan preferentemente en toda la Constitución. Muchas de ellas, como lo hemos señalado, establecidas en el artículo 19. Dice allí que la Constitución asegura a todas las personas los derechos que en esa extensa norma se reconocen. Aquí hay dos tipos de normas, algunas que hacen referencia al legislador, vale decir, facultándolo para que éste precise la forma en que se debe desarrollar la actividad que constituye el derecho de que se trata

y, las otras, que contienen referencias directas a su regulación intrínseca, es decir, se refieren al contenido mismo del derecho.

Por ejemplo, las disposiciones del artículo 19 N° 11 inciso 4°, N° 12, N° 21, N° 24 señalan que tales actividades se realizan en conformidad a la ley. Asimismo, el N° 15 del mismo artículo prescribe sobre el derecho de asociación que las entidades que allí se reconocen deben "constituirse en conformidad a la ley". En cambio, el N° 24 inciso 2° señala que sólo la ley puede introducir el modo de adquirir, de manera tal que dicha definición conceptual de adquisición del derecho está entregada en plenitud al legislador.

Desde luego y por lo dicho, podemos afirmar que la Ley 19.628 no encuentra su fundamento o soporte en considerarla como una ley que regula una actividad económica en los términos que considera el artículo 19 N° 21 de la Carta, aunque así lo entiendan algunos esta conclusión es errónea. En efecto, este indicado precepto constitucional reconoce y asegura el derecho a desarrollar cualquiera actividad económica que no sea contraria a la moral, al orden público o a la seguridad nacional, respetando las normas legales que la regulen. Esta regulación, debemos admitirlo, no se refiere al ejercicio externo del derecho, lo que exigiría que la ley normara su ejercicio, sino que al contenido interno de la actividad en sí: v.gr. la actividad económica de distribución eléctrica, que aparece intensamente regulada por el legislador; la actividad económica que surge en el ámbito del servicio sanitario también resulta esencialmente regulada, desde el tipo societario que corresponde asumir al prestador hasta el minucioso detalle tarifario que el legislador traza para esta actividad. En aquellas legislaciones se definen normalmente y con detalle los contenidos internos del derecho y las restricciones y condiciones de ejercicio del mismo; en otras palabras, se definen los contenidos de la actividad económica que el legislador ha conceptualizado. De tal manera que las definiciones externas a este contenido no son propiamente preceptos legales que regulen una actividad económica.[126]

Una correcta apreciación de la fuente constitucional de la que emana su regulación legal parte por analizar el objeto de esta ley. Pues bien, ésta trata de la vida privada de las personas, garantía que está consagrada en el artículo 19 N° 4 de la Constitución, conclusión que se vislumbra prístina de su propia denominación:

[126] Sobre esta diferencia de aplicación del artículo 19 N° 21 y el contenido de la regulación, de suma utilidad Iván Aróstica Maldonado, Derecho Administrativo Santo Tomas; (Libre iniciativa privada y actividad empresarial del Estado),. Ed. (2001), en especial 71-86.

protección de la vida privada y, bien sabemos, que la vida privada ha sido tratada en dicho artículo. Pero, nuevamente, debemos poner en evidencia que en este numeral no hay referencia o convocatoria a la ley, de donde se sigue que la fuente de esta legislación, para su creador, está –lisa y llanamente- en una aplicación directa de la Constitución, puesto que el legislador no ha sido convocado mediante el clásico reenvío –técnica usual del constituyente del 80- puesto que particularmente respecto a este derecho la norma constitucional se satisface a sí misma, sin convites de ninguna especie.

En este punto conviene tener a la vista el artículo 19 N° 26 de la Constitución, el cual señala que los preceptos legales pueden regular garantías, pero también pueden "complementar garantías" y esta es, precisamente, una ley que complementa la garantía indicada.

Luego se está complementando un derecho. Complemento es añadir algo, ampliarlo, mejorarlo, por lo que a través de ella se trata de resguardar la vida privada de las personas a tal punto que sólo a las personas privadas, naturales. Todo su contenido ha sido para ampliar y mejorar el derecho garantido y de acá que, en estricto rigor, esta ley no es una ley que verse acerca de la pluralidad informativa, ni respecto de la transparencia de actos del Estado, sino que se refiere, exclusivamente, acerca de la persona, su personalidad y su privacidad.

Pero curiosamente la protección de la vida privada se rescata con un criterio de nimiedad. Se protege o amplía frente a datos personales y nos obnubilamos con referencias tales como lo "económico", lo "financiero", "lo bancario" y "lo comercial". Sin embargo, se olvida que esa información normalmente la tienen los particulares, y aún más que en estrictu senso ella es intrascendente para la libertad y vida de las personas, salvo por el acceso al crédito o la molestia de recibir cartas no deseadas en nuestro domicilio.

Estos elementos son francamente irrelevantes en la vida de las personas, pues el verdadero peligro está en el poder y la información personal que acerca de nosotros posee el Estado. Es normalmente el burócrata quien llega a nuestras profundas intimidades y ahí, curiosamente, se produce una suerte de ruptura respecto del criterio de bilateralidad que, al menos formalmente, se quiso enunciar en su tramitación de modo tal que, en rigor, esta ley omite desarrollar esta esfera de custodia que explicaría y fundamentaría, con creces, su dictación.

La Ley 19.628, sobre Protección de Datos de Carácter Personal, nos habla de registros o bases de datos, en ocasiones indistintamente, lo que nos lleva necesariamente a tener que indagar en torno a la actividad registral de la Administración.

Es un hecho cierto que el Estado es quien tiene la mayor cantidad de registros[127] de datos, son la propia naturaleza y finalidad de sus órganos los elementos que determinan que sean estos entes los que con mayor facilidad puedan recoger antecedentes relativos a las personas y por ende mantenerlos en archivos y registros, las más de las veces, además, unido al condicionante fundamental que significa el hecho de que para ejercer determinadas actividades deba en forma previa sindicarse y anotarse a la persona en Registros que lleva e impone la misma autoridad.

La ley habla, impropiamente, de registros o bases de datos como una expresión de sinonimia, aunque es evidente que ambos conceptos son distintos. Mientras la voz "registros" denota un conjunto organizado de datos de carácter personal, los "bancos de datos" imponen un concepto más especializado que comprende a un fondo común de datos, característica que comparte con los registros, pero que se diferencia de ellos porque son accesibles a varios usuarios. Es en este último sentido en el que parecen haber sido tomados los registros que se tratan en este cuerpo legal. Así por lo demás lo demuestra la práctica legal chilena.

Por su parte, los datos a los que se refieren estos registros o bases de datos han sido también incorrectamente conceptualizados. De esta manera la ley los agrupa bajo la nomenclatura "de datos de carácter personal" o sencillamente "datos personales"; enseguida, los define sin distinción como aquellos "relativos a cualquier información concerniente a personas naturales, identificadas o identificables", siendo que en doctrina son tratados separadamente, ya que, por un lado, no siempre los datos personales son datos de carácter personal, y así viceversa.

---

[127] Sólo por vía ilustrativa podemos señalar los siguientes: Registro Nacional de Servicios de Transporte de Pasajeros, Registro Internacional de Obras Audiovisuales y su Reglamento, Registro de Consultores del Ministerio de Planificación y Cooperación, Registro Nacional de Contratistas de Gendarmería de Chile, Registro de Consultores del Ministerio de Obras Públicas, Registro de Corredores, Registro Nacional de Contratistas de Trabajos Topográficos y Jurídicos, Registro de Productos Agropecuarios; Registro Nacio¬nal de Acuicultura, Registro Nacional de Condenas por Violencia Intrafamiliar, Registro Nacional de Condenas, Registro General de Contratistas de Carabineros de Chile, Registro Especial de Faltas por Tráfico ilícito de Estupefacientes y Sustancias Psicotrópi¬cas, Registro Nacional de Constructoras de Viviendas Sociales, Registro Nacional de Órganos Técnicos de Capacitación, Registro Nacional de Embarcaciones Artesanales, Registro Nacional de Subsidios Habitacionales, Registro de Afiliados a Juntas de Veci¬nos, Registro de Certificación de Exportación, Registro Nacional de Receptores de órganos, Registros de Producción Pecuaria, Registro Municipal de Carros y Remolques, Registro Nacional de Armas, Registro de los Contribuyentes, Registro Nacional de Telecomunicaciones, Registro de Naves y Artefactos Navales, Registro Nacional de Criadores y Engorderos Porcinos, etcétera.

En principio, los datos de carácter personal son de tres clases:

- Datos personales stricto sensu, que son los datos existenciales, en la medida en que (y sólo cuando) pueden ser asociados a una persona identificada o identificable; v.gr., nacimiento, muerte, estado civil, domicilio, etc.;

- Informaciones sobre cosas y bienes, lo que se revela en la ley con bastante amplitud y que constituye "cualquier información", y

- Ejercicio de determinadas actividades.

Sin embargo, esta enunciación no es comprensiva de todos los datos que es posible referir a una persona; así también pueden ser objeto de un registro o bases de datos, por ejemplo, la información numérica, alfabética, digital (huellas) o acústica, y en general toda aquella información que pueda ser recogida y almacenada.

Asimismo, mención aparte merecen los llamados datos sensibles, los que sí son propiamente datos personales, y en tal sentido son definidos por la ley como "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o síquicos y la vida sexual".

Desde otro punto de vista, el llamado dato de carácter personal puede ser de dos clases: dato accesible al público y dato no accesible al público; esta diferenciación nos revela un aspecto de la actividad registral, entendiendo por ella no el registro de las personas, sino que la incorporación de un grupo de personas, bienes o actividades a un instrumento que se va a llamar registro y que traduce una significativa circunstancia: dicha actividad no es, necesariamente, un camino de publicidad de información, sino que más bien puede ser de limitación o de regulación del derecho, mas no de transparencia de la gestión administrativa.

Lo anterior indica que la existencia de un registro público no traduce como equivalente significado que su contenido sea necesariamente público, sino que la denominación es identificatoria de una situación orgánica. Se trata, entonces, del órgano público que contiene o mantiene ese registro para el cual el acceso de los particulares a la información contenida en ellos es regulada por las normas particulares que rijan para

cada uno en particular, porque así lo exige el principio de competencia para el cual cada órgano tiene funciones propias y por ello cada registro que lleven ha de tener también una configuración peculiar y cumplir esa función específica, que, por de pronto, legitima su existencia. De allí que existan:

- Registros públicos-públicos;
- Registros públicos, con listado público que lo acompaña;
- Registros públicos, de acceso restringido, y
- Registros públicos, de acceso único o reservado.

Entendida de esta forma la denominación pública de los registros que ordena la Administración cabe desechar de plano una relación intrínseca entre su regulación (fundada en el ánimo de dar protección a la vida privada) y la publicidad y transparencia de la actuación del Estado, exigida por la Ley 18.575, de Bases Generales de la Administración del Estado.

En el seno mismo de la Comisión Constituyente se planteó la problemática descrita (información manejada por un órgano público), pero a raíz de otra discusión, que fue la de la garantía constitucional del artículo 19 N° 11, acerca de la libertad para informar y emitir opinión. En esa ocasión se criticó duramente el concepto propuesto para esa norma de "fuente accesible a todos". Se dijo que ella no podía entenderse genéricamente como aquellos documentos o fuentes de información que son públicos pues ese sentido era peligroso y por eso se intentó desestimar, ya por su amplitud, ya por la dudosa aplicación práctica que pudiese tener un mandato de esa naturaleza.

Sobre esas consideraciones, Alejandro Silva Bascuñán expuso ante la Comisión lo superfluo de tales justificaciones y solicitó el mantenimiento de la expresión, pues insistía en su aclaración de que aunque no existiera la obligación de informar, ella sí se plantea a los órganos públicos en relación con sus competencias, debido a que de otra manera se haría imposible el ejercicio de la libertad de opinión. En su parecer el legislador debía ser el encargado de establecer las situaciones en las que hay obligación de no informar, y a contrario sensu de lo anterior, respecto de los órganos públicos, viene el grado de esfera que les corresponde en la accesibilidad. Si se quita esta frase no existiría más influencia en la materia que la dada a los Tribunales de Justicia, cuestión del todo poco recomendable.

El sistema chileno actual de tratamiento de la información está fundamentalmente regulado en esta ley y en las normas dispersas que se le refieren[128].

Por su parte la Ley 18.575, sobre Bases Generales de La Administración del Estado, en los artículos 11, 11 bis y 11 ter –que le incorporara la Ley 19.653[129]–, los cuales presuponen los principios de transparencia y publicidad de los actos de la Administración y sus fundamentos tratan, asimismo, de la información que maneja la Administración y el deber de darla a conocer a quienes lo requieran, a menos que concurran ciertas causales de justificación que la releven de este mandato. De esta manera reconoce la posibilidad de que los órganos del Estado constituyan secretos o reservados ciertos actos cuestión que si observamos la Ley 19.268 comparten similares fundamentos en el caso de tratarse de actos que afecten a la persona en su vida privada y que por lo mismo sean secretos.

Ello se encuentra justificado por el artículo 6° de la Constitución, el que prescribe que en todo caso la Administración está sujeta directa y expresamente a la Constitución, y por ello, le corresponde a ella –y sus funcionarios– el deber de resguardar el ámbito de intimidad de aquellos terceros que le han proveído de datos e informaciones personales. De allí surge que, primeramente, existen los asuntos reservados por naturaleza, respecto de los cuales los funcionarios están en el deber de mantenerlos dentro de la esfera de intimidad que corresponde, de modo tal que si se vulnera este deber, aparte de las responsabilidades funcionarias que corresponden, el Estado está en el deber de reparar el daño que se ocasionare, por aplicación directa de los artículos 6° y 7°, en sus correspondientes incisos".

Además esta restricción a la publicidad encuentra su fundamento en la ley, ya que es sólo esta norma la que puede encargarse de establecer el secreto o la reserva de determinadas materias, y las autoridades administrativas podrán hacerlo sólo en cuanto hayan recibido el encargo del legislador para así disponerlo[130]. En algunos casos la ley

---

[128] En efecto, existen otras normas que antes sustentaban el tratamiento de la información por parte de los órganos del Estado, así la ley 18.834, Estatuto Administrativo, en su artículo 55 h) impone como obligación a cada funcionario "guardar secreto en los asuntos que revisten el carácter de reservados en virtud de la ley, del reglamento, de su naturaleza o por instrucciones especiales", por cierto que en esta parte fue bastante más generoso en la creación de medios de establecimiento de reserva que su antecesor, el DFL 338/60 que consignaba sólo a la naturaleza y a la instrucción como habilitantes de tal reserva. Por su parte el D.S. 291 de 15 de febrero de 1974 consignó que los documentos y oficios se clasificarán en secretos, reservados y ordinarios.

[129] DFL 1/19.653, de 13 de diciembre de 2000 y pub. en Diario Oficial de 17 de noviembre de 2001.

[130] Sobre las limitaciones a la publicidad conviene tener presente los dichos del profesor Silva Bascuñán (sesión 233, de 15.7.1976) en la Comisión de Estudios de la Nueva Constitución, "...en su opinión, el legislador ya tiene una serie de casos en los cuales está perfectamente establecido el derecho de no

impondrá la plena publicidad de un registro, siendo tal publicidad uno de los fines de la creación del mismo; en otros, se exigirá acreditar un interés, pero en todo caso se protegerá la intimidad y la vida privada del titular de esa información.

Es un hecho conocido que la Administración registra. Cabe preguntarse ¿cómo y cuándo establece registros? La búsqueda de la respuesta a estas interrogantes hace necesario indagar acerca de la actividad registral y el principio de legalidad, o lo que es lo mismo, cuál es la fuente de la actividad registral.

Hay un problema de sentido común: si la vida privada está garantizada en los términos del artículo 19 N° 4 de la Constitución, pareciera que al menos cuando la Administración se inmiscuye en lo que hace una persona, en lo que tiene o bien, quién es, sólo lo puede hacer a partir de una especial habilitación normativa, es decir, de una atribución, o lo que es igual de una potestad y, por ello, al menos en nuestro ordenamiento jurídico, por vocación expresa del principio de juridicidad[131], es siempre la ley la que debe considerar la creación del Registro.

Es innegable que esta regulación nace del ejercicio de una potestad y, siendo las potestades materia de ley al claro tenor del artículo 62 inciso 4° N° 2 de la Constitución, en relación con el artículo 7° de la misma, esta habilitación orgánica se fundamenta, innegablemente, en el principio de competencia. Este poder jurídico, además, tiene una finalidad la cual está dada por el artículo 19 N° 4 de la Constitución. En efecto, es la protección de la persona respecto de sus datos personales como corolario del derecho constitucional al respeto de la vida privada el contenido garantístico que justifica la expresa y previa habilitación de la ley en el tema que nos ocupa.

Por su parte la existencia de un registro público se justifica por la existencia de cierta información que, referida a la persona, es manejada porque así lo implica la naturaleza del órgano del Estado que la tenga, o bien porque es de utilidad para el cumplimiento de los fines o funciones de dicho órgano, el que dentro de su competencia atesora estos datos. La especialidad de esta información está en el hecho de que ella en

---

informar: toda la esfera de lo que corresponda a la reserva y al secreto, que está en la Constitución y en las leyes. De manera, entonces, que no hay problema alguno en cuanto a que vaya a quedar en descubierto toda racionalidad por falta del encargo del legislador. Se trata, precisamente, de permitir a este que en el futuro establezca, por norma expresa y dentro de los valores que constitucionalmente se consignaran, las reglas que podrían impedir la información. A su juicio, es muy importante que sea el legislador quien asuma esta tarea. Se sabe que, para negar en concreto esta información, debe existir una determinada autoridad o persona que niegue la información y esa está basada en la ley".

[131] Eduardo Soto Kloss, su Derecho Administrativo, Bases Fundamentales, Principio de Juridicidad, t. II, 1' edición; Editorial Jurídica de Chile, 1996.

sí dista de ser un elemento carente de contenido por la particular esencialidad que les da su titular, y que por ello su uso o recopilación no debiera ser dejado a la discrecionalidad de un ente, del que bien sabemos está a su servicio, y no es dueño de mandar por sí mismo lo que le plazca saber de las personas.

El aspecto más importante de estos registros privados es el vínculo obligacional que se da entre el responsable del registro y el titular de los datos proporcionados; en este caso también le compete al responsable el deber de mantener reserva de los datos que le han sido confiados, y de la misma forma, manejarlos y administrarlos de conformidad a lo convenido. Estos temas necesitan también de regulación toda vez que, aun cuando exista un principio de voluntad o consentimiento en ello, es la misma garantía constitucional la que se compromete, y que por tanto debe ser protegida ante abusos de particulares.

De esta forma reconocemos solamente registros creados por ley o por la convención, de conformidad a la ley.

En cuanto se ha producido una numerosa regulación legal que establece registros, es evidente que el legislador está yendo más allá de ese dominio máximo legal que hoy día se pregona. Efectivamente, lo que está ocurriendo es que se está reconociendo desde el punto de vista de las atribuciones, es decir, desde el punto de vista de las potestades, que la obligatoriedad particular del desarrollo de una actividad registral que implica la transferencia o incorporación de ciertos datos que son propios a la persona humana (derecho subjetivo) involucra necesariamente una relación entre los artículos 62 inciso 4° N° 2 y 19 N° 4 de la Constitución. Si dicha incorporación resulta obligatoria, dicha potestad sólo puede encontrar abrigo en la ley.

Un punto distinto son las bases de datos. Hemos ya señalado que en estricto rigor la acepción registro y bases de datos son diferentes. Estas últimas son la información que recaba la Administración para el funcionamiento de ella misma, la que puede ser objeto de tratamiento, esto es, de cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal o utilizarlos de cualquier otra forma.

Reconozcamos, desde ya, que al tenor del artículo 20 de la Ley 19.628, el tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse

respecto de las materias de su competencia y con sujeción a las reglas que la misma ley establece. En esas condiciones no necesitará consentimiento de su titular. Así las cosas, al tenor de la ley, las bases de datos se pueden crear por el propio desarrollo de la actividad propia del ente. No obstante, aunque la ley no lo diga, es menester hacer presente que las leyes se han referido expresamente autorizando su creación, v.gr., Ley 19.212, que crea la Oficina de Informaciones.

Ahora si la ley ha debido incorporar esta autorización legal es porque de una u otra manera sigue la idea de la expresa y previa habilitación legal, trátase como hemos dicho de potestades que se crean y que se pueden ejercer. A este respecto, la historia fidedigna del establecimiento de esta ley, en particular de este artículo 20, señala que se consideró como criterio de legitimación del tratamiento de datos la competencia del órgano que pretenda llevar estas bases y, que en relación a la habilitación legal, se optó por desechar el principio de especialidad, bastando la autorización legal otorgada en términos generales.

En este sentido se dijo: "La primera parte de este artículo, que deja sujeto el tratamiento de datos personales por parte de un organismo público a aquellos que se refieran su competencia, encuentra su origen en el artículo 6 de la H. Cámara de Diputados, que establecía que el tratamiento de datos "sólo será admisible cuando sea indispensable para el cumplimiento de las tareas que les corresponden y dentro del ámbito de su competencia", y en el artículo 19, N° 1 del texto preparado durante el tercer trámite constitucional, conforme al cual "el tratamiento de datos debe efectuarse dentro del ámbito de la competencia legalmente determinado del respectivo organismo". Se añadía: "Si bien es una norma que puede estimarse innecesaria, al tenor del artículo 7° de la Constitución Política, presta utilidad su inclusión en un cuerpo legal que por primera vez da reglas en forma sistemática de los datos personales, más aún si se considera que numerosos organismos públicos tiene solamente normas de carácter reglamentario sobre la materia o, incluso, ni siquiera de esa jerarquía".

Enseguida, se hizo referencia al tema de la legalidad de las bases de datos, aceptándose una pretendida competencia implícita de la Administración para ello, echando por tierra el principio de especialidad en la materia, de esta manera se dijo que: "La tercera parte del artículo 20, al expresar que, en esas condiciones, no se necesita el consentimiento del titular para tratar sus datos personales, se inclina por el predicamento del artículo 6 de la H. Cámara de Diputados, en orden a que los distintos organismos públicos pueden tener todos los registros o bancos de datos personales que

sean necesarios para el cumplimiento de sus funciones. Se desecha, de esa forma, la exigencia adicional planteada en el texto del tercer trámite constitucional, en cuanto a que, además de la habilitación legal general para realizar su cometido, cada organismo público requiriese otra, específica, que le permitiese organizar y mantener bancos de datos personales. Entendió la Comisión Mixta y los señores representantes del Ejecutivo que la existencia de un registro general de bancos de datos personales del sector público, prevista en artículo 22 de la misma proposición del Ejecutivo, así como los diferentes derechos sustantivos y mecanismos procesales que consulta este cuerpo legal, son suficiente garantía para las personas frente a los actos que la Administración realice en esta materia".

Son numerosas las críticas que se le pueden hacer a la postura del legislador, especialmente en lo que se refiere al debido complemento de la garantía constitucional del artículo 19 N° 4 de la Constitución, el cual se ve palmariamente afectado en cuanto por esta normación se permite la intromisión amplia de la Administración en la vida privada de las personas. Al desechar el principio de especialidad de la ley en la creación de bases de datos y dejar su legitimidad casi en manos del principio de competencia, el cual es medido según el órgano de la Administración que realice el tratamiento de datos, se deja un marco de discrecionalidad confiando sólo en la buena fe del órgano (se dice para el cumplimiento de sus funciones).

La ley 19.628, sobre Protección de Datos Personales, al definir el concepto de tratamiento de datos incluye dentro de las formas que puede revestir dicho tratamiento el de la cesión de datos, la que se define como la transferencia de los datos desde una base de datos a otra distinta. En efecto, posteriormente, la ley trata de la cesión de datos en los registros privados o convencionales, mas respecto de la Administración no hace referencia legal alguna, más que someterla en esta regulación a las normas contenidas en "las reglas precedentes".

Sin embargo, y considerando el extenso análisis al principio de legalidad, no es posible suponer que los órganos del Estado que realicen el tratamiento de datos puedan cederlos a su discreción; es más, resulta forzoso concluir que la referida cesión sólo se podrá efectuar cuando la ley expresamente lo habilite para ello[132]. En esto hay razones de legalidad y de competencia.

[132] En este sentido Contraloría General de la República no ha tenido un criterio estable. Así en dictamen 2.267 de 1998 ha señalado que el Convenio celebrado entre la Dirección del Trabajo y la Sociedad Dicom

Esto implica, por una parte, que el Estado –la Administración (y cualquiera de sus integrantes– no puede realizar aquellos actos mercantiles que supone la cesión o venta de esta información, puesto que la ley en comento ni siquiera tiene el rango que habilita tal actividad para las personas jurídicas de derecho público y, además, porque dicho actuar por parte de los órganos del Estado importaría, lisa y llanamente, el ejercicio de potestades de las que en verdad carecen, máxime cuando ellas sólo explicarían su fin en razón de la protección de la intimidad y la vida privada de las personas.

En definitiva, son cuatro los criterios a los que se debe atender para desechar la referida pretensión: legalidad, especialidad, intimidad y el del precedente legal[133].

En segundo lugar, en lo que respeta al problema de la petición de los datos que se puede hacer a la Administración, conviene hacer una distinción básica, puesto que se podrán solicitar datos referidos a uno mismo o bien que sean de terceros y respecto de los cuales se tiene algún interés.

Es el primer supuesto el que en este estudio merece nuestra atención. La Ley 19.628 trata en el Título II "De los derechos de los titulares de datos", en éste se reconoce el derecho a la información y al acceso a ella por parte de las personas a cuyos datos se refieren las bases o registros, otorgando varias posibilidades relacionadas con ello, v.gr., cancelación, modificación, eliminación, etc.

La historia fidedigna de este Título señala que el H. Senado durante el tercer trámite constitucional, en su sugerencia de texto para el artículo 12, diferenció con mayor precisión las distintas situaciones que pueden darse en relación a dichos datos, esto es, la eliminación, la modificación y el bloqueo de datos; suprimió la limitación al denominado "derecho de acceso", y reglamentó el aviso de la cancelación y la

---

S.A., según el cual la referida Dirección envía a la sociedad la información contenida en el boletín de infractores a la legislación laboral y previsional, quien se encarga de procesarla computacionalmente a fin de elaborar y actualizar una base de datos, que contiene íntegramente el indicado boletín, se enmarca dentro de la órbita de competencia del señalado servicio. Ello porque el mencionado convenio no impone a ese organismo público ninguna obligación de exclusividad para Dicom S.A., en cuanto a la entrega de la información contenida en el boletín, en la forma convenida con la indicada empresa, ya que persigue el mejor cumplimiento de la función pública que desarrolla la Dirección del Trabajo, información que no reviste, además, el carácter de secreta o reservada. En este caso, se trata de un convenio de prestación de servicios en cuya virtud un órgano del Estado le encomienda a una entidad privada procesar computacionalmente determinada información, sin costo alguno para éste, ya que el beneficio que obtiene la contraparte consiste en utilizar esa información en el desarrollo propio de las actividades de su giro.

[133] Así lo dispone la misma Constitución en el artículo 60 N° 10 al exigir que toda enajenación de bienes del Estado se realice por ley; el artículo 55 letra h), tampoco permite la disposición de datos por parte de los funcionarios que los manejen.

modificación a los terceros a quienes se hubiese comunicado previamente los datos personales respectivos.

Propuso, al efecto, señalar que toda persona tiene derecho a exigir a quien sea responsable de un banco de datos que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

Por su parte en la H. Comisión Mixta consideró también otro punto que fue la concordancia del procedimiento de solicitud de información, rectificación, etc., que por esta ley se establece con el proyecto (en ese momento) de Ley sobre Probidad Administrativa, especialmente en lo que respecta a las causales de denegación de la información de los datos requeridos.

De esta manera es el artículo 15 de la misma ley el encargado de imponer restricciones al ejercicio de este derecho, señalando "No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las labores fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional".

Claro está que esta negativa se debe sujetar a lo prescrito por la ley y en caso de que no sea así el afectado puede recurrir a la Justicia de conformidad al procedimiento previsto en el artículo 16 de la misma ley.

Por todo lo anteriormente dicho, podemos concluir que los registros o bases de datos son, indudablemente, materia de ley. Es innegable que en cuanto la información que en ellos esté contenida se refiera a la persona humana, particularmente a su vida privada, se encuentra comprometida en su regulación, entonces, la garantía constitucional del artículo 19 N° 4 de la Constitución; y considerando que por mandato del constituyente estos derechos fundamentales son siempre materia de ley (artículos 60 N° 20, 61 inc. 2°, 62 N° 2 inciso 4°), no corresponde que estos registros sean creados por otra norma que no sea la de fuente legal.

Pero, además, sólo pueden tratarse datos personales cuando la ley lo autorice. Se requiere por tanto de ese marco autorizatorio. Ahí sí que hay un criterio de especialidad; no basta entonces acudir al criterio de competencia general ni para el registro, ni para el

tratamiento de datos. En ambos casos se requiere, por parte del Estado, ley especial, ya que la propia Ley 19.628 hoy lo exige en múltiples de sus disposiciones que hacen referencia directa siempre a la fuente legal.

3) Privacidad de la Información Pública y el Derecho a su acceso.

Basado en el principio fundamental de transparencia de los órganos del Estado (que consiste en permitir y promover el conocimiento de los procedimientos, contenidos y fundamentos de las decisiones que tales órganos adopten), a través del derecho de acceso a la información pública se reconoce el deber de publicidad de los actos y documentos de los órganos de la Administración; y la obligación de estos órganos de responder a los requerimientos de información de los ciudadanos.

Desde el punto de vista normativo, para algunos la consolidación de este derecho, como derecho subjetivo o personal, surge como consecuencia de la incorporación en la Declaración Universal de Derechos Humanos, en el año 1948, del derecho a la libertad de opinión y de expresión y del derecho a manifestar y a expresar libremente las ideas, conocidos en conjunto y universalmente como derecho a la información. Este derecho es recogido también en la Convención Americana de Derechos Humanos y en la Convención Europea de Derechos Humanos. Para otros, el derecho de acceso a la información pública tiene un carácter colectivo, pues considera la transparencia y publicidad como un bien público o social, y en ese sentido resulta ser un derecho básico de la democracia y un instrumento de control y participación ciudadana.

En Chile, la Ley N° 19.653 sobre probidad administrativa de 1999 modificó la Ley orgánica constitucional de bases generales de la administración del Estado, para establecer el derecho de acceso a la información pública por parte de los ciudadanos y regulando un procedimiento para hacer efectivo dicho derecho en caso de negativa por parte del servicio público requerido.

Sin embargo, de acuerdo a la misma normativa, se exceptúan de esta publicidad los actos administrativos, documentos y antecedentes declarados secretos o reservados conforme a las normas sobre este tipo de documentos, los cuales mantendrán dicho carácter durante el plazo de 20 años.

En virtud de las normas del reglamento, las autoridades administrativas del país han dictado una diversidad de resoluciones y decretos declarando la reserva o secreto de actos y documentos sobre materias tan objetables, en la perspectiva del derecho de acceso que la ley protege, como los resultados de auditorias internas, los procesos de licitación, las denuncias presentadas por los usuarios ante los servicios públicos, los contratos de prestación de servicios a honorarios, y en algunos casos hasta las remuneraciones del personal. Al respecto, la Contraloría General de la República recientemente se pronunció declarando la ilegalidad de muchas de estas resoluciones por cuanto infringían el principio de transparencia resguardado en la ley.

En el mismo sentido, diversas voces de la sociedad civil organizada se han manifestado en contra de esta cultura del secretismo que aún insisten en cultivar los servicios públicos. Para ello han utilizado el procedimiento establecido en la propia ley e incluso han recurrido a tribunales internacionales para obtener acceso a la información denegada. Es así como se presentó, en septiembre de 2000, el primer recurso de amparo de acceso a la información, luego que la Corporación Nacional Forestal (CONAF) no respondiera a una solicitud de información hecha por la Fundación Terram, organismo no gubernamental (ONG). Posteriormente el recurso ha sido utilizado en contadas ocasiones por particulares y organizaciones ambientalistas con resultados variables, que no indican un tendencia definida de los tribunales. Los organismos requeridos han sido también diversos, entre estos se cuentan el Banco Central de Chile, varias superintendencias, ministerios y el Servicio Nacional de Aduanas.

Los cambios para revertir esta tendencia de secretismo ya se han echado a andar. Las recientes reformas a la Constitución de 1980 introdujeron un nuevo artículo 8°, que dice: "Son públicos los actos y resoluciones de los órganos del Estado, así como sus fundamentos y los procedimientos que utilicen. Sin embargo, sólo una ley de quórum calificado podrá establecer la reserva o secreto de aquéllos o de éstos, cuando la publicidad afectare el debido cumplimiento de las funciones de dichos órganos, los derechos de las personas, la seguridad de la Nación o el interés nacional".

I. Ley nº 19.653

La Ley Nº 19.653[134], de 1999, sobre Probidad Administrativa aplicable a los órganos de la Administración del Estado, modificatoria de la Ley Nº 18.575, Orgánica

[134] EL DFL 1/19.653 Texto refundido de la Ley 18.575 sobre Bases Generales de la Administración del Estado.

Constitucional de Bases Generales de la Administración del Estado, incorpora expresamente disposiciones que reconocen la publicidad de los actos administrativos de los órganos de la Administración, y los documentos que le sirven de sustento o complemento; y la obligación de los jefes de servicios de responder a los requerimientos de información de los ciudadanos, estableciendo incluso un plazo para ello.

Sin embargo, se puede afirmar, siguiendo al profesor Fernández González[135], que la publicidad de los actos de los órganos del Estado, de sus fundamentos, de los documentos que les sirven de base y de los procedimientos que involucran, es un principio de rango constitucional, que la Ley Nº 19.653 vino a refrendar en el ámbito legal, y que permite en definitiva darle concreción o aplicación al derecho.

Siendo un principio fundamental es o debe ser rector de los actos de los órganos estatales, y debe tener como consecuencia el principio de transparencia, definido por la Ley Nº 19.653 como aquel que consiste en "permitir y promover el conocimiento de los procedimientos, contenidos y fundamentos de las decisiones que se adopten"[136].

Para la consulta de los actos y documentos que se encuentran a disposición permanente del público, el reglamento de la ley, obliga a cada servicio a mantener un índice o registro actualizado en las oficinas de información o atención del público usuario de la Administración del Estado, establecidas en el decreto supremo Nº 680, de 1990, del Ministerio del Interior.

El índice o registro se formará con los actos y documentos dictados o emanados de cada servicio dentro del ámbito de su competencia, los que se incorporarán a él desde la fecha de su publicación.

Cada Jefe Superior de Servicio establecerá la forma y contenido del índice o registro, el que en todo caso deberá consignar los siguientes datos mínimos: Individualización del acto o documento, señalando su naturaleza, identificación o numeración y la fecha de su emisión, y la fecha y lugar de la publicación del acto o documento.

Se exceptúan de esta publicidad los actos administrativos, documentos y antecedentes declarados secretos o reservados de conformidad a las normas del reglamento, sin perjuicio de lo establecido en leyes o reglamentos especiales. Éstos mantendrán dicho carácter durante el plazo de 20 años, a menos que con antelación a

[135] FERNANDEZ GONZALEZ, Miguel Ángel. El Principio de Publicidad Administrativa. Editorial ConoSur Ltda. Santiago de Chile, 2000. Págs. 730 a 742.
[136] Artículo 11 bis inciso 2º de la Ley 18.575, agregado por la ley Nº 19.653.

dicho plazo el respectivo Jefe de Servicio, mediante resolución fundada, los excluya de tal categoría.

Se entiende que están obligados por esta norma, los órganos de la Administración del Estado, que de acuerdo con la misma ley, está constituida por los Ministerios, las Intendencias, las Gobernaciones y los órganos y servicios públicos creados para el cumplimiento de la función administrativa, incluidos la Contraloría General de la República, el Banco Central, las Fuerzas Armadas y las Fuerzas de Orden y Seguridad Pública, los Gobiernos Regionales, las Municipalidades y las empresas públicas creadas por ley. Respecto del Congreso Nacional, la ley N° 19.653, incorporó el artículo 5° A en la Ley Orgánica de esta Institución por el cual dispuso:

"Los diputados y senadores ejercerán sus funciones con pleno respeto de los principios de probidad y transparencia, en los términos que señalen la Constitución Política, esta ley orgánica constitucional y los reglamentos de ambas Cámaras.

El principio de probidad consiste en observar una conducta parlamentaria intachable y un desempeño honesto y leal de la función, con preeminencia del interés general sobre el particular.

El principio de transparencia consiste en permitir y promover el conocimiento de los procedimientos, contenidos y fundamentos de las decisiones que se adopte".

Al respecto, durante la discusión, se estableció que "el desarrollo de los principios de probidad y transparencia queda encomendado, en su detalle, a los reglamentos de ambas Cámaras, los cuales podrán optar por consagrarlos en un cuerpo reglamentario separado, tal como un Código de Ética Parlamentaria, o por incorporar las normas pertinentes en sus actuales reglamentos, que ya contemplan algunas de ellas.

Por ejemplo, en materia de transparencia existen normas sobre discusiones y votaciones secretas, que podrán mantenerse, si se concluye que no afectan a esos principios, o modificarse, si se estima más apropiado para una mejor aplicación de ellos y no se afecta algún otro bien jurídico que también sea preciso proteger".

- Causales de Excepción Informativa

En la Ley Nº 18.575, se incorpora por la Ley de Probidad, un nuevo artículo que contempla una serie de causales para denegar la entrega de los documentos o antecedentes requeridos a un órgano público.

Estas causales son las siguientes:

1. Reserva o secreto establecido en disposiciones legales o reglamentarias

Entre otras materias, esta causal incluye el denominado secreto y reserva bancario, que se encuentra regulado en el artículo 154 de la Ley General de Bancos. No obstante, la norma deja abierta la puerta a la imposición de restricciones al acceso a la información, por la autoridad administrativa.

De acuerdo a lo establecido en esta disposición, se dictó en el año 2001, el reglamento sobre secreto o reserva de los actos y documentos de la administración del Estado, en el cual se dispone que la declaración de secreto o reserva, basada en la protección de intereses públicos, procederá respecto de los siguientes actos y documentos: Los relativos a la defensa y seguridad nacional; los relativos a la política exterior o las relaciones internacionales; los relativos a la política monetaria y divisas; aquellos cuya comunicación pueda perjudicar a la moneda y al crédito público; los relativos al mantenimiento del orden público y la prevención y represión de la criminalidad; aquellos cuya comunicación o conocimiento perjudique el desarrollo de procedimientos jurisdiccionales o de actuaciones preliminares o preparativas de aquellos que la ley encomiende a organismos de la Administración; aquellos cuya comunicación o conocimiento perjudique la investigación por los servicios públicos competentes, de los delitos y las infracciones administrativas, tributarias o aduaneras; aquellos cuyo conocimiento actual pueda impedir u obstaculizar gravemente el ejercicio de la acción administrativa del órgano administrativo requerido; y la correspondencia oficial debidamente calificada por la autoridad responsable de conformidad a lo dispuesto en el DS N° 291 de 1974 del Ministerio del Interior.

El mismo reglamento, agrega que la declaración de secreto o reserva, basada en la protección de intereses privados, procederá respecto de los siguientes actos y documentos: Los de carácter nominativo, es decir, que conlleven o contengan una apreciación de juicio o valor sobre una persona determinada o claramente identificable; aquellos cuya comunicación o conocimiento afecte la vida privada de una persona individualizada o identificable; los expedientes relativos a procedimientos sancionatorios o disciplinarios de cualquier naturaleza, solo respecto de terceros ajenos a dichos procedimientos; los expedientes médicos y sanitarios; y los que contengan o se refieran a secretos industriales y comerciales, incluyendo los procedimientos de fabricación, las informaciones económicas y financieras y las estrategias comerciales.

Expuestas estas causales, resulta evidente que la cultura del secretismo se impuso, burlando el principio constitucional y legal de transparencia, ampliando el

ámbito de discrecionalidad para la declaración de secreto por la autoridad administrativa a actos y documentos que resultan discutibles por el alcance que pudiera dárseles.

Confirma la falencia de la norma, las más de 80 resoluciones y decretos dictados por autoridades administrativas declarando la reserva o secreto de actos y documentos que obran en su poder.

Entre las materias a las que se ha aplicado la restricción figuran fundamentalmente los resultados de auditorias internas, los procesos de licitación, la correspondencia oficial, las denuncias contra el servicios presentadas ante el propio servicio, los contratos de prestación de servicios a honorarios, y en algunos casos hasta las remuneraciones del personal.

2. Afección de las funciones de los órganos públicos requeridos

El establecimiento de esta causal resulta paradojal si se compara con el debate parlamentario y texto definitivo aprobado por la Comisión Mixta del Congreso Nacional, respecto de la Ley Nº 19.628, sobre protección de la vida privada. En dicha oportunidad se restringió la excepción exclusivamente a las funciones fiscalizadoras, y no a cualquier otro caso. Más incomprensible aún resulta, si observamos la historia fidedigna del establecimiento del precepto analizado, en la que se señaló expresamente que "estas limitaciones implican una desventaja muy grande, ya que su vaguedad o generalidad hacen imposible dar cumplimiento a la publicidad de las correspondientes actuaciones. Una autoridad podrá reclamar de que la publicidad entorpece su función".

3. Oposición de los terceros a quienes se refiere o afecta la información

4. Que se afecte sensiblemente los derechos o intereses de terceras personas, según calificación fundada efectuada por el jefe superior del servicio.

Estamos en ambas situaciones confrontados a un conflicto de bienes jurídicos: por un lado el derecho a acceso a información y por otro la protección de la vida privada, conflicto que ya habíamos enunciado. Sin embargo, resulta extraña la facultad entregada al jefe superior del servicio requerido quien puede negar la información a los requirentes fundando su negativa en la afección de derechos o intereses sensibles de los terceros, aún cuando éstos no se opongan. La calidad de sensibles se define en la Ley de Protección de la Vida Privada. Esta facultad, otorgada a un jefe de servicio, viene a dificultar una vez más el acceso a información pública.

5. Que la publicidad afecte la seguridad de la Nación o el interés nacional.

- Procedimiento de Amparo

En la norma sobre probidad, se establece un procedimiento de amparo para recurrir en caso que la entrega de la documentación no se realice, y se invoque una causal distinta a la seguridad de la Nación o el interés nacional, que contempla un procedimiento especial. La sentencia dictada en estos procedimientos, puede ordenar la entrega de los documentos e información requerida, señalando el plazo para hacerlo, y además aplicar una multa al jefe de servicio.

En virtud de estas normas, que entraron en vigencia en diciembre de 1999, se presentó en septiembre de 2000 el primer recurso de amparo de acceso a la información, luego que la Corporación Nacional Forestal (CONAF) no respondiera a una solicitud de información hecha por la Fundación Terram, organismo no gubernamental (ONG).

Este recurso fue acogido. Posteriormente el recurso ha sido utilizado en contadas ocasiones por particulares y organizaciones ambientalistas con resultados variables, que no indican un tendencia definida de los tribunales. Los organismos requeridos han sido también diversos, entre estos se cuentan el Banco Central de Chile, varias Superintendencias, Ministerios y el Servicio Nacional de Aduanas.

II. Ley N° 19.880

La Ley N° 19.880, de 2003, que establece las bases de los procedimientos administrativos de los órganos de la Administración del Estado, vino a complementar las disposiciones contenidas en la ley de probidad, específicamente referidas a la publicidad y transparencia en materia de procedimiento y tramitación de los actos administrativos, otorgando el derecho al ciudadano de conocer el estado en que se encuentran las actuaciones solicitadas a un órgano público, los resultados y estableciendo plazos breves y el denominado silencio administrativo positivo como regla general[137].

El artículo 16 de esta norma consagra el principio de transparencia y publicidad, al disponer “el procedimiento administrativo se realizará con transparencia, de manera que permita y promueva su conocimiento, contenidos y fundamentos en las decisiones

[137] Se entiende por silencio administrativo positivo el resultado positivo para el peticionario de la solicitud presentada a la autoridad si ésta no da su respuesta dentro de los plazos establecidos en la ley.

que se adopten en él. En consecuencia, salvo las excepciones establecidas por la ley o el reglamento, son públicos los actos administrativos de los órganos de la Administración del Estado y los documentos que sirvan de sustento o complemento directo o esencial".

En el artículo 17 se establece el derecho de las personas a conocer en cualquier momento el estado de tramitación de los procedimientos en los que tengan la condición de interesados y obtener copias autorizadas de los documentos que rolan en el expediente y la devolución de los originales, salvo que por mandato de la ley o reglamentario, éstos deben ser acompañados. Se establece también el derecho de las personas a acceder a los actos administrativos y sus documentos, y a obtener información acerca de los procedimientos jurídicos o técnicos que las disposiciones vigentes impongan a los proyectos, actuaciones o solicitudes que se propongan realizar.
Respecto de la obligación de publicación, la nueva norma legal dispone en el artículo 48, que deberán publicarse en el Diario Oficial los actos administrativos que contengan normas de general aplicación o que miren al interés general, los que interesen a un número indeterminado de personas, los que afectaren a personas cuyo paradero fuere ignorado, los que ordenare publicar el Presidente de la República, y los actos respecto de los cuales la ley ordenare especialmente este trámite

Análisis crítico del marco legal chileno

• Hay consenso, en la autoridad pública, que una materia tan relevante debió ser regulada como cuerpo normativo independiente y no mediante disposiciones agregadas en otras legislaciones. Chile se merece una ley de acceso a la información pública, que recoja los principios, conceptos y procedimientos que hagan efectiva la protección y aplicación de este derecho en nuestro ordenamiento.

• Las normas existentes, no definen qué debe entenderse por información pública, ni consagra una definición amplia de organismo y/o autoridad pública que permita delimitar el ámbito de aplicación de la ley.

• Un régimen legal moderno sobre la materia, no puede entregar una facultad tan amplia para declarar secreto o reservado un acto o documento público a los respectivos jefes de servicios, como lo hace la norma revisada. Analizada en nuestro ordenamiento, tal

• La norma analizada restringe igualmente el ejercicio del derecho a la información, por cuanto exige requisitos más bien formales para pedir documentos públicos, lo que impide en la práctica el acceso a gran parte de los archivos en poder de los órganos públicos.

En definitiva, si bien con el Principio de Publicidad de los actos estatales, recogido la ley sobre probidad administrativa y en la ley sobre procedimientos administrativos, se buscó garantizar el acceso a la información, la aplicación de la misma no otorga garantías de la celeridad y oportunidad con que dicha información puede ser obtenida, ni los medios que deberán poner en marcha los organismos para proveerla, de modo que efectivamente haya acceso para todos. El recurso de amparo no está al alcance de aquellos a quienes se les niega información, y las sanciones, de escasa fuerza, no logran persuadir a quienes incumplen la norma, a revertir su conducta.

4) Nuevo Sistema Nacional de Registros de ADN v/s privacidad

Antes de comenzar a hablar sobre el nuevos Sistema Nacional de Registros de ADN debemos reflexionar en torno a lo que significa el ADN, el establecimiento de verdaderos "Bancos de ADN" y su regulación en Chile.

En primer lugar debemos señalar que pocas noticias científicas han tenido tanta y tan vasta difusión en el planeta como son las relativas a las tecnologías de ADN y su punta de lanza conocida como "Proyecto Genoma Humano", iniciativa emblemática de la comunidad científica internacional que pretende descubrir la secuencia completa del ADN de los seres humanos (y que lo logró en abril del año 2003 con el apoyo de la empresa privada Celera Genomics), para luego encontrar su localización precisa dentro de cada cromosoma y así estudiar la relación entre las distintas partes de la secuencia y las características genéticas de las personas.

El camino para alcanzar estos fines no sólo ha implicado el espectacular posicionamiento de la biología molecular como disciplina, si no que también ha significado el desarrollo de las tecnologías de la información, las que ahora no sólo

trabajan combinadamente, si no que han caminado progresivamente a "la disolución de las fronteras entre la biología (lo natural) y las máquinas (lo artificial)", ello por que "la revolución de la información se desarrolla al mismo tiempo que la revolución de la ingeniería genética, cuyo descendiente es la biotecnología". Las consecuencias de estos progresos son insospechados hasta hoy día, por lo que siempre requerirán la atención permanente de la sociedad civil, sobre todo si consideramos que dramáticos hechos del siglo XX evidenciaron que la ciencia no es neutral ni aséptica respecto del medio en que se desarrolla.

Pero abordando derechamente el fondo del asunto que nos ocupa debemos preguntarnos, ¿qué es el ADN?. La respuesta nos indica que básicamente el ADN o ácido desoxirribonucleico es un conjunto de moléculas en las cuales está consignada toda la información genética de un ser vivo, es decir, de los animales y las plantas, y se encuentra replicada en todas y cada una de las células de los organismos[138].

El ADN está compuesto por una sucesión de moléculas, también llamadas bases nitrogenadas, unidas entre sí por azúcares y fosfatos a manera de esqueleto, formando una secuencia continua de bases las cuales solamente son cuatro: ADENINA, TIMINA, CITOSINA y GUANINA (a las cuales se les identifica por sus respectivas iniciales, esto es, A, T, C, y G), las que se combinan y recombinan sucesivamente hasta conformar los aproximadamente 30.000 genes del ser humano (cada gen tiene un largo variable que va de miles a millones de pares de bases nitrogenadas), los cuales "constituyen la unidad física y funcional de la herencia", en el decir del profesor ROMEO CASABONA, la cual se transmite de padres a hijos gracias a las características propias del ADN, como es su carácter único e inequívoco[139], su permanencia e inalterabilidad (normalmente no varía a lo largo de la vida del individuo), su indestructibilidad (salvo supuestos de destrucción total del cuerpo, e.g., por incineración), y su carácter de constituir información no voluntaria.

De lo dicho se deduce claramente la importancia que tienen los perfiles de ADN como sistema infalible de identificación, pues las características, como son su transmisibilidad hereditaria (procede en partes iguales de su padre y madre, lo que

[138] Estas explicaciones preliminares están basadas fundamentalmente en los capítulos introductorios de las obras de Carlos María ROMEO CASABONA, Los Genes y sus Leyes. Editorial Comares, Granada,2002, y de Juan Miguel MORA SÁNCHEZ, Aspectos Sustantivos y Procesales de la Tecnología del ADN Edit Comares y Cátedra de Derecho y Genoma Humano, Bilbao – Granada, 2001.

[139] Estadísticamente la probabilidad de que dos personas tengan un mismo código genético es de una entre 50 trillones, al igual que con las huellas dactilares, de acuerdo al "Draft Recommendation on the use of analyses of DNA within the framework of the criminal justice system and Draft Explanatory Morandum", Consejo de Europa, Estrasburgo, 1991,pág. 9.

determina su superioridad como método de individualización respecto de otros tipos de huellas), su universalidad (se encuentra presente en el ADN de todas las células) y, por supuesto, que se trata claramente de un mecanismo privilegiado de identificación, con todas las implicancias sociales, económicas, jurídicas y políticas que ello conlleva.

Quizás éste sea uno de los temas que en forma más intuitiva y efectiva se ha traducido en una reacción internacional con un posicionamiento público relevante, aun cuando podría ser sólo la expresión del temor o la desconfianza que generan estas cuestiones entre la ciudadanía, sobre todo al considerar las regresiones democráticas de los últimos años (aguzadas por las amenazas reales o imaginarias del terrorismo) que han llevado a exacerbar el rol de los Estados en el control social directo e indirecto y el desarrollo de un ingente poder de observación por las corporaciones privadas.

En definitiva, asistimos a una época en que la información genética es un bien muy codiciado por diversos entes, quienes consideran estos datos como claves de sus procesos de toma de decisiones.

Tal es el caso de las compañías de seguro, empresas químicas y farmacéuticas, empresas de colocaciones, empleadores en general y, desde luego, del principal tenedor de datos del país: el Estado.

Especialmente de claro ha sido al respecto WHITAKER, quién ha dicho:

Los augurios respecto del control gubernamental de las bases de datos se hacen aún más sombríos con el desarrollo cada vez más importante de conexiones mediante interfaz con el sector privado, lo que conlleva diversas transferencias de datos. Ericsson y Haggerty, por ejemplo, concluyen, tras su investigación sobre la institución policial, que la cantidad de información que entra en sus bases de datos, así como la velocidad de acceso a las mismas, han transformado su naturaleza: de ser uno de los servicios más reservados del gobierno ha pasado a convertirse, gracias a las nuevas tecnologías, en un servicio de información para instituciones como las compañías de seguros, las mutuas de salud u otros servicios de asistencia social. El interés común que comparten tanto la policía como estas organizaciones privadas consiste en la eliminación del riesgo.[140]

- Perfiles de ADN y protección de datos personales

[140] WHITAKER, op. cit, pág. 159

En la actualidad, los sistemas informáticos son hábiles para el tratamiento automatizado de la información, tanto textual como de imágenes y sonido, en volúmenes que hasta hace muy poco tiempo no parecían posibles. Esto ha permitido la creación de grandes ficheros estructurados en que se almacenan dichos documentos, los que son susceptibles de ser relacionados y consultados fácilmente a través de procedimientos específicos. Por supuesto, esta es la lógica que está detrás de las bases de datos de ADN o, más específicamente, las bases de datos de perfiles de ADN, las cuales son promovidas por el Estado con miras de investigación criminal, búsqueda de personas desaparecidas e identificación general para efectos civiles (e.g. reconocimiento de paternidad).

Conforme a los estatutos jurídicos generalmente reconocidos, las huellas de ADN son datos personales y esa consideración nos impone analizar de acuerdo a esa naturaleza los mecanismos de protección que se han previsto por la normativa a su respecto; ello nos permitirá una adecuada calificación de los datos de ADN dentro de las distintas categorías de datos, para luego determinar quiénes pueden tratar información de este tipo con finalidades de investigación e identificación y cómo sería lícito realizar estas operaciones.

En efecto, el estatuto jurídico de protección de datos personales es un tema presente e inevitable de ser considerado al momento de decidir sobre la construcción de una base de datos de perfiles de ADN. Los principios y normas que rigen la materia necesariamente la informarán, e incluso influenciarán o determinarán su forma y contenidos.

No en vano el Tribunal Constitucional, en el caso de España, en sentencia 292/2000 de 30 de noviembre, precisó expresamente que son datos sujetos al derecho fundamental a la protección de datos:

Todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquiera otra índole, o que sirvan para cualquiera otra utilidad que en determinadas circunstancias constituyan una amenaza para el individuo.

No cabe duda que los datos de perfiles de ADN cumplen sobradamente con este requisito, pues su tratamiento permite entre otros males la concreción de las más atávicas amenazas del Estado totalitario que, traducidas a un lenguaje de estilo gangsteril cinematográfico, son equivalentes a decir:

"Sabemos quién eres, qué es lo que has hecho, qué es lo que haces y dónde has estado. Y, por supuesto, sabemos quiénes son tu familia".

En todo caso, a pesar de esta espada de Damocles, estamos ciertos que en la Sociedad de la Información no es posible cerrar las puertas al tratamiento de este tipo de datos, pues como nos recuerda el profesor SAARENPÄÄ:

No, no podemos manejarnos sin disponer de datos personales. Estamos acostumbrarnos a usar diferentes formas de identificación, desde nuestro nombre o una imagen hasta diversos identificadores biométricos. Usamos estas formas de identificación para comprobar nuestra identidad y permitirnos ser identificados en diferentes situaciones.[141]

Por ende, es y será la identificación el elemento que nos permite tomar una posición en el desarrollo de las cosas y de los hombres.

- Alcances al estatuto jurídico del perfil de ADN en cuanto dato personal

Por supuesto que el punto de partida de este análisis será la consideración que "dato" es aquel antecedente o noticia primera que permite investigar acerca de la verdad de un hecho; y "personal" será cualquier antecedente o noticia que proporcione información acerca de las circunstancias de una persona.

Así lo ha recogido el legislador comunitario, cuando la Directiva 95/46/CE, del Parlamento Europeo, dispone que es dato personal: "Toda información sobre una persona física identificada o identificable"[142].

Como podemos apreciar, el concepto considera dato personal a "toda información"; por tanto se trata de un concepto amplio, que no discrimina los datos por su naturaleza ni por el soporte en el cual consta. Abarca tanto imagen, sonido, o conjuntos de caracteres grafológicos y/o numéricos, debiendo tenerse presente que pueden manifestarse por distintos medios y adoptar diversas formas de representación. Esto es importante de tener en cuenta al examinar lo referido a los datos de perfiles de ADN, por cuanto en primer lugar podemos sostener a priori que son datos personales, y en segundo lugar, que pueden constar en distintos soportes.

[141] Ahti SAARENPÄÄ, "Europa y la Protección de Datos Personales" en Revista Chilena de Derecho Informático n° 3, editada y publicada por el Centro de Estudios en Derecho Informático de la Universidad de Chile. Santiago de Chile, 2003, pág. 15.
[142] Artículo 2 a) de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, publicada en el Diario Oficial de la Comunidad Europea de 23 de Noviembre de 1995.

Ahora bien, aun cuando constituye una máxima generalmente aceptada que los datos de carácter personal deben ser objeto de un régimen de garantías en tanto son necesarios para la protección de la persona, no todo dato goza del mismo nivel de protección. En efecto, conforme a la normativa, la doctrina y la jurisprudencia, estos son susceptibles de una clasificación a partir de sus condiciones de las mayores o menores posibilidades de afectación de las garantías fundamentales comprometidas.

Es así como dentro de los datos de carácter personal se ha establecido un orden de prelación, que va desde datos públicos o irrelevantes, hasta datos "sensibles" o especialmente protegidos, previéndose para cada uno de estos tipos un régimen de protección diferenciado.

De esta manera, cada uno de ellos ocupará un lugar en el orden de prelación atendiendo principalmente a su naturaleza y aptitud para vulnerar, mediante su difusión, los derechos fundamentales objeto de la protección. Dicho de otra forma, para determinar la ubicación que corresponde a cada tipo de dato de carácter personal dentro de dicha escala deberemos atender al grado de riesgo de vulneración de derechos fundamentales que el tratamiento de esos datos lleva implícito.

De esta manera, y siguiendo el criterio antes enunciado, se reconocen las siguientes categorías de datos de carácter personal, a saber:

En primer lugar los datos públicos, que son aquellos que "de acuerdo con el valor que les atribuye la conciencia social, son conocidos por cualquiera"[143]. Se caracterizan porque son comúnmente conocidos por la generalidad de las personas o, al menos son fácilmente accesibles por encontrarse en registros públicos de libre acceso, tales como guías telefónicas. Originalmente también se les denominó "datos irrelevantes", pero actualmente se tiene plena conciencia de que no hay datos personales irrelevantes, pues por escasa importancia que parezca tener un dato individualmente considerado, al relacionarlos con otros suelen adquirir un valor trascendental.[144]

En contraposición a los anteriores, los datos sensibles son aquellos que conforme al valor que les asigna la conciencia social, "solamente serán conocidos o por voluntad del titular o en circunstancias especiales y tasadas por las leyes". Estos datos se refieren

[143] Miguel Ángel DAVARA RODRÍGUEZ, Manual de Derecho Informático, 3ª edición. Editorial Aranzadi, Navarra, 2001, pág. 55.

[144] Así lo reconoce expresamente la famosa sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983, que se pronuncia sobre la inconstitucionalidad de la ley de Censo y da lugar al Recht auf informationelle Selbstbestimmung (derecho a la autodeterminación informativa); fue traducida al castellano por Manuel Daranas y se encuentra publicada en el Boletín de Jurisprudencia Constitucional Nº 33 de las Cortes Generales. Madrid, 1984, págs.126 a 170.

a cuestiones especialmente delicadas, directamente vinculadas al núcleo de la personalidad y dignidad humana, que incluso pueden inducir a decisiones discriminatorias a su respecto o cuya revelación constituirá una lesión a su intimidad, propia imagen, honor, libertad sindical, etc. Es por esto que se les engloba dentro de la categoría de "especialmente protegidos", en cuanto el legislador es extremadamente cuidadoso al momento de señalar los procedimientos y limitaciones en su tratamiento. Siendo así la Directiva en principio prohíbe su tratamiento, salvo circunstancias específicas que se exigen como condición legitimante del tratamiento de datos personales, e.g., el consentimiento del interesado.

Y aquí se inicia el problema, pues una cuestión tan relevante como si una secuencia alfanumérica que identifica inequívocamente a una persona respecto de toda la humanidad es un dato público o sensible, no está del todo resuelta.

Ahora bien, y considerando lo antes expuesto, claramente podemos preguntárnos ¿qué opinan organismos internacionales respecto al ADN y la privacidad de los datos que ella conlleva?

Frente a esta interrogante nos encontramos con la Declaración Internacional de la UNESCO sobre los Datos Genéticos Humanos. Esta Declaración fue aprobada, por unanimidad y por aclamación, por la 32ª sesión de la Conferencia General de la UNESCO, el 16 de octubre de 2003 y principalmente nos dice:

“Artículo 1: Objetivos y alcance

a) Los objetivos de la presente Declaración son: velar por el respeto de la dignidad humana y la protección de los derechos humanos y las libertades fundamentales en la recolección, el tratamiento, la utilización y la conservación de los datos genéticos humanos, los datos proteómicos humanos y las muestras biológicas de las que esos datos provengan, en adelante denominadas “muestras biológicas”, atendiendo a los imperativos de igualdad, justicia y solidaridad y a la vez prestando la debida consideración a la libertad de pensamiento y de expresión, comprendida la libertad de investigación; establecer los principios por los que deberían guiarse los Estados para elaborar sus legislaciones y políticas sobre estos temas; y sentar las bases para que las instituciones y personas interesadas dispongan de pautas sobre prácticas idóneas en estos ámbitos.

b) La recolección, el tratamiento, la utilización y la conservación de datos genéticos y datos proteómicos humanos y de muestras biológicas deberán ser compatibles con el derecho internacional relativo a los derechos humanos.

c) Las disposiciones de la presente Declaración se aplicarán a la recolección, el tratamiento, la utilización y la conservación de datos genéticos, datos proteómicos humanos y muestras biológicas, excepto cuando se trate de la investigación, el descubrimiento y el enjuiciamiento de delitos penales o de pruebas de determinación de parentesco, que estarán sujetos a la legislación interna que sea compatible con el derecho internacional relativo a los derechos humanos."

Por otro lado y relativo a privacidad, el artículo 14 nos dice:

"Artículo 14: Privacidad y confidencialidad

a) Los Estados deberían esforzarse por proteger la privacidad de las personas y la confidencialidad de los datos genéticos humanos asociados con una persona, una familia o, en su caso, un grupo identificables, de conformidad con el derecho interno compatible con el derecho internacional relativo a los derechos humanos.

b) Los datos genéticos humanos, los datos proteómicos humanos y las muestras biológicas asociados con una persona identificable no deberían ser dados a conocer ni puestos a disposición de terceros, en particular de empleadores, compañías de seguros, establecimientos de enseñanza y familiares de la persona en cuestión, salvo por una razón importante de interés público en los restringidos casos previstos en el derecho interno compatible con el derecho internacional relativo a los derechos humanos o cuando se haya obtenido el consentimiento previo, libre, informado y expreso de esa persona, siempre que éste sea conforme al derecho interno y al derecho internacional relativo a los derechos humanos. Debería protegerse la privacidad de toda persona que participe en un estudio en que se utilicen datos genéticos humanos, datos proteómicos humanos o muestras biológicas, y esos datos deberían revestir carácter confidencial."

Existen actualmente empresas que ofrecen el servicio de determinación de ADN sobre todo en lo relativo al parentesco y paternidad. Conjuntamente se han formado agrupaciones de clínicas especializadas que mantienen verdaderas bases de datos y bancos de ADN para efectos de mantener un código genético de una persona determinada o tienen ADN de personas anónimas para efectos de investigación universitaria y estudios.

En este caso tenemos a una empresa, en cuya declaración se servicios señala[145]:

"Nuestro servicio de banco de ADN provee a las organizaciones y a las personas particulares la tranquilidad de conciencia que se deriva de saber que sus muestras de ADN están almacenadas en un ambiente seguro y altamente protegido. El ADN almacenado puede ser usado para futuras pruebas de ADN, como por ejemplo:

* Para protegerse contra reclamaciones ilegítimas sobre el patrimonio de una persona.

* Para proveer un estándar de comparación e identificación de personas en profesiones de alto riesgo, tales como hombres y mujeres en la fuerza militar, bomberos, y contratistas en el exterior.

* Para ayudar en la identificación de personas extraviadas o dar pistas sobre el rastro de un ser querido.

* Para identificar rasgos hereditarios, tales como enfermedades genéticas y otras características físicas.

El ADN almacenado proporciona una historia genética que tendrá una importancia vital en la medida en la que el rompecabezas genómico se completa. El ADN de un padre anciano podría un día proveer pistas sobre enfermedades hereditarias y otros aspectos genéticos. En el futuro cercano, este tipo de conocimiento sobre el árbol genealógico podría salvar vidas con probada eficacia.

Nuestros servicios son completamente confidenciales. Únicamente revelamos información relacionada al ADN almacenado a las personas que usted autorice. Existen cuatro opciones de servicio de donde usted puede escoger:

* Banco de ADN con Cadena de Custodia

* Banco y Perfil de ADN con Cadena de Custodia

* Banco de ADN Privado

* Banco y Perfil de ADN Privado

- Banco de ADN con Cadena de Custodia

En el Banco de ADN con Cadena de Custodia, las muestras de ADN son tomadas y almacenadas usando un proceso que asegura que las Cortes y otras Agencias de gobierno considerarán los resultados de cualquier futura Prueba de ADN realizado en el ADN almacenado.

[145] La empresa en cuestión es el Centro de Diagnósticos de ADN (DDC), es el más grande y más experimentado laboratorio privado de Pruebas de ADN. DDC realiza 3 de cada 4 pruebas privadas de paternidad en los Estados Unidos y es el proveedor de pruebas para más de 600 socios afiliados en 168 países. Se puede visitar su página web en http://www.paternidad.com

De conformidad con los procedimientos de la Cadena de Custodia, profesional capacitado tomará su muestra de ADN. Su cita para la toma de muestra de ADN será programada en un hospital o laboratorio cerca de usted. Una vez ingresada en el Banco de ADN, le entregaremos un certificado del banco indicando el periodo de almacenamiento (15 años), los nombres de las personas que usted autorice a retirar o usar sus muestras, y otra información importante.

El costo de almacenamiento en el Banco de ADN es de $145. Este valor incluye la coordinación de la cita, la toma y transportación de la muestra, la verificación de la presencia de ADN en la muestra, y el almacenamiento por 15 años.

- Banco y Perfil de ADN con Cadena de Custodia

Nuestro servicio de banco y perfil de ADN permite a las personas almacenar sus muestras de ADN en un lugar seguro y protegido, y obtener un registro de su perfil genético. Realizamos una prueba de ADN sobre las muestras usando marcadores para 16 loci, incluyendo los 13 loci del CODIS que son reconocidos a nivel mundial como los estándares para las pruebas de identidad humana.

- Banco y Perfil de ADN Privado

En ocasiones, los clientes solicitan nuestros servicios de Banco y Perfil de ADN Privado, en cuyo caso ellos toman sus propias muestras en la privacidad de su hogar. Los servicios privados no siguen ningún proceso de Cadena de Custodia durante la toma de la muestra, y los resultados de las pruebas de ADN no podrán ser aceptados para trámites legales. Este servicio es para aquellos que requieren el banco y perfil de ADN únicamente por razones personales.

Usted puede optar por Banco de ADN Privado solamente o Banco y Perfil de ADN Privado. Le haremos llegar un equipo de toma de ADN que contiene todo lo que usted necesita para tomar su propia muestra de ADN usando hisopos bucales. Envíenos la muestra tomada, y nosotros almacenaremos su ADN en un paquete especialmente sellado por 15 años en un ambiente seguro. Usted recibirá un certificado del banco indicando el periodo de almacenamiento, los nombres de las personas que usted autoriza a recibir sus muestras, y otra información importante.

El costo del Banco Privado de ADN es de $50. Este valor incluye el Equipo de Toma de Muestra de ADN, los costos de envío y el almacenamiento por 15 años. Si usted escoge el Banco y Perfil de ADN privado, realizaremos un test de ADN en las muestras usando marcadores para 16 loci, incluyendo los 13 loci del CODIS que son econocidos a nivel mundial como estándares para las pruebas de identidad humana. El costo del Banco y Perfil de ADN privado es $195."

- Registro de ADN y Legislación Chilena.

El 6 de octubre de 2004 fue publicada en el Diario Oficial la Ley N° 19.970[146], que crea el Sistema Nacional de Registros de ADN.

Dicho sistema existe con objeto de apoyar investigaciones criminales, por lo que su constitución y mantención obedecerán estrictamente a ese propósito. Contiene registros alfanuméricos de huellas genéticas obtenidas durante procedimientos de investigación policial y tiene (en teoría) sólo función identificatoria de individuos.

El sistema está integrado por cinco tipos de registro:

* Registro de Condenados: Contiene las huellas genéticas de los condenados por los delitos de: aborto, violación, estupro, homicidio, secuestro, robo con violencia, amenazas, lesiones, adulteración de medicamentos, incendio, diseminación de gérmenes patógenos, delitos terroristas, narcotráfico, entre otros.

Las huellas genéticas de los condenados permanecerán en el registro aun cuando sus antecedentes penales hayan sido eliminados por vías legales.

* Registro de Imputados: Contiene las huellas genéticas de quienes hayan sido imputados en alguno de los delitos mencionados. Este registro es temporal: la huella específica será borrada una vez finalizado el proceso judicial o trasladada al Registro de Condenados si la persona es declarada culpable.

* Registro de Evidencias y Antecedentes: Conserva las huellas genéticas de personas no identificadas que sean obtenidas en el curso de una investigación criminal.

* Registro de Víctimas: Contiene las huellas genéticas de víctimas de los delitos mencionados, siempre y cuando exista consentimiento para ello de parte de la persona involucrada. También estas huellas serán eliminadas al finalizar el proceso judicial.

[146] La ley se encuentra agregada en el capítulo IX de la presente memoria.

* Registro de Desaparecidos y sus Familiares: Contiene las huellas genéticas de restos humanos no identificados, material biológico que provenga de personas presuntamente extraviadas y de personas que accedan voluntariamente a dar una muestra de ADN para facilitar la identificación de algún familiar extraviado.

El Servicio Médico Legal es el encargado de obtener las huellas genéticas a partir de las muestras biológicas que surjan en la investigación criminal y de alimentar el registro. Su administración y custodia serán responsabilidad del Servicio de Registro Civil e Identificación. Ambas entidades estarán obligadas además a mantener reserva de la información que se pueda obtener de las muestras, que además se consideran datos sensibles de sus titulares de acuerdo a la Ley N° 19.628 sobre protección de la vida privada.

Para implementar el sistema, el SML debió incorporar un poderoso software denominado CODIS (Sistema Índice de ADN Combinado, por su sigla en inglés), el cual fue traído desde EE.UU. e instalado por agentes de la Oficina Federal de Investigaciones (Federal Bureau of Investigation, FBI), que viajaron especialmente a Chile para esta misión.

Asimismo, el computador que contiene la base de datos está protegido por un riguroso sistema de seguridad, con el fin de que sólo personal autorizado pueda acceder o modificar la información contenida en el servidor.

El costo de todo el sistema, más el proceso de capacitación para los especialistas, significó una inversión que superó los 800 millones de pesos y se enmarca en las 20 medidas gubernamentales antidelincuencia, que fueron aprobados por mayoría en el Congreso Nacional en el mes de mayo de 2004.

La información del registro sólo puede ser consultada directamente por el Ministerio Público y los tribunales. La policía y los abogados defensores pueden también acceder a la información, pero necesitan permiso del ministerio y de la corte.

La ley también detalla los procedimientos para la administración del registro, cómo debe obtenerse e ingresarse la información genética, qué requisitos se deben cumplir para eliminar información y las sanciones para quienes divulguen datos o rompan la confidencialidad del registro, sanciones que consisten en multas y presidio.

Este proyecto ingresó al Senado el 8 de enero de 2002 y finalizó su tramitación en agosto de 2004.

El sistema, que es utilizado hace varios años en países como Estados Unidos, Alemania y Canadá, consiste en mantener una base de datos virtual con toda la

información genética de las personas que han sido detenidas y condenadas por algún delito. De esta forma, si es que se llega a presentar un nuevo caso, la policía podrá comparar las pistas obtenidas en el sitio del suceso con los datos disponibles y determinar de forma más rápida a los posibles culpables.

En 1995 se realizó por primera vez un peritaje de este tipo. En esa oportunidad se comparó el ADN extraído de la sangre encontrada en las ropas de un imputado y se pudo establecer una probabilidad de 96,4% que el flujo correspondía a la víctima. A partir de ese estudio, la demanda aumentó paulatinamente hasta el 2000, año en que comenzó a implementarse la Reforma Procesal Penal. Esta contribuyó a un importante aumento en la realización de esta prueba.

Como dato podemos decir además que el Servicio Médico Legal (SML) de Chile viene aplicando técnicas de análisis de ADN, al crear en 1991 la Unidad de Biología Molecular, de cobertura nacional, que utilizaba técnicas manuales de análisis que permitían trabajar un máximo de seis muestras diarias.

En noviembre del 2000 se inauguró el laboratorio de Biología Molecular y Genética del SML, con tecnología automatizada de última generación, con tres analizadores y secuenciadores genéticos, que pueden procesar 80 muestras diariamente, con un grado de confiabilidad del 99,9% de sus resultados.

Durante el 2001, entre otras pericias, realizó 2 mil 300 identificaciones de paternidad por orden de los tribunales de justicia. Hasta abril del año 2002 había realizado 430.

En 1998 se comenzó a formar un Banco de Muestras Biológicas de familiares de la línea materna de detenidos desaparecidos para su identificación a través de la secuenciación mitocondrial.

A partir del 2000, con una inversión cercana al millón y medio de dólares, el SML adquirió la tecnología necesaria para iniciar el trabajo de secuenciación mitocondrial, que se destina preferentemente a la identificación de detenidos desaparecidos.

Frente a esta ley y analizándola en forma somera, podemos comentar que ya en su artículo 3º menciona que “La información contenida en el Sistema y, en particular, las muestras biológicas y las huellas genéticas, se considerarán datos sensibles de sus titulares, según lo dispuesto en la ley Nº19.628, sobre protección de la vida privada…”

por tanto hace aplicables en principio las facultades y derechos que posee una persona frente al tratamiento de sus datos.

Decimos en principios, pues contrastando ambas leyes, claramente existe una gran limitación para el titular del ADN. En primer lugar el artículo 4º nos indica "El Sistema estará integrado por el Registro de Condenados, el Registro de Imputados, el Registro de Evidencias y Antecedentes, el Registro de Víctimas y el Registro de Desaparecidos y sus Familiares." Por tanto solo aquellas personas que participaran en alguna de las hipótesis de acción establecidas por el legislador serán ingresados sus datos.

Por un lado vemos que el ingreso de sus datos sensibles para algunos es completamente voluntario y requiere de su autorización expresa (como en el caso de Registro de Víctimas y el registro de Desaparecidos y sus Familiares), autorización tácita (Registro de Evidencias y Antecedentes, en caso de obtención de personas no identificadas) e incluso en forma obligatoria, aunque no exista autorización (como en el caso de Registro de Condenados).

Otro punto a considerar es el tiempo durante el cual estarán disponibles en los registros los datos sensibles. Hay una diferenciación al igual de los casos antes mencionados, encontrando situaciones que la ley exige que una vez cumplido el procedimiento sean eliminados los datos. Asi el artículo 18 reza: "Las huellas genéticas contenidas en los Registros de Imputados y de Víctimas, serán eliminadas una vez que se hubiere puesto término al procedimiento criminal respectivo." En cuanto al registro de condenados, el artículo 5º inciso 2º dice "La eliminación de los antecedentes contenidos en el prontuario penal, realizada en conformidad a la ley y a los reglamentos correspondientes, no implicará la eliminación de la huella genética contenida en el Registro de que trata este artículo".

Lo novedoso de esta ley es que establece distintas responsabilidades de acuerdo al actuar de las personas que intervienen en este Registro.

Asi, se establece:

- una responsabilidad administrativa para los funcionarios que, debiendo proceder a la destrucción del material biológico, no lo hicieren.
- Una responsabilidad penal por ejemplo en caso del que alterare las muestras biológicas que debieren ser objeto del examen de ADN; falseare el resultado de dichos exámenes o la determinación de la huella genética; faltare a la verdad en el informe pericial de examen o cotejo, o adulterare su contenido.

- Una responsabilidad civil que, a simple vista no se encuentra expresamente señalada, pero la podemos inferir claramente del artículo 22 que nos dice que Serán aplicables, en cuanto no se opusieren a lo previsto en esta ley, las normas contempladas en la ley Nº 19.628 sobre protección de la vida privada. Por tanto esta sería nuestra fundamentación para demandar civilmente en caso de perjuicios por el uso indebido de la información contenida en estos registros.

- Bancos de Datos Internacionales

Ahora bien, respecto de la situación de Registros y Bancos de Datos de ADN en otros países, podemos señalar que por ejemplo Gran Bretaña ha comenzado ya a recopilar ADN e información médica de cientos de británicos para realizar un base de datos genética a nivel nacional. Después de varias pruebas piloto, el proyecto empezará a funcionar a pleno rendimiento en 2006, para cuando se prevé disponer de información de medio millón de ciudadanos.

Esta biblioteca genética recogerá y analizará las muestras de 500.000 voluntarios mayores de 30 años. La base de datos, avalada por el Gobierno británico, podría ayudar a los investigadores a entender de qué manera los genes, el estilo de vida y el medio ambiente desencadenan enfermedades como el cáncer.

El objetivo de esta primera fase es determinar el funcionamiento de los centros que atenderán a los participantes que deseen ofrecer su ADN a la ciencia. Los voluntarios tendrán que responder unas cuestiones sobre su estilo de vida en una pantalla táctil y serán sometidos a análisis de la presión sanguínea, la función pulmonar, o el peso entre otros.

La idea no es nueva: Suecia e Islandia ya han recopilado una cantidad similar de datos durante años, y otros países, como Estados Unidos, están patrocinando estudios de menor envergadura en pacientes con cáncer o enfermedades como la diabetes o la esquizofrenia.

A pesar de este fin académico, defensores de los derechos de las personas, sobre todo lo realtivo a privacidad e intimidad creen que la proliferación de este tipo de organismos tare consigo un grave peligro frente a la manipulación no autorizada de los datos allí registrados.

Frente a lo mismo han surgido leyes que han regulado su funcionamiento, como en el caso de Chile que acabámos de revisar, siendo pues, nuestro país, el primer país en

Latinoamérica en contar con una legislación acorde al tema, sin embargo En Estados Unidos, las pruebas genéticas en procesos judiciales se utilizaron por primera vez en 1986 y en el Reino Unido en 1987. Actualmente esta práctica es aceptada en casi todos los países del mundo.

Ahora bien, otros países se han sumado a esta necesidad de regular lo relativo al ADN y tenemos el caso, por ejemplo de Puerto Rico que por Ley Núm. 527 de 29 de septiembre de 2004 crea la llamada Ley del Banco de Datos de ADN de Puerto Rico.

En caso de Panamá Según la Ley 80 de 1998 –que crea la base de datos de ADN– las muestras de DNA serían colectadas entre todos los integrantes de la Fuerza Pública (15 mil en total); de las detenciones preventivas (un promedio de 4 mil al año); de la población penal (8 mil 500 el primer año y otros 4 mil anuales) y de 4 mil 500 muestras "para investigaciones criminales"; los extranjeros que pidan permisos de trabajo; los que soliciten la ciudadanía y residencia (2 mil al año); los empleados de las agencias de seguridad (7 mil el primer año y 700 en los siguientes); todos los que soliciten permiso de armas (2 mil al año) o que lo renueven (7 mil 650).

La situación de España fue regulada a partir de La ley 23.511, que crea el Banco de Datos Genéticos para determinar y esclarecer conflictos relativos a filiación, que funciona en el Hospital Carlos Durand, establece en el art. 8 que los registros y asientos se conservarán de modo inviolable.

5) Intervención del Estado contra la privacidad en los Países Desarrollados.

- Las pruebas de ADN

Un edificio de oficinas en Edimburgo alberga actualmente uno de los más extraordinarios episodios de la antigua lucha entre la intimidad individual y el poder del Estado. Ahí, en la sede central de la Lothian and Borders Police, se está archivando sistemáticamente el ADN de la población local.

Durante los últimos dos años, cada persona arrestada o detenida por la policía de Edimburgo ha sido obligada a someterse a una prueba de ADN. Los delitos

merecedores de esta práctica no se limitan a las categorías obvias de asesinato, violación o robo, sino que se extienden también a las infracciones de tráfico, hurtos en comercios y alteraciones del orden público tales como la Breach of the Peace[147].

En lo que respecta a la privacidad, la política seguida en Edimburgo reviste enorme trascendencia. La recogida y almacenamiento de ADN debe ser considerada, con toda seguridad, como una de las mayores invasiones de la intimidad personal pero, a pesar de ello, parece haberse asegurado un apoyo público sustancial. Un reciente sondeo de opinión sugiere que alrededor de las tres cuartas partes de la población local estaría dispuesta a facilitar su ADN en la «persecución de un crimen».

La policía se niega a reconocer que tales prácticas tengan consecuencias para los derechos civiles. Un portavoz de la policía manifestó recientemente a la BBC: «Tenga en cuenta que la persona que comete una infracción de tráfico puede ser un delincuente de importancia y es nuestra oportunidad para recoger su ADN e identificarlo».

Es aún demasiado pronto para hacerse una idea del éxito obtenido por tal programa, pero el Primer Ministro Tony Blair ya ha señalado que él quiere que todas las fuerzas de policía del Reino Unido sigan el ejemplo de Edimburgo. Si es así, es probable que dentro de una generación el ADN de la mayoría de la población del Reino Unido haya sido archivado en la base de datos nacional de ADN.

También el Ministerio del Interior y otras instituciones gubernamentales se han entusiasmado por el potencial de las pruebas de ADN. La legislación reciente de la Child Support Agency obliga a todos los que nieguen su paternidad a someterse a una prueba de ADN. La negativa a hacerlo así es legalmente equivalente a un reconocimiento de culpabilidad.[148]

La actual obsesión por las pruebas de ADN apunta directamente al centro de la cuestión de la privacidad. Tradicionalmente, la invasión de la intimidad se ha justificado sobre la base de un gobierno efectivo de la sociedad. La policía ha argumentado siempre que la privacidad y el anonimato son malas noticias para la aplicación de la ley. Las

[147] Una traducción literal al español sería "Quebrantamiento de la Paz"

[148] Esta idea es compartida por el legislador nacional, que, a través de la LEY nº 20.030 publicada el 05/07/2005 y que modifica el código civil, específicamente en el artículo 199, quedando dentro de sus incisos el siguiente texto: "La negativa injustificada de una de las partes a practicarse el examen (… de ADN…) hará presumir legalmente la paternidad o la maternidad, o la ausencia de ella, según corresponda.

Se entenderá que hay negativa injustificada si, citada la parte dos veces, no concurre a la realización del examen. Para este efecto, las citaciones deberán efectuarse bajo apercibimiento de aplicarse la presunción señalada en el inciso anterior."

autoridades siempre se han esforzado por conseguir una perfecta identificación de los ciudadanos. Y el ADN es el identificador perfecto.

- El individuo y el Estado

Pero la popularidad de las pruebas de ADN es meramente un síntoma de una tendencia mucho más amplia en todo el mundo. Gobiernos y organizaciones del sector privado han ido avanzando en años recientes hacia la inclusión de la vigilancia en casi todos los aspectos de nuestras finanzas, comunicaciones y forma de vida. Mientras se alaba la privacidad de boca para fuera, se argumenta que la vigilancia es necesaria para mantener la ley y el orden y para conseguir eficacia económica. La justificación es a menudo interesada y algo falsa, pero una cantidad sustancial de personas han sido persuadidas, no obstante, de que la renuncia a la intimidad es el precio que hay que pagar por una sociedad mejor y más segura.

La cuestión no ha sido nunca sencilla. La protección de la privacidad individual ha sido siempre una de las grandes polémicas de los derechos humanos. En su centro se encuentra la lucha por encontrar el equilibro ideal entre la autonomía del individuo y el poder del Estado.

Esta lucha por el equilibrio se desarrolla cada día de mil maneras. Con cada nueva intromisión en la vida privada --ya sea Televisión en Circuito Cerrado (TVCC), vigilancia del correo electrónico o publicidad directa-- la gente se ve obligada a elegir entre sus derechos individuales y los derechos de la sociedad.

Sin embargo, aunque el problema --hay que admitirlo-- es más complejo de lo que lo ha sido jamás, también es más acuciante que nunca. Probablemente, nunca ha habido un momento en la historia en el que se haya acumulado tanta información sobre la población en general. Los detalles de un adulto medio económicamente activo, del mundo desarrollado, se encuentran en cerca de 400 de las principales bases de datos: suficiente información procesada como para recopilar un enorme historial de cada persona.

La vigilancia visual electrónica en los centros urbanos es ya omnipresente. Casi todas las formas de comunicación electrónica se exploran y analizan ya rutinariamente.

Estas actividades han dado lugar a un sector económico floreciente. En Gran Bretaña, la industria de vigilancia en todas sus formas --investigadores privados, agencias de crédito, servicios de seguridad, etc.-- emplea a más de un millón de

personas. Tal población de fisgones profesionales se explica, en parte, por la aparición de la vigilancia de masas. En el pasado, la vigilancia apuntaba a individuos o grupos específicos. Ahora, la vigilancia sistemática en un número creciente de ámbitos analiza activamente a millones de personas a la vez.

Tradicionalmente, la reacción pública a la invasión de la intimidad ha sido contradictoria e impredecible. Aunque las encuestas de opinión muestran consistentemente que la gente se preocupa por la intimidad, la oposición pública, incluso a la más descarada invasión de la privacidad, es escasa.

En los Estados Unidos, la toma de huellas digitales a los perceptores de la beneficencia social ha proseguido con un escaso murmullo de protesta mientras que, en Australia, los intentos del gobierno federal de introducir una tarjeta nacional de identidad provocaron en los años ochenta las mayores protestas públicas que se recuerdan en ese país. Sin embargo, mientras la legislación australiana que obliga a los bancos a informar de las transacciones sospechosas pasó sin llamar la atención, leyes similares en los Estados Unidos provocaron más de un cuarto de millón de quejas por escrito.

En Alemania y Australia, las propuestas de introducir servicios de telefonía digital desataron un amplia preocupación por la intimidad. Idéntica tecnología fue introducida en Gran Bretaña con escasa o nula discusión.

- La privacidad como Derecho Humano

Causa o efecto, la privacidad ocupa ahora un lugar poco envidiable en el catálogo de los derechos humanos. Junto a la censura y la libertad de expresión, la privacidad sigue siendo una polémica compleja, y su solución un desafío. Durante el último cuarto de siglo, ningún otro derecho fundamental en el ámbito de la política pública ha generado tanta turbulencia y controversia. Y sin embargo, como un escritor ha observado, «la privacidad es el derecho del cual todos los demás se derivan». Es el centro de la libertad y autonomía del pueblo y es, tal vez, el factor clave que limita el poder del Estado.

Tortura, discriminación, odio racial: todas estas cuestiones han conseguido un consenso básico en la comunidad internacional. La privacidad, sin embargo, es percibida por muchos gobiernos y corporaciones como el «coco» de los derechos humanos. Es un lugar común para muchas organizaciones el que la privacidad y la

protección de la información personal impiden el rendimiento económico y la aplicación de las leyes. El resultado es que muchos países se están convirtiendo en sociedades vigiladas. La justificación es seductora y difícil de contrarrestar (los habitantes de Edimburgo saben todo ésto demasiado bien). Y en nuestro inocente y natural deseo de ahorrarnos unos pocos dólares, o simplemente de ser buenos ciudadanos, cedemos constantemente información acerca de nuestras finanzas, compras, empleo, intereses, actividad telefónica, e incluso nuestros desplazamientos geográficos. Inevitablemente, cuando así lo hacemos, las organizaciones están listas para explotar esos datos. La vigilancia se ha convertido en un componente fijo de la próspera economía de la información.

Es ya un lugar común que la potencia, capacidad y velocidad de la tecnología de la información se están acelerando rápidamente. El alcance de la invasión de la privacidad --o al menos el potencial para invadirla-- crece a la par. Pero no es sólo la acrecentada capacidad y el costo decreciente de la tecnología de la información lo que genera amenazas a la privacidad. La globalización de sistemas como Internet elimina las limitaciones geográficas (y las protecciones legales) al flujo de los datos. La convergencia está conduciendo a la eliminación de las barreras tecnológicas entre sistemas. Los modernos sistemas de información tienen una creciente capacidad de interacción con otros sistemas y pueden intercambiar mutuamente y procesar diferentes clases de datos. Entretanto, el fenómeno multimedia, que funde varias formas de transmisión y expresión de datos e imágenes, crea enormes dificultades a los legisladores que desean proteger la intimidad personal.

Recientemente, se presentó en la cadena de TV BBC2 un documental sobre la privacidad, en el que describía uno de los resultados imprevistos de estas macro-tendencias de la tecnología: una compañía, UK InfoDisc, ha producido un CD-ROM que cruza los datos de las listas electorales con los de la guía telefónica y datos geodemográficos. Así, la más elemental e inocente información acerca de usted puede ser introducida en el disco, revelando toda clase de hechos. Su número de teléfono lleva instantáneamente a su dirección. Su nombre lleva automáticamente a su profesión y edad. No es necesario decir que los sectores de finanzas y créditos, investigadores privados, periódicos, empresas de mercadotecnia y policía hacen uso intensivo de este producto.

Estas cuestiones son importantes porque el creciente lazo de información entre el ciudadano y el Estado (y el sector privado, naturalmente) disminuye la autonomía

humana. Conforme se automatiza la toma de decisiones por las instituciones, los factores que afectan a nuestras vidas se construyen sobre la base de una masa creciente de datos personales íntimos. El riesgo de desarraigo o discriminación se intensifica paralelamente.

- Los países en vías de desarrollo (como el caso de Chile)

En los países en vías desarrollo, la amenaza es aún mayor. La perfecta identificación de los individuos puede tener fatales consecuencias. Los gobiernos de las naciones en desarrollo confían en que los países del primer mundo los equipen con tecnologías de vigilancia como equipos de intervención telefónica digital, equipos de descifrado, escáners, escuchas, equipos de seguimiento y sistemas de intervención en ordenadores. La transferencia de tecnología de vigilancia desde el primer al tercer mundo es ahora un lucrativo negocio suplementario para la industria de armamento.

Esta visión fué corroborada por el informe de 1997, «Evaluación de las Tecnologías de Control Político», encargado por el Comité de Libertades Civiles del Parlamento Europeo, y llevado a cabo por la Oficina de Evaluación de Opciones en Ciencia y Tecnología (STOA) de la Comisión Europea.

El comercio internacional en tecnología de vigilancia (algunas veces conocido como el Comercio de la Represión) implica la fabricación y exportación de tecnologías de control político. Estas tecnologías incluyen una sofisticada tecnología informática que amplía enormemente el poder de las autoridades.

El informe de Privacidad Internacional listaba las compañías que exportan dicha tecnología a países en desarrollo con un escaso historial de derechos humanos. Los intentos realizados, tanto por el informe del Parlamento Europeo como por Privacidad Internacional, por aumentar el grado de conciencia acerca de las implicaciones éticas de la transferencia de tal tecnología, se han visto acrecentados por informes recientes de Amnistía Internacional, Human Rights Watch y Oxfam. La imagen es convincente: «El comercio de vigilancia es casi indistinguible del comercio de armas. Más de un setenta por ciento de las compañías que fabrican y exportan tecnología de vigilancia también exportan armas convencionales, químicas o equipo militar. La vigilancia es un elemento crucial para el mantenimiento de cualquier infraestructura no democrática y una actividad importante en la consecución del control político y de inteligencia. Muchos

países en transición a la democracia también confían ampliamente en la vigilancia para satisfacer las demandas de la policía y los militares».

Según el informe STOA, gran parte de esta tecnología se utiliza para seguir las actividades de disidentes, activistas de derechos humanos, periodistas, líderes estudiantiles, de minorías o sindicales, y opositores políticos. Los sistemas de identificación a gran escala son también útiles para monitorizar grandes sectores de la población. Como señalaba Privacy International, «en ausencia de un significado legal o protecciones constitucionales, tal tecnología es lo opuesto a una reforma democrática. Puede, ciertamente, resultar fatal para cualquiera persona 'de interés ' para un régimen».

- Las tecnologías de vigilancia

La visión de que la tecnología de vigilancia es inherentemente hostil a los derechos individuales fue expuesta con cierta vehemencia en el informe STOA de 1997. El informe sitúa varias categorías de tecnologías de la información --sistemas de identificación, tecnología biométrica, sistemas de intervención telefónica, etc.-- bajo una luz negativa, vinculando su realización a la denegación de derechos humanos básicos. El informe concluye que tales tecnologías (que describe como «nueva tecnología de vigilancia») pueden ejercer un poderoso efecto disuasorio sobre todos aquellos que «pudieran tomar un punto de vista disidente y pocos se arriesgarán a ejercer su derecho a una protesta democrática». Estos factores se hallan también presentes en el incipiente debate sobre el uso por el Estado de la Televisión en Circuito Cerrado (TVCC).

El informe también pone de relieve el uso hostil que esta tecnología podría recibir en distintos regímenes, y las implicaciones éticas derivadas de la exportación de dicha tecnología a esos países.

Mientras que las compañías de TI presentan rutinariamente sus tecnologías como una manera de lograr una reforma de la sociedad, los defensores de los derechos humanos las definen como un medio de control social y político.

Este control será mucho más evidente en los años venideros. Hacia el 2020, de seguir las actuales tendencias, es probable que el alcance de la invasión de la intimidad sea absoluto.

La TVCC puede resultar la más obvia --y onerosa-- de las intromisiones futuras.

En Gran Bretaña, se han colocado cientos de miles de cámaras en autobuses,

trenes, ascensores e incluso cabinas telefónicas. Mucha gente ahora da por hecho que será filmada desde el momento en que sale por la puerta. Cámaras ocultas, antes objeto de desaprobación, están siendo instaladas ahora sin más problemas en cines, cascos de policías, bares, zonas de alterne, vestuarios y bloques de viviendas. Considerada hace tiempo como una indisimulada herramienta de vigilancia, tras un plazo de quince años la TVCC es ahora percibida como una parte integral y benigna del entorno urbano.

Olvide por un momento la engorrosa tecnología representada en 1984. Es la integración de la vigilancia con el entorno lo que la hace más eficaz.

En Gran Bretaña, la vigilancia visual se está convirtiendo en un componente fijo del diseño de los modernos centros urbanos, nuevas áreas de viviendas, edificios públicos e incluso a través de la red de carreteras (una red masiva de cámaras, conectadas, para la identificación de matrículas terminarán con el anonimato en la carretera de aquí a diez años). Pronto, la gente esperará que la tecnología de espionaje se integre en todas las formas de arquitectura y diseño. Es, tal vez, sólo una cuestión de tiempo antes de que las presiones legales y colectivas introduzcan las cámaras en nuestras casas.

- ENFOPOL, ECHELON, SORM ....

La omnipresencia de la vigilancia visual tendrá su paralelo en la vigilancia en masa de la actividad telefónica y de Internet. Las instituciones de seguridad de Europa y Estados Unidos han puesto ya los cimientos para un sistema de escucha masiva capaz de interceptar los teléfonos móviles, las comunicaciones por Internet, los mensajes de fax y buscapersonas a través de toda Europa.

El plan, conocido como ENFOPOL 98, ha sido llevado en secreto por funcionarios de Policía y Justicia, como parte de una estrategia paneuropea para crear una red sin fisuras para la vigilancia de las telecomunicaciones por encima de las fronteras nacionales.

La estrategia, que ha recibido un amplio apoyo del Consejo de Justicia e Interior de la UE --máximo servicio policial de Europa-- obligará a todos los proveedores de servicios Internet e intercambios telefónicos a dar a las instituciones acceso «en tiempo real y a tiempo completo» a todas las comunicaciones, independientemente del país de origen. Todos los nuevos medios de comunicación, incluyendo la televisión interactiva por cable, serán también obligados a dar pleno acceso a las fuerzas de seguridad.

El sistema ENFOPOL se ayudará de un sistema de «etiquetado de un sujeto» capaz de seguir la pista de un individuo a cualquier lugar que vaya. Conocido como International User Requirements for Interception (IUR), el sistema de etiquetado, que está siendo desarrollado actualmente, creará una red de transmisión y proceso de datos que incluirá no sólo nombres, direcciones y números de teléfono de los «objetivos» y sus asociados, sino direcciones de correo electrónico, detalles de tarjetas de crédito, PINs y contraseñas.

El sistema cruzará además los datos de teléfonos móviles para crear un sistema exhaustivo de seguimiento de localización geográfica.

ENFOPOL es sólo uno entre los varios sistemas que están surgiendo para rastrear y analizar las comunicaciones internacionales. Tal vez el más sorprendente sea ECHELON, un sistema global de escucha establecido por la Agencia Nacional de Seguridad de los Estados Unidos. Este sistema fue diseñado para operar en el núcleo de los sistemas internacionales de telecomunicaciones y puede escudriñar decenas de millones de mensajes de correo y faxes para descubrir palabras de interés para los Estados Unidos y sus aliados.

En el Reino Unido, el proyecto de ley de Regulación de Poderes de Investigación (conocido en Rusia como Ley SORM), en su tercera revisión por hoy, proporcionará al gobierno un arsenal de poderes para poner los ordenadores e Internet bajo vigilancia. Las medidas tienen el efecto potencial de criminalizar a los usuarios de sistemas de cifrado (y ésto, en última instancia, significa cualquier futuro usuario de ordenadores). El proyecto también da a casi todas las autoridades el derecho, sin necesidad de mandamiento judicial, de supervisar la información sobre el tráfico de Internet. Esto es, qué sitios web se ha visitado, a quién se ha enviado correo electrónico o qué grupos de noticias se leen.

Las autoridades fiscales usarán la ley en el futuro para dirigir una masiva operación de captura por toda la Internet, analizando y elaborando perfiles sobre las actividades de millones de usuarios.

Una vigilancia perfecta requiere una no menos perfecta identificación y los próximos veinte años verán un exhaustivo esfuerzo de las autoridades para conseguir este fin. Además de establecer el uso extensivo de pruebas de ADN para distintos propósitos, es probable que administraciones públicas y empresas introduzcan un sistema nacional de huellas digitales electrónicas y escáners de mano.

Estos sistemas, conocidos como «identificadores electrónicos», están ya en uso en todo el mundo. Según afirman, obtienen una identificación casi perfecta del individuo escaneando los más finos detalles de una mano, un dedo o un ojo.

Diversos planes de biometría están siendo llevados a cabo por todo el mundo.

España ha comenzado un sistema nacional de huellas digitales para los beneficiarios del desempleo y la seguridad social. Rusia ha anunciado sus planes para un sistema nacional de huellas digitales electrónicas para los bancos. Los jamaicanos están obligados a escanear sus pulgares en una base de datos antes de ser autorizados a votar en las elecciones. En Francia y Alemania se están probando equipos que permitan incluir huellas digitales en las tarjetas de crédito. Esta tecnología está siendo utilizada por concesionarios, guarderías, fuerzas de seguridad y cajeros automáticos. Microsoft anunció recientemente que tiene intención de incorporar biometría en sus nuevos sistemas operativos para ayudar a la seguridad en Internet.

Durante los últimos cinco años, el Servicio de Inmigración y Naturalización de los Estados Unidos (INS), o «Migra» como la denominan los hispanos, ha estado desarrollando un sistema automático de control de pasaportes utilizando la geometría de la mano. En este proyecto, los viajeros habituales tienen su geometría manual almacenada en una tarjeta inteligente. El viajero coloca una mano en un escáner e inserta su tarjeta en una ranura. Más de setenta mil personas han participado en la prueba. Un portavoz del INS informó reciente al Daily Telegraph que la organización pretende crear un sistema biométrico para viajeros de amplitud mundial.

- Vigilancia en el puesto de trabajo

Pero será el incremento de la vigilancia en el puesto de trabajo lo que afectará más directamente a la gente. En la mayoría de los países, los trabajadores casi no tienen derecho a la privacidad. Los empresarios tienen permiso --«justificado»--para poner a todos los empleados bajo constante vigilancia. Pueden intervenir los teléfonos, leer el correo electrónico y controlar las pantallas de los ordenadores. Pueden escuchar las conversaciones, analizar el comportamiento del ordenador y del teclado, curiosear mediante cámaras de TVCC, utilizar tecnología de seguimiento para controlar los movimientos personales, analizar la orina para detectar el uso de drogas y exigir la revelación de datos personales íntimos. La creciente precariedad de la fuerza de trabajo acelera todas estas actividades.

Software telefónico como WatchCall, de Harlequin, analiza los números de las llamadas que los empleados realizan y reciben. En las industrias basadas en el ordenador y el teléfono, tales programas han convertido a los supervisores en el equivalente digital de los capataces de los asilos victorianos para indigentes. La nueva generación de tecnología de supervisión es extremadamente efectiva. Puede analizar las pulsaciones en un teclado para determinar si los empleados usan eficientemente su tiempo entre conversaciones telefónicas.

Incluso los trabajadores altamente cualificados pueden esperar ser puestos de forma habitual «bajo el microscopio». Es probable que cualquier director que adquiere un software de sistema operativo de red reciba al mismo tiempo funciones, ya incluidas, de escucha. Algunos paquetes como Win Watch Professional y Norton Lambert 's Close-Up/LAN, permiten a los administradores de la red observar las pantallas de los empleados en tiempo real, explorar los archivos de datos y el correo electrónico, analizar las pulsaciones del teclado e incluso saltarse las contraseñas.

Estas tendencias sólo pueden tener un resultado: el puesto de trabajo del mañana tendrá muchas de las características de los asilos de indigentes descritos por Dickens.

- Vigilancia en el hogar

Incluso su hogar no estará a salvo de la vigilancia. Considere la nueva generación de servicios de televisión digital interactiva. Estos productos ofrecen una nueva familiaridad entre el proveedor de servicios de TV y el cliente. Extrayendo directamente la información de los hábitos televisivos del cliente, transacciones financieras y encuestas «en pantalla», la compañía puede crear un perfil complejo de cada cliente.

Un nuevo libro Spy TV (La televisión espía) del investigador estadounidense David Burke explica cómo el nuevo sistema invade subrepticiamente la privacidad de los clientes. Burke ha incluído algunas citas literales de entusiasmados directores de mercadotecnia. En palabras del jefe de Procter&Gamble, Edmin Artzt, quieren «hincarle el diente a toda esta nueva tecnología y convertirla en una época de bonanza para la publicidad».

La televisión interactiva (también conocida como i-TV) va mucho más allá de la publicidad, ya que promete --según la apreciación del analista de información del Reino

Unido, William Heath-- «crear unas condiciones experimentales totales en el hogar de cada usuario, con un ciclo mensura¬ble de estímulos, medida y respuesta».

«Podemos elaborar perfiles de la gente... En último término, el producto se dirigirá por sí mismo a los clientes individuales», dice Simon Cornwell, de Two Way TV. «La gente revela muchísmo acerca de sí misma», dice Nick Bryant, de BiB. «Es publicidad despersonalizada», dice Howard Hughes, de NTL: «Con los datos que nos llegan de vuelta, recordaremos todo acerca de cada uno». Pat Dade, de Synergy Consulting cree incluso que los incomprendidos consumidores de hoy recibirán con agrado la posibilidad de ser psicoanalizados a través de sus propios televisores.

Como Heath ha señalado, «No es que los consumidores lo estén reclamando clamorosamente, pero los promotores pueden ver que les puede hacer ganar más dinero que Internet. Es como un promotor inmobiliario mirando el éxito de Portobello Road e intentando entusiasmar al mundo acerca de su nuevo proyecto de centro comercial que viene completo con TVCC y tarjetas de fidelidad».

Hace tan solo en el mes de noviembre de 2005 se determinó que las impresoras de color dejan una huella digital, técnica que identifica la fuente del documento, codificando silenciosamente información sobre la hora y fecha de la impresión, y el número serial de la impresora en cada página impresa..

La Electronic Frontiers Foundation recientemente liberó los resultados del Machine Identification Code Technology Project, el cual disecciona los detalles técnicos del sistema de codificación oculta de al menos una impresora, revelando la mecánica simple tipo de dejar un trozo de papel en más de una manera.

Jason Tuohey documentó esta historia el año pasado en un artículo en PC World.com, Este sistema de identificación de impresora ha estado existiendo desde hace dos décadas, y crea una herramienta valiosa ideada para arrestar a los falsificadores, pero también es una complicada noción para los defensores de la privacidad fatigados del gran hermano.

El reporte de la EFF revela como las impresoras DocuColor de Xerox cubren toda la página con una grilla repetida de minúsculos puntos amarillos, invisible para el ojo desnudo pero facilmentes reconocibles bajo una lámpara LCD azul. Ésta grilla es capaz de codificar hasta catorce bytes de siete-bits de información de rastreo, presentado en filas y columnas de puntos.

Si bien los puntos pueden parecer confusos al principio, una vez que uno sabe cómo leer el código, la información identificatoria es fácilmente interpretada.

El criptograma es relativamente simple, y el reporte EFF incluye un programa que le permita a cualquiera chequear la validez de este sistema de seguimiento simplemente ingresando el código de la página impresa.

Los usuarios necesitan solamente imprimir una página en su impresora color, mirarla bajo una luz LCD azul, ingresar la coordinación de puntos en el programa, y el sistema le dirá el número serie de su impresora, la fecha y la hora de la impresión - en menos de un minuto.

Este software también está disponible como una descarga de código abierto, licenciado bajo la GNU General Public License.

No todas las impresoras de color codifican la información esta manera, y la EFF ha incluido esta lista de impresoras que no utilizan el sistema de pequeños puntos amarillos, pero advierte que pueda haber otros sistemas de rastreo que estén trabajando en esas impresoras.

Mientras que el sistema de puntos amarillos es alarmante, su edad y relativa simplicidad podría indicar que ha sido reemplazado por sistemas más sofisticados que el público todavía no conoce. Esto puede ser probable porque ahora que el sistema de codificación ha sido revelado, cualquiera puede manipular las marcas utilizando varias impresoras.

De acuerdo al artículo de Tuohey, esta tecnología comenzó hace aproximadamente 20 años, “ para mitigar los miedos de que las copiadoras color pudieran ser utilizada fácilmente para falsificar billetes ." Esta tecnología desde entonces se ha hecho práctica común para muchos fabricantes de impresoras de todo el mundo.

El codificador está enterrado profundamente en las impresoras, y Tuohey advierte que remover el delgado chip probablemente romperá la impresora “ Las travesuras habituales no lo ayudarán a evitar esto ," dijo Peter Crean, un investigador senior de Xerox.

Lorelei Pagano, especialista en falsificaciones del servicio secreto de los Estados Unidos le dijo a Tuohey que la tecnología es extremadamente útil para rastreara a los falsificadores, y no se la utiliza para mantener un registro del público en general. " El único momento en que cualquier información se obtiene de esos documentos es solamente es en [el caso de] un acto criminal," Dijo Pagano.

A pesar de lo anterior la EFF informa que “ no hay leyes para impedir que el Servicio Secreto utilice código de impresora para rastreara secretamente el origen de

documentos no aceptados ,” un hecho alarmante considerando la ola de leyes supresoras de libertades civiles aprobada por muchos gobiernos tal como la US Patriot Act.

De acuerdo a la EFF, a las compañías impresoras tampoco se les requiere que informen a los clientes si sus impresoras utilizan algún tipo de sistema de identificación.

Por tanto y como moraleja solo podemos decir que hay que ser cuidadoso con lo que se imprime y a quien se lo da. En esa impresión láser que acaba de hacer está estampada su firma invisible y todo gracias a los gobiernos de grandes países (especialmente EEUU) y las empresas de impresoras.

CAPITULO VII: Protección Laboral

"En Internet, nadie sabe que eres un perro."
Humor gráfico en el periódico New Yorker

1. Uso de Tecnologías de la Información por parte de trabajadores.

La masificación del uso de las Tecnologías de Información y Comunicación ha llevado a que los trabajadores deban disponer de las herramientas necesarias para realizar sus labores diarias en las empresas o lugar de trabajo. El uso del e-mail para enviar archivos a jefes o subordinados, la necesidad de mantener contacto constante con los clientes hace necesario que la empresa utilice cada vez más las TIC para mantener comunicados a sus empleados y a sus clientes.

Por otra parte, la necesidad de mantenerse informado, realizar transacciones en línea; por ejemplo el pago de cotizaciones previsionales, operaciones bancarias, requerir de información de la web, hace necesario que los trabajadores tengan acceso a Internet para realizar esas labores, pero ¿tienen que tener acceso a internet todos los trabajadores? ¿Se utilizará internet sólo para fines labores? ¿Puede el empleador controlar el uso del e-mail de sus trabajadores? ¿Puede revisar los contenidos que visita en internet? ¿Qué derecho predomina el del empleador o la privacidad del trabajador?. Estas nuevas interrogantes son algunos de los problemas que se están presentando en la empresa de hoy, a todo nivel, sean grandes medianas o pequeñas y que en teoría el legislador debiera de regular, considerando sobre todo la posibilidad de que empleadores violenten en forma ilícita la privacidad de los trabajadores.

Se hace necesario tener una clara normativa laboral que permita a empleadores y

trabajadores velar por la protección de cada uno de sus derechos, por un lado el derecho de propiedad del empleador sobre sus computadores, conexiones a internet, servidores, y otros equipamientos para que sean utilizados para los fines de la empresa, y por otro el derecho a la protección de la intimidad del trabajador. El uso de las TIC en la empresa exigen una mirada especial tanto por el uso que el trabajador da a esas herramientas, como el control que ejerce el empleador.

a globalización de los mercados, la expansión de las tecnologías ha llevado a que las empresas cuenten con la adecuada red de comunicación interna-externa, cada vez más trabajadores acceden al uso de las tecnologías desde sus puestos para contactar a sus jefes, sus clientes o a sus compañeros de trabajo. Estos instrumentos son para fines estrictamente laborales y utilizados para la producción, sin embargo pueden llegar a ser utilizados por el trabajador para fines personales. Hoy muchas empresas comienzan a tener problemas con sus trabajadores porque el uso de estas herramientas se está constituyendo en un perjuicio, afectando el rendimiento de los trabajadores y por tanto generando una disminución en la productividad. Sin embargo no es el único perjuicio que se origina, otros como la perdida de la calidad de la red de comunicaciones, el uso del computador para negocios personales, la recepción y difusión de virus en los sistemas informáticos de la empresa, las filtraciones de información a terceros y que forma parte del patrimonio de la empresa, acoso sexual a compañeros de trabajo, lesiones contra la propiedad intelectual, etc.

n el caso de Chile podemos hacer referencia al dictamen de la Dirección del Trabajo que interpretando las disposiciones del Código del Trabajo, respecto a los derechos fundamentales, estableció una línea de acción en la materia. El dictamen 0260/0019 del 24 de enero de 2002 sostiene que "de acuerdo a las facultades con que cuenta el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos, pero en ningún caso podrá tener acceso al contenido de la correspondencia electrónica privada enviada o recibida por los trabajadores".

diferencia de las herramientas tradicionales, las TIC poseen la capacidad de conservar todas y cada una de los rastros dejados por el trabajador durante su utilización, de allí que los empleadores no tarden en ejercer el control denominado como cibervigilancia a fin de evitar que se utilicen en forma abusiva o inapropiada las TIC en ambientes laborales.

o importante en esta materia no es el cómo lo ejecuta el empleador sino hasta

dónde. ¿Tiene autorización total?. Si el reglamento de la empresa lo establece, ¿es legitimo para el trabajador?. Cada situación se encuentra limitada por el ejercicio de los derechos fundamentales del trabajador en la relación laboral. Que el empleador entregue al trabajador una cuenta de correo electrónico no le habilita a controlar en forma autoritaria las comunicaciones realizadas a través de del mismo, ni la protección de las garantías constitucionales puede servir de amparo al trabajador para realizar lo que desee, y por tanto despojar al empleador de la facultad de dirección y control. Frente a un conflicto, se deben ponderar los bienes y derechos constitucionalmente protegidos, ello debe dar la luz si el eventual recorte que se produce a través de los medios de vigilancia y control respeta las garantías constitucionales de los trabajadores afectados. Para ello deberemos recurrir a determinar si se ha autorizado o no la utilización de las TIC para fines no laborales, ver si existen medidas de seguridad, códigos de conductas, el tipo de actividad que se desarrolla, etc. Pero lo más importante antes de determinar la legitimidad o no de los controles será el definir la naturaleza y las condiciones de uso que se hayan establecido respecto de las herramientas informáticas entregadas a los trabajadores para que realicen sus labores, ya sea en contratos colectivos, convenios colectivos, contratos individuales, reglamentos de la empresa o incluso en códigos de conductas establecidos por la empresa, ya sea desde el inicio de la relación laboral o por posteriores anexos, todo en virtud de la facultad de dirección y control que posee el empleador.

2. Control del empleador en el uso de las Tecnologías de la Información.

La relación laboral es un escenario donde entran en juego distintos derechos fundamentales en busca de equilibrio. Un caso que se presenta a menudo ocurre con el legítimo interés del empleador en acceder a información sobre sus trabajadores para desarrollar su actividad –amparado por las libertades de información y de empresa-, y los derechos de estos últimos a la intimidad, a la propia imagen, a la libertad sindical y al secreto de las comunicaciones. Este viejo conflicto ha resurgido a propósito de la utilización del correo electrónico y de otros servicios que ofrece la red Internet en el ámbito laboral, ante la posibilidad que tiene el empleador para controlarlos.

Es público y notorio el hecho que Internet constituya una potente herramienta que la empresa puede poner a disposición de los trabajadores para optimizar el cumplimiento de su prestación laboral. Sin embargo, también es indiscutido que puede –y de hecho así ocurre-, ser utilizada para fines personales, al igual que los teléfonos o faxes, influyendo ello no sólo en el coste que el empresario tiene que asumir, sino principalmente en la productividad –sobre todo en los primeros meses de implementado el acceso a la red- al distraer parte de la jornada laboral en su utilización privada. Pero por tratarse de una red abierta, los problemas pueden ir más allá, por ejemplo, desde la sustracción de información confidencial de la empresa, no sólo desde fuera de ella sino, en especial, por los propios trabajadores; pasando por la transmisión de virus informáticos, actos de intrusismo y utilización de programas no autorizados; hasta llegar a la difamación de un empleado o, incluso, al acoso sexual a través del correo electrónico.

Por ello, no parece que la verdadera finalidad del empresario al aplicar medidas de control sea conocer o censurar el contenido de mensajes o archivos, sino más bien su preocupación radica en evitar el consumo descontrolado de sus recursos y la pérdida de horas de trabajo, y mantener la propia seguridad de la información contenida en sus sistemas informáticos, razón por la cual este trabajo pretende defender como tesis la legitimidad del control tecnológico del empleador indicando los límites dentro de los cuales se encontraría, a nuestro juicio, justificado frente a los derechos fundamentales de los trabajadores.

- Fundamentos del control

El control tecnológico que realiza el empleador sobre sus trabajadores no es per se arbitrario o abusivo, sino que emana como una manifestación de la libertad de empresa que le reconoce el artículo 38 de la Constitución española, en el marco de la economía de mercado. Además, el acceso a datos del trabajador puede realizarlo, en principio y bajo una serie de matices que indicaremos más adelante, amparado en el derecho a recibir libremente información veraz por cualquier medio de difusión, según la letra d) del artículo 20 de la Carta Fundamental.

La normativa específica que desarrolla los derechos constitucionales antes mencionados en el ámbito laboral la encontramos en el artículo 20 del Estatuto de los Trabajadores, contenido en la Ley 8/1980, el cual, al referirse a la dirección y control de

la actividad laboral, faculta al empresario para adoptar las medidas de vigilancia y control que estime más oportunas –por ejemplo, utilizando medios tecnológicos- para verificar el cumplimiento de las obligaciones y deberes laborales del trabajador. Dichas obligaciones pueden resumirse en: a) realizar el trabajo convenido bajo la dirección del empresario, y b) prestar la diligencia y colaboración en el trabajo que marque la ley o la costumbre, los convenios colectivos y las órdenes o instrucciones adoptadas por el empleador en ejercicio de sus facultades de dirección. Además, el Estatuto es explícito frente a los deberes básicos del trabajador, que van desde el cumplimiento diligente y de buena fe de sus obligaciones laborales y de las órdenes e instrucciones impartidas por el empresario, hasta la contribución a la mejora de la productividad.

Por otra parte, en caso de incumplimiento contractual grave y culpable, el empresario puede despedirlo. Así, una trasgresión de la buena fe contractual por no respetar la confidencialidad de la información de la empresa; el abuso de confianza en el desempeño del trabajo ocurrido al utilizar la conexión a Internet que le proporciona el empresario para navegar por sitios de ocio o pornografía; una disminución continuada y voluntaria en el rendimiento de trabajo normal o pactado a causa de dedicarle mucho tiempo a participar en chat de conversación en línea; o incluso situaciones más graves, como la utilización del correo electrónico para enviar ofensas o acosar sexualmente a compañeros de trabajo, habilita al empleador para alejar al trabajador de la empresa.

- Tipos de control Tecnológico ejercido por el Empleador en el marco de una Política de Seguridad Informática

Como puede apreciarse, el justificado control tecnológico que ejerce el empleador en su empresa obedece principalmente a una necesaria política de seguridad informática. En efecto, el estado actual de la tecnología permite cubrir uno de los aspectos básicos para el desarrollo de la actividad empresarial: la seguridad de los sistemas informáticos. Tal es su importancia que en ocasiones se impone como una obligación legal o reglamentaria para resguardar la información y garantizar su confidencialidad, integridad, disponibilidad y verificabilidad.

Sin entrar en detalle y a modo ilustrativo, cabe mencionar algunas medidas utilizadas para realizar una protección lógica de los datos, las comunicaciones y los sistemas al interior de una empresa. Las hay básicas, como la instalación de programas antivirus, de identificadores de usuarios basados en contraseñas o tarjetas de acceso, y

otras más complejas, como la utilización de cortafuegos para controlar los ingresos y salidas de datos en una red, la identificación por técnicas biométricas o firmas digitales, o el cifrado de las comunicaciones. También es importante referirnos a log o registros de auditoría que permiten a los administradores del sistema, el estudio a a de algunas acciones importantes como el arranque y apagado de los equipos y de su software básico, las conexiones y desconexiones de los usuarios, las operaciones de transmisión de datos por la red y los intentos de acceso no autorizados, para identificar así riesgos de seguridad y adoptar medidas correctivas.

Apoyado en estas medidas tecnológicas el empresario puede comprobar si el trabajador cumple o no con sus deberes laborales básicos y realiza el trabajo convenido. Además, le permiten controlar la productividad y utilización de los recursos, supervisando de forma rutinaria la actividad de los trabajadores. Igualmente, con ellos puede velar por la custodia de secretos profesionales y generar pruebas que lo protejan frente a posibles responsabilidades de la empresa por conductas de sus empleados.

Lo anterior fundamenta la vigilancia del empresario, el cual se puede apoyar, incluso, en la implementación de instrumentos de escucha y filmación. Pensemos que de las circunstancias que habilitan al empresario, por ejemplo para despedir al trabajador por incumplimiento contractual grave y culpable, solo se puede tener conocimiento a través del control y supervisión a través de cualesquiera medios de vigilancia, ya sean previos o posteriores a la falta, medios que deberán ser adoptados de forma equilibrada, pero garantizando el resultado que se pretende.

Es más, la instalación de cámaras de vídeo y de equipos de grabación de audio permiten preconstituir pruebas de las pretensiones del empresario, de acuerdo con el artículo 90, del RDL 521/1990, por el que se aprueba el texto articulado de la Ley de Procedimiento Laboral, al establecer que “las partes podrán valerse de cuantos medios de prueba se encuentren regulados en la Ley, admitiéndose como tales los medios mecánicos de reproducción de la palabra, de la imagen y del sonido, salvo que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales o libertades públicas”.

Sin perjuicio de ello, si el empresario estima como oportunas estas medidas para verificar el cumplimiento de las obligaciones y deberes del trabajador debe circunscribirlas a un ejercicio que respete la dignidad humana, según veremos.

Ahora bien, estos tipos de control tecnológico sobre el trabajador han suscitado diversos puntos de conflicto. Por ejemplo, la comunicación entre los trabajadores y sus

representantes en la empresa y con los sindicatos difícilmente puede ser controlada por el empresario sin violar el derecho fundamental a la libertad sindical. Además, es usual que no se determinen ni pacten claramente los usos de los ordenadores conectados a Internet en los puestos de trabajo, y no se avisen las políticas de control y vigilancia previstas, por lo que al detectar usos incorrectos o excesivos del correo electrónico u otros servicios, se toman medidas extremas, e incluso ilegales, sin previo aviso, como abrir los mensajes, registrar el ordenador que utiliza un trabajador o poner filtros. Por último, la captación masiva de imágenes y sonidos de los trabajadores en el lugar de trabajo plantea la interrogante sobre si constituye una intromisión ilegítima de la intimidad.

Entonces, ¿debe el trabajador tener acceso a Internet en la empresa para usos no laborales?, ¿cuándo y cómo puede el empresario ejercer su legítimo derecho de control en las redes digitales?, ¿qué límites tiene la instalación de videocámaras en el lugar de trabajo?...

Finalmente, cabe agregar que los actuales sistemas de control y vigilancia no están diseñados para vulnerar derechos fundamentales y libertades públicas. Son las conductas reflejadas en los procedimientos de utilización y en las políticas empresariales de control y dirección, las que pueden llegar a ser excesivas y desproporcionadas, atacando directamente la intimidad, las libertades y la dignidad del trabajador. Por eso, el correcto funcionamiento de la empresa no puede ser utilizado como argumento para conculcar arbitrariamente derechos, puesto que el poder de dirección del empresario, imprescindible para la buena marcha de la organización productiva, no es, como veremos a continuación, en ningún caso, ilimitado.

- Límites Jurídicos al control Legítimo del Empresario

La determinación de los límites al control tecnológico del empresario emanado de sus derechos constitucionales a la libertad de empresa y a la libertad de información, es una exigencia de la seguridad jurídica que, más que restringir, busca definir el contenido de un derecho que posee el empleador y que puede ejercer legítimamente.

Lo expuesto hasta ahora podría llevar a pensar en la existencia de un conflicto entre derechos fundamentales de las partes ligadas por la relación laboral. Sin embargo, debemos precisar que no son los derechos los que eventualmente chocarían, al igual que no es la tecnología la causante de las injerencias ilegítimas, sino que son las conductas

que intentan ampararse en una apariencia de derecho las que colisionan, y es el juez quien debe despejar en cada caso en concreto, luego de ponderar los hechos y contrastarlos con las disposiciones jurídicas que hemos visto y otras que mencionaremos, qué conducta está realmente protegida por el derecho que se invoca.

Además, téngase presente que los derechos fundamentales se encuentran sometidos a relaciones de coordinación, no de subordinación, formando un sistema que conduce a albergar derechos equilibrados entre sí, que no hace necesaria la existencia de jerarquías de derechos, e impide que se anulen mutuamente. Dicho sistema encuentra explicación en los propios derechos constitucionales, que al ser inherentes a la dignidad del hombre no pueden desconocer que el ser humano es básicamente una unidad. Por lo tanto, ni la capacidad de control del empresario es absoluta, ni los derechos del trabajador son ilimitados. De hecho, ambos derechos se hayan sometidos al principio jurídico de buena fe contractual.

Precisamente, no podemos dejar de mencionar el papel de la buena fe en el ejercicio de los derechos fundamentales y la prohibición del abuso del derecho. En el primer caso, interesa destacar que los derechos deben ser ejercidos conforme a las exigencias de la buena fe, según unas determinadas pautas de comportamiento sobreentendidas que no pueden ser ignoradas si se quiere comprender el funcionamiento de un sistema jurídico.

En el segundo supuesto, la ley no ampara el abuso del derecho. Es más, resulta ilógico que su ejercicio, que representa para los demás un deber moral de abstención o de actuación, pueda realizarse con abuso. El respeto incondicionado del propio derecho sólo puede ser racionalmente exigido en la medida en que su ejercicio se haga ateniéndose a pautas de comportamiento conformes con las exigencias de una convivencia que garantice los derechos de los demás y la paz social. Esto, sin duda, va más allá de las actuaciones que constituyen delitos, porque se refiere a situaciones en que queda fuera del ejercicio legítimo la acción que de manera desproporcionada e irrazonable, de forma intempestiva e impeditiva de cualquier otra solución, podría haber causado un grave daño a otro.

En otro orden de ideas, la Constitución ha establecido como garantía frente a las limitaciones un núcleo irreductible: el contenido esencial de los derechos fundamentales, que según el Tribunal Constitucional son aquellas facultades o posibilidades de actuación necesarias para que el derecho sea reconocible como pertinente al tipo descrito y sin las cuales deja de pertenecer a ese tipo y tiene que pasar

a quedar comprendido en otro desnaturalizándose. Todo ello referido a un momento histórico y a las condiciones inherentes en las sociedades democráticas. Lo anterior se traduce en la obligación de respetar el contenido esencial para cualquier limitación que pretenda mantener su legitimidad.

En este breve repaso por los límites al control tecnológico del empresario debemos aludir al artículo 10.1 de la Constitución española, que radica en la dignidad humana el antecedente para reconocer a la persona los derechos inviolables que le son inherentes. Además, el propio Estatuto de los Trabajadores, en su artículo 18, se refiere a la inviolabilidad de la persona, al preceptuar que sólo podrán realizarse registros sobre la persona del trabajador, en sus taquillas y efectos particulares, cuando sean necesarios para la protección del patrimonio empresarial y del de los demás trabajadores de la empresa, dentro del centro de trabajo y en horas de trabajo. En su realización se respetará al máximo la dignidad e intimidad del trabajador y se contará con la asistencia de un representante legal de los trabajadores o, en su ausencia del centro de trabajo, de otro trabajador de la empresa, siempre que ello fuera posible. Es decir, los registros están autorizados bajo ciertas condiciones, garantizando transparencia e información al trabajador afectado.

En el artículo 10.1 de la Constitución aparecen como límites genéricos el respeto a la ley que desarrolle o regule el ejercicio del derecho constitucional –en este caso, es el Estatuto de los Trabajadores el que trata los derechos de éstos-, y al resto del ordenamiento jurídico. También se menciona como limitación el respeto a los derechos de los demás, tolerando su ejercicio, que en el caso en estudio se tratará, en principio, del secreto de las comunicaciones, la libertad sindical, la propia imagen y la intimidad. Veamos cada uno de ellos.

En primer lugar, el contenido esencial del secreto de las comunicaciones –que debe ser respetado por el control tecnológico del empresario- protege contra la interceptación o el conocimiento antijurídico de las comunicaciones ajenas. Cuenta además con la garantía de que sólo mediante resolución judicial puede levantarse el secreto y con el resguardo punitivo que brinda el artículo 197 del Código Penal, que sanciona al que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodera de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, o intercepta sus telecomunicaciones o utiliza artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación,

castigándolo con penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Por lo tanto, para controlar el uso del correo electrónico, por ejemplo, el empresario debe demostrar que interfiere en el trabajo ya que, al equipararse al resto de las comunicaciones, es inviolable y su control puede constituir un delito contra la intimidad, si no cuenta con el consentimiento inequívoco del trabajador.

En segundo termino, el trabajador goza del derecho constitucional de sindicación cuyo contenido esencial, en su fase colectiva, no se agota en los aspectos meramente organizativos o asociativos, sino que comprende también los derechos de actividad o los medios de acción necesarios para que el sindicato pueda cumplir las funciones a las que es llamado, medios que el Tribunal Constitucional ha identificado en la huelga, la negociación colectiva y la promoción de conflictos colectivos. Esta libertad sindical comprende la prohibición de injerencias del empresario, quien debe abstenerse de toda interferencia en su ejercicio y, por supuesto, de adoptar represalias contra los trabajadores que legítimamente ejerzan la actividad sindical.

Un tercer derecho involucrado es el de la propia imagen, que garantiza el ámbito de libertad de una persona respecto de sus atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre, cualidades definitorias del ser propio y atribuidas como posesión inherente e irreductible a toda persona.

Por último, el cuarto derecho es la intimidad, que para el Tribunal Constitucional implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de vida humana.

En tal sentido, adoptar como acción limitadora de estos derechos la instalación de videocámaras requiere, junto con todos los matices que estamos mencionando, también del consentimiento del trabajador o, cuando se funda en las necesidades lógicas de seguridad del lugar, por ejemplo, en bancos o supermercados, debe limitarse al principio de la proporcionalidad.

Cabe agregar que la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en su artículo 1 establece que estos derechos fundamentales garantizados en el artículo 18 de la Constitución, son irrenunciables, inalienables e imprescriptibles y serán protegidos civilmente frente a todo género de intromisiones ilegítimas. El artículo 7, en relación con el artículo 2 de la misma ley, considera intromisiones ilegítimas en el derecho a la

intimidad, entre otras, el emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas, salvo que cuenten con consentimiento expreso del titular del derecho o sean actuaciones autorizadas por una ley.

El derecho a la intimidad deriva de la dignidad de la persona e implica la necesidad de un ámbito propio y reservado. No cabe, por tanto, afirmar que la actividad y relación laboral de un individuo esté absolutamente excluida de su "vida íntima". El Tribunal Constitucional rechaza que el lugar de trabajo no constituya, por definición, un espacio en el que el trabajador pueda ejercer con plena efectividad sus derechos fundamentales, entre ellos, la intimidad. El trabajador, en el horario y lugar de desarrollo y ejercicio de su actividad laboral, debe estar sometido a una razonable vigilancia por aquellos medios, sean técnicos o no, que en cada caso el empresario estime adecuados, pero en determinados momentos o lugares, los actos del trabajador, su comportamiento, conversación y actitud, pueden ser ajenos al interés empresarial y corresponder a su intimidad personal. Y en ese punto, y salvo supuestos muy excepcionales, la captación indiscriminada de imágenes y voz supondrá una intromisión injustificada del empresario en la intimidad del trabajador que atentará directamente contra sus derechos fundamentales y que será, además, constitutiva del delito previsto en el artículo 197 del Código Penal.

Junto con estos límites genéricos se han fijado, en algunos casos, límites específicos a los derechos fundamentales. Respecto a la libertad de empresa, el Tribunal Constitucional estima que no existe un contenido esencial constitucionalmente garantizado de cada una de las actividades empresariales concretas. El contenido esencial garantizado en el artículo 38 de la Constitución se reduce a iniciar y sostener en libertad la actividad empresarial, cuyo ejercicio está disciplinado por normas de muy distinto orden, como es el caso del Estatuto de los Trabajadores que desarrolla la facultad de dirección y control de la actividad laboral. Así, la libertad de empresa es sólo libertad de moverse en un marco definido legalmente.

Por su parte, la libertad de información también tiene un contenido preciso. Las libertades del artículo 20 de la Ley Fundamental tienen un valor preponderante únicamente cuando se ejerciten en conexión con asuntos que son de interés general, por las materias a que se refieren y por las personas que en ellos intervienen, y contribuyen en consecuencia, a la formación de la opinión pública, alcanzando el máximo nivel de eficacia justificada frente a los derechos garantizados por el artículo 18 de la

Constitución. Entonces, difícilmente podrá argumentar un empresario que las injerencias que realice al derecho a la intimidad del trabajador, se justifican en un derecho a la libertad de información que reúna los elementos recién mencionados.

Ahora bien, el Tribunal Constitucional ha establecido que frente a medidas limitadoras como las que puede adoptar el empresario en el caso que nos ocupa, los límites de los derechos deben ser interpretados restrictivamente, por eso, dichas limitaciones, además de estar previstas en la ley, deben ser siempre razonables y proporcionadas en relación con el bien o derecho que limitan, justificadas y destinadas a cumplir realmente el fin para las que fueron establecidas.

La razonabilidad y proporcionalidad de las medidas no puede establecerse en abstracto. Para comprobar si una medida restrictiva supera el juicio de proporcionalidad, es necesario constatar si es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido que exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto).

La justificación de la medida limitadora debe ser exteriorizada adecuadamente con objeto de que los destinatarios conozcan las razones por las cuales su derecho se sacrificó y los intereses a los que se entregó. Por último, la medida limitadora debe servir para hacer efectivo un fin legítimo real, no para encubrir objetivos espurios.

Finalmente, cabe destacar un límite de gran importancia práctica, que ya hemos insinuado en nuestra exposición: el derivado de los propios actos del titular del derecho, como manifestación de su consentimiento en la limitación. Al respecto, cada persona es soporte y sujeto jurídico de estos derechos, por lo que su tutela efectiva estará en función del celo que en su guarda y custodia manifieste cada persona o imponga el ordenamiento jurídico. Por ejemplo, la intimidad y la propia imagen constituyen un valor absoluto, permanente e inmutable, pero su tutela efectiva puede aparecer en algunos casos limitada por ciertos condicionamientos que provengan de las leyes, de los valores culturales de la sociedad de cada momento y, de un modo especial, del propio concepto que cada persona tenga respecto a sus particulares pautas de comportamiento por lo que quien descuida estos derechos o consiente la injerencia, no será acreedor de la protección jurídica.

- Reflexiones

Es evidente que un comportamiento laboral abusivo de confianza o desleal frente al empleador, como el uso reiterado de los recursos de la empresa con fines particulares, constituye un incumplimiento del contrato de trabajo que debe ser sancionado, aunque pueda resultar discutible en ciertos casos el optar por el despido. Sin embargo, como consecuencia de la propiedad empresarial sobre el ordenador que usa el trabajador y sobre la dirección del correo electrónico, por ejemplo, cabe preguntarse si realmente puede el empresario acceder, de forma indiscriminada, cuando y como lo desee al contenido de los mensajes que emite y/o recibe el empleado.

Al respecto, parece razonable distinguir si el uso es para fines particulares o profesionales que se derivan de la actividad laboral diaria. En el primer caso, la potestad de control y dirección que corresponde al empresario en uso de la libertad de empresa le ha de permitir establecer, si llega el caso, medidas impeditivas o condicionantes sobre el uso particular de los servicios que ofrece Internet.

En tal caso, resulta fundamental informar al trabajador de los medios que se utilizarán para verificar el cumplimiento de lo pactado y establecer una normativa interna, buscando incluso la aceptación o consentimiento tanto del trabajador como de sus representantes. De hecho, el artículo 64 de la Ley del Estatuto de los Trabajadores establece como competencias del comité de empresa la emisión de un informe previo a la ejecución por parte del empresario de las decisiones adoptadas sobre la implantación o revisión de sistemas de organización y control del trabajo y el ejercicio de una labor de colaboración con la dirección de la empresa para conseguir el establecimiento de cuantas medidas procuren el mantenimiento y el incremento de la productividad, de acuerdo con lo pactado en los convenios colectivos.

Todo ello de acuerdo con el debido respeto a la dignidad humana como valor constitucional recogido en el artículo 20.3 del Estatuto de los Trabajadores y como límite al poder de dirección y control de la actividad laboral por el empresario. Es decir, la adopción de medidas de control será válida, en un principio, cuando se establezca una clara política de empresa al respecto, por ejemplo, a través de la elaboración de un código de conducta que se comunique a los trabajadores con carácter periódico y que indique claramente las reglas a las que el trabajador debe someterse cuando utilice los medios técnicos puestos a disposición de la empresa para la realización de su prestación laboral. También son aconsejables otras medidas, como la separación entre un correo

electrónico personal y uno profesional, o el control gradual de las comunicaciones, las que deben ser analizadas caso por caso.

Pero la cuestión puede resultar distinta si se trata del acceso a Internet para uso profesional. Aunque los equipos sean de su propiedad no corresponde que el empresario tenga un acceso indiscriminado y sorpresivo sobre la actividad laboral llevada a cabo por el empleado. Ciertamente, la libertad de empresa supone el poder de decisión del empresario sobre la estructura y funcionamiento de aquélla; la disponibilidad sobre los medios de producción y la dirección del trabajo del personal contratado, de acuerdo con las condiciones pactadas en el contrato de trabajo. Pero un contrato que no puede ignorar que las relaciones laborales se basan en los principios de buena fe y diligencia profesional. Y, como es obvio, aquellas condiciones no pueden establecerse con abstracción de los derechos reconocidos por la Constitución. La autonomía organizativa del empresario no es ni puede ser ilimitada.

En este sentido, el contrato laboral no es un área autónoma ajena a la vigencia de la Constitución. Por esta razón, el acceso indiscriminado al correo electrónico, por ejemplo, vulnera el derecho del trabajador al secreto de las comunicaciones, que protege la libertad de comunicación y la reserva sobre la comunicación emitida, con independencia del contenido de la misma.

Creemos que no basta con no vulnerar los derechos constitucionalmente protegidos, sino que el empresario deberá, además, optar, sensata y ponderadamente, por políticas adecuadas de control de la actividad laboral que favorezcan un ambiente de trabajo relajado y confiado que proporcione autonomía e intimidad, evitando el recelo, la presión y el malestar de los trabajadores ante conductas excesivas derivadas del poder empresarial.

En definitiva, el empresario podrá ejercer un control tecnológico legítimo sobre sus trabajadores, pero considerando en cada caso y atendiendo a estrictos criterios de idoneidad, necesidad y proporcionalidad, la utilización de medidas de vigilancia y control que, sirviendo a los fines que se pretendan, supongan el menor impacto posible sobre la intimidad y dignidad del trabajador. El derecho a la intimidad, al igual que los demás derechos fundamentales, no es absoluto y puede ceder ante intereses constitucionalmente relevantes, siempre que sea necesario para lograr un fin legítimo, proporcionado y respetuoso con el contenido esencial del derecho.

3. Legitimidad en Chile del despido originado por el control del empleador por uso de las Tecnologías de la Información y las Comunicaciones.

En noviembre del año 2001 el Tribunal Superior de Justicia de Cataluña acogió un recurso de súplica, presentado por el Deutsche Bank, declarando procedente el despido de un trabajador sin indemnización, que envió en el transcurso de 5 semanas 140 e-mail ajenos a la prestación de servicios en horario laboral. Este mismo tribunal, en julio del 2002, estimó que hacer uso excesivo de Internet con fines ajenos al trabajo es causa suficiente de despido.

Los despidos que originaron estos fallos dan cuenta de un conflicto de intereses actualmente existente entre empleador y trabajador, producto del uso de tecnologías de la información en el puesto de trabajo tales como el correo electrónico e Internet. En este conflicto se contraponen, por una parte, la facultad de control que tiene el empleador sobre los trabajadores en el uso de las TICs que utilizan en sus puestos de trabajo, y por otra, los derechos que tienen los trabajadores en el uso de estas tecnologías controladas por el empleador. En los casos antes señalados, para despedir a los trabajadores, el empleador accedió a las cuentas de correo electrónico del trabajador y a sus conexiones a Internet, detectando el uso de estos medios en intereses ajenos a sus labores. Sin embargo, los trabajadores alegaron haber sido afectados sus derechos a la privacidad y a la inviolabilidad de las comunicaciones.

En el derecho comparado este conflicto ya ha sido regulado por ley o se aborda en proyectos de ley actualmente en discusión. En Europa la legislación en esta materia no ha sido uniforme. El Reino Unido, a través de la Ley de Regulación de Poderes de Investigación, de octubre de 2000, permite a los empresarios británicos el acceso rutinario al correo electrónico de sus trabajadores. Alemania, en cambio, promueve legislar en favor del trabajador, prohibiendo a la empresa leer el correo electrónico privado enviado desde el lugar de trabajo. En el caso de Estados Unidos, no existen a nivel estatal y federal normas que prohíban al empleador ejercer este control; en general las empresas han seguido el camino de la autorregulación estableciendo políticas de uso

de las TICs dentro de la empresa. A nivel latinoamericano, en Argentina, la Secretaría de Comunicaciones trabaja en el Anteproyecto de Ley de Protección del Correo Electrónico, mediante el cual se intenta equiparar el correo electrónico a la correspondencia epistolar, contemplando sus autores que en las relaciones laborales la titularidad de los e-mail corresponde al empleador.

En Chile este debate recién está comenzando. No obstante, sin duda, este ya ha tomado fuerza considerando la creciente conectividad a Internet que hoy presentan las empresas en Chile[149] y la entrada en vigencia de distintas reformas laborales que modifican la legislación aplicable en este punto.[150]

- Legitimidad del control del empleador

El poder de dirección y control que tiene el empleador sobre la labor de sus trabajadores se origina por ser el primero el dueño del negocio y por tener la libertad para desarrollar cualquier actividad económica, ambos derechos –propiedad y libertad económica– consagrados en nuestra Constitución. En el caso de la empresa, el poder del empleador se explica también por ser este un organizador de medios personales, materiales e inmateriales, ordenados bajo una dirección, hacia un fin económico, social, cultural o benéfico[151]. Como tal debe velar por la coordinación y buen rendimiento de estos medios así como de su seguridad.

Este poder cobra relevancia con la incorporación de las TICs en los puestos de trabajo de una empresa. En efecto, son conocidas las ventajas en términos de eficiencia y reducción de costos que el uso de las TICs provoca en la empresa. Esto explica el actual acondicionamiento de oficinas básicamente con computadores personales que cuentan con conexión a Internet y aplicaciones de correo electrónico. No obstante, el uso de estas tecnologías puede desviarse fácilmente en contra de los intereses de la empresa o de los mismos trabajadores de esta. Veamos algunos casos:

1) El uso desmedido del correo electrónico y de Internet por parte del trabajador en asuntos personales significa costo para el empleador, no tanto en términos de valor de

[149] A marzo de 2001 el porcentaje de empresas con conexión a Internet era de 61,4% distribuyéndose de la siguiente manera: Micro: 57,6%; Pequeña 77,2%; Mediana 92,7% y Grande 97,2%. Cámara de Comercio de Santiago, Economía Digital 2001, abril 2001, pág. 126

[150] Con fecha 11 de septiembre de 2001 el Congreso Nacional aprobó un proyecto de ley que introduce importantes modificaciones al Código del Trabajo.

[151] Artículo 3° inciso final Código del Trabajo: " ... se entiende por empresa toda organización de medios personales, materiales e inmateriales, ordenados bajo una dirección para el logro de fines económicos, sociales, culturales o benéficos, dotada de una individualidad legal determinada".

conectividad, sino como por desatender el trabajador las labores para las que fue contratado. La novedad y efectividad de estos medios, así como el costo cero que significa para los trabajadores, incentivan a estos su uso en horarios de trabajo perjudicando su productividad.

2) Mientras más trabajadores cuentan con acceso a Internet y correo electrónico más aumenta el riesgo de la empresa de sufrir ataques informáticos tanto desde dentro de esta como desde fuera, sea por culpa o dolo del trabajador. Muchos virus llegan a través de correos personales que reciben los trabajadores y que reenvían a sus compañeros de trabajo.

3) La empresa puede ser responsabilizada civilmente por ilícitos cometidos por sus trabajadores. Injurias, acoso sexual, violación de propiedad intelectual o delitos informáticos, como los tipificados en la Ley 19.223, pueden ser realizados por trabajadores desde sus ordenadores personales que pone la empresa en sus puestos de trabajo. En su calidad de tercero civilmente responsable, al empleador puede exigírsele que indemnice perjuicios si en consideración a su autoridad y el cuidado que su calidad le confiere y prescribe pudo haber evitado que el trabajador cometiera el ilícito que se le imputa[152].

En razón de lo anterior, el empleador entrega hoy al trabajador el uso de estas tecnologías en forma controlada. En algunos casos el uso de las TI es reglamentado dentro de la empresa y el trabajador conoce exactamente los usos que debe dar al correo electrónico y a Internet. En otros, el empleador controla este uso sin saberlo el trabajador. Desde luego, tecnológicamente el empleador puede conocer exactamente cuál es el uso que el trabajador da a su correo electrónico y a Internet. Incluso puede implementar aplicaciones, por ejemplo filtros, que impidan al trabajador acceder mediante Internet a cierta información que el empleador considera vedada.

En nuestra legislación no existe hoy una norma que regule este tipo de control que hace el empleador al trabajador, sea permitiéndolo o no como ocurre en el derecho comparado. No obstante, la Dirección del Trabajo se ha pronunciado en varias oportunidades sobre el alcance que deben tener la medida de control y revisión que disponga el empleador sobre sus trabajadores.[153]

---

[152] Ver artículo 2320 del Código Civil.

[153] Ordinario N° 8381/191, de 16 noviembre 1990; Ordinario N° 1936/124, de 22 abril 1993; Ordinario N° 4842/300, de 15 septiembre 1993; Ordinario N° 287/24, de 11 enero y Ordinario N° 0363/0021 de 25 enero 2001. En este mismo sentido, la Corte de Apelaciones de Concepción, en sentencia confirmada por la Corte Suprema, dispuso el deber de las empresas de velar por la seguridad de las personas y bienes en

Desde el año 1990 la doctrina de la dirección en esta materia ha sido uniforme y complementaria estableciendo que las medidas de control que ejerza el empleador sobre el trabajador deben cumplir a lo menos con los siguientes requisitos:

1) Ser incluidas en el Reglamento Interno de Higiene y Seguridad de la empresa, dictado conforme a la ley, por lo tanto, no cabe ejercer este control sin ponerlo en conocimiento de los trabajadores a través de este medio.

2) Ser idóneas al objetivo de mantenimiento del orden, higiene y seguridad de la empresa y sus trabajadores, no importando actos ilegales o arbitrarios del empleador que afecten derechos del trabajador garantizados constitucionalmente, como la honra, la dignidad y la privacidad de los trabajadores.

3) No pueden tener un carácter prepolicial, investigatorio o represivo frente a supuestos ilícitos dentro de la empresa, sino un carácter preventivo y despersonalizado, siendo requisito su ejecución uniforme respecto de todo el personal de la empresa y en caso de selección, la aleatoriedad de la misma.

La reforma laboral aprobada en el Congreso Nacional el año 2001 ha ratificado esta jurisprudencia, recogiendo al parecer los cambios que ha experimentado la relación laboral en los últimos años con motivo de la incorporación de las TICs a la empresa.

Efectivamente, el texto de este proyecto agrega un nuevo inciso primero al artículo 5° del Código del Trabajo que reza: "El ejercicio de las facultades que la ley le reconoce al empleador, tiene como límite el respeto a las garantías constitucionales de los trabajadores, en especial cuando pudieren afectar a la intimidad, la vida privada o la honra de estos".

En el mismo sentido, el proyecto agrega un nuevo inciso final al artículo 154 del Código del Trabajo que regula las disposiciones que debe contener todo Reglamento Interno de una empresa: "Las obligaciones y prohibiciones a que hace referencia el número 5 de este artículo, y en general, toda medida de control, solo podrán efectuarse por medios idóneos y concordantes con la naturaleza de la relación laboral y, en todo caso, su aplicación deberá ser general, garantizándose la impersonalidad de la medida, para respetar la dignidad del trabajador".

Considerando las normas anteriores, es posible concluir que el control que realiza el empleador sobre el trabajador en el uso de las TICs que opera en su puesto de

---

el recinto de sus establecimiento, siempre que cumpla con lo dispuesto en el artículo 153 del Código del Trabajo consignando el sistema de control en el Reglamento Interno de la empresa. (Corte de Apelaciones de Concepción, 4 noviembre 1997, recurso de protección Sociedad Supermercado Hiperbrisas Limitada y otros con Inspección del Trabajo de Concepción).

trabajo será legítimo si cumple con las limitaciones y condiciones antes señaladas en resguardo de los derechos del trabajador.

- Derechos del trabajador frente al control del empleador

Establecido que el control que hace el empleador al trabajador en el uso de las TICs debe respetar los derechos de este último, corresponde ver ahora qué derechos del trabajador son susceptibles de ser afectados mediante este sistema de control.

1. Derecho a la privacidad y derecho a la inviolabilidad de las comunicaciones privadas

Es preciso distinguir si el trabajador utilizó las TICs en asuntos personales o laborales. En el primer caso, interceptar una comunicación o conocer su contenido es una infracción a la vida privada del trabajador y a su derecho a la inviolabilidad de sus comunicaciones privadas, ambos derechos consagrados en el artículo 19 N° 4 y N° 5 de la Constitución Política. En el segundo caso, las TICs se consideran una herramienta de trabajo puesta a disposición del trabajador para el ejercicio de sus labores contratadas, por lo tanto, en esta situación no se violaría la privacidad del trabajador, sino más bien habría violación a una comunicación privada.

Con todo, en el caso del correo electrónico, se discute si puede ser considerado correspondencia o comunicación privada así nada más. Para que tenga esta calidad y en consecuencia quede amparado su emisor y receptor por esta garantía constitucional, el correo electrónico debiera incluir algún elemento que demuestre que es confidencial o privado, por ejemplo que se envíe encriptado o que para acceder a la cuenta de correo electrónico del trabajador exista una clave de ingreso. Asimismo, es un tema de discusión relevante determinar si en el puesto de trabajo el correo electrónico e Internet son herramientas de trabajo o medios de comunicación como sería el teléfono fijo. Para zanjar esta discusión se recurre a la autorregulación, mediante la cual empleador y trabajador definen la naturaleza de estos acordando cuál es el uso que 'debe darse al correo electrónico y a Internet en el lugar de trabajo.

2. Derecho a la información

En el uso de las TICs el trabajador ejerce su derecho a informar y ser informado en forma libre y por cualquier medio sin restricciones y censura previa. Así lo consagra el artículo 19 N° 12 de la Constitución Política. Pues bien, podrían afectarse estos derechos mediante filtros o aplicaciones computacionales impuestas por el empleador que restrinjan el acceso y envío de esta información o censuren su contenido. Como contraargumento se sostiene que el empleador es el dueño o el responsable del servidor que permite la conectividad a Internet y el uso del correo electrónico y en su calidad de tal puede disponer su uso con las más amplias facultades. En este caso, nuevamente mediante la autorregulación, empleador y trabajador pueden acordar el uso de las TICs de manera tal que no afecte este derecho del trabajador.

3. Derecho a la libertad sindical

En España se ha planteado que medidas de control al uso del correo electrónico por parte de los trabajadores sindicados que impidan o restrinjan sus comunicaciones en interés del sindicato, podrían atentar contra la libertad sindical[154]. En Chile el derecho a la libertad sindical está consagrado expresamente en el artículo 19 N° 19 de la Constitución Política y son consideradas prácticas desleales o antisindicales del empleador las acciones que atenten contra este derecho, especialmente las indicadas en los artículos 289 y siguientes y 387 y siguientes del Código del Trabajo. Cabe destacar que la reforma laboral antes aludida sustituyó el artículo 294 del Código del Trabajo, disponiendo que si una cualquiera de las prácticas desleales o antisindicales mencionadas implica el despido del trabajador no amparado por fuero laboral, este despido no producirá efecto alguno.

4. Derecho a la protección de datos personales del trabajador

Mediante el control que ejerce el empleador en el uso de las TICs por parte del trabajador, el primero puede acceder a datos personales del segundo. El tratamiento que haga de estos datos como su comunicación a terceros solo podrá hacerlo de

[154] Una demanda presentada ante la Audiencia Nacional española por la CCOO (Comisiones Obreras) contra el BBVA puso en el tapete la afectación del derecho de libertad sindical, ya que la demandante alegaba que el BBVA bloqueó sus correos electrónicos a través de un filtro que interceptaba y devolvía las informaciones sindicales enviadas a empleados y afiliados. La Audiencia Nacional rechazó la demanda pero reconoció el derecho de los sindicatos de utilizar sus e mail para hacer llegar sus comunicaciones a los trabajadores

conformidad a lo dispuesto en la ley de protección de la vida privada[155]. Refuerza este derecho el nuevo artículo 154 bis del Código del Trabajo contemplado en la reforma laboral aludida cuyo texto es el siguiente: "El empleador deberá mantener reserva de toda la información y datos privados del trabajador a que tenga acceso con ocasión de la relación laboral".

5. Dignidad del trabajador

La dignidad del trabajador debe ser respetada por el empleador en cada uno de los aspectos de la relación laboral e implícitamente se protege en la medida que se respete cada uno de los derechos del trabajador antes mencionados. Con todo, el deber del empleador de respetar la dignidad del trabajador en el uso de sistemas de control se dispone expresamente en el artículo 154 inciso final del Código del Trabajo, cuyo texto incorpora la reciente reforma laboral en los términos citados anteriormente.

Todos los derechos antes indicados están consagrados constitucionalmente y hoy día el proyecto de reforma laboral los incorpora a la legislación laboral, existiendo entonces un mandato expreso del legislador de ser respetados por el empleador. Junto con lo anterior, debe tenerse en cuenta que estos derechos pasan a tener la categoría de irrenunciables, según dispone el artículo 5° inciso primero del Código del Trabajo que en el texto del proyecto pasa a ser inciso 2°. Por esta razón, sea a través de la autorregulación o cualquier otra forma en que el empleador reglamente el control sobre el trabajador en el uso de las TICs en su puesto de trabajo, no puede significar en caso alguno la renuncia de estos derechos por parte del trabajador.

- ¿Despido justificado o injustificado?

Mediante el control que realiza el empleador sobre el trabajador en el uso de las TICs incorporadas en su puesto de trabajo, el primero puede detectar y considerar que el segundo ha incurrido en alguna de las causales de despido consagradas en el artículo 160 del Código del Trabajo y despedir al trabajador sin derecho a indemnización alguna. Desde luego, el empleador mediante sistemas de control tecnológico podría detectar por ejemplo que uno de sus trabajadores le injuria a través de mensajes que

[155] Ley 19.628 sobre Protección de la Vida Privada.

envía por e-mail dentro y/o fuera de la empresa; o que en forma imprudente abre mensajes de e-mail o se conecta a páginas web que exponen a la empresa al ingreso de un virus afectando su seguridad; o que durante horas de trabajo navega por largos espacios de tiempo en páginas de ocio de la Internet o ajenas al interés de la empresa.

Al hacer efectivo este término de la relación laboral, el empleador además de cumplir con las disposiciones legales sobre aviso de despido y estar al día en el pago de cotizaciones e imposiciones, deberá ser capaz de comprobar que el trabajador ha incurrido efectivamente en alguna de las causales del artículo 160 del Código del Trabajo, puesto que a él corresponde la carga de esta prueba. El empleador, entonces, debe necesariamente encasillar estas conductas del trabajador en alguna de las causales antes señaladas y probarlas. En la medida que así lo haga, el despido será justificado.

Sin embargo lo anterior, demostrar que el despido ha sido justificado no es tarea fácil en estos casos ya que la conducta del trabajador se produjo en un medio virtual o electrónico, no susceptible de acompañarse al tribunal como instrumento privado o público en el cual se consigne una conducta del trabajador, mientras no se le dé valor al documento electrónico homologándolo al documento soportado en papel[156]. En estos casos lo más probable es que se llegue a solicitar una inspección personal de tribunal o un informe de peritos que permitan demostrar la autenticidad de la conducta que motivó el despido, es decir, si fue o no efectivamente el trabajador quien la realizó. Puede también presentarse un documento en que conste impreso el documento electrónico que da cuenta de esta conducta, el que podría constituir una base para una presunción judicial o un principio de prueba por escrito. En todo caso, un punto a favor del empleador es que el tribunal en las causas laborales aprecia estas pruebas conforme a la sana crítica.

Aunque el empleador pruebe que el trabajador incurrió con su conducta en una de las causales del artículo 160 del Código del Trabajo, debe enfrentar un segundo problema cual es la impugnación de su sistema de control por parte del trabajador.

Efectivamente, el trabajador podría alegar ante el juez laboral que el sistema de control ejercido por el empleador era ilegítimo y por lo tanto el despido es injustificado o ineficaz. Al respecto, considero que si el control fuera ilegítimo, por no cumplir con

[156] Debemos considerar que ya existe en la Legislación Nacional la Ley 19.799 sobre firma electrónica donde nos habla sobre el documento electrónico definido en el artículo 2 letra d como "toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior" y establece instituciones certificadoras que dan valor probatorio a un documento electrónico que se encuentra firmado digitalmente.

alguno de los requisitos y condiciones señaladas anteriormente, este hecho no debe afectar el despido. Así ocurre cuando el empleador comete errores u omisiones en las comunicaciones de despido (artículo 162 Código del Trabajo), estas faltas no invalidan la terminación del contrato. Por lo demás, la tendencia del legislador ha sido no quitarle efecto al despido salvo que la ley así lo disponga. Es inválido el despido si el empleador no hubiere efectuado el integro de las cotizaciones previsionales al momento del despido (artículo 162 inciso 4 del Código del Trabajo). También no tiene efecto el despido si este se origina en alguna práctica desleal o antisindical, como prescribe la reforma laboral en su nuevo artículo 294 del Código del Trabajo. Este último caso sería el único en que el control del empleador al ser considerado una práctica desleal o antisindical, podría invalidar el despido originado precisamente por ese control.

Ahora bien, la ilegitimidad del sistema de control podría hacer merecedor al empleador de una multa administrativa impuesta por una Inspección del Trabajo. Asimismo, nada impide que el trabajador impugne el sistema de control y eventualmente accione contra el empleador ante la justicia criminal por el delito de apertura o registro de correspondencia que consagra el artículo 146 del Código Penal, asimilando en este caso un correo electrónico a un correo epistolar. También puede recurrir de protección ante la Corte de Apelaciones respectiva por considerar el control que le ha hecho el empleador como un acto arbitrario o ilegal que priva, perturba o amenaza alguno de sus derechos corno los indicados más arriba.

- Conclusiones

Entendemos que es legítimo el control que hace el empleador sobre el trabajador en el uso que haga de las TICs incorporadas a sus puestos de trabajo. Sin embargo, este control no es ilimitado, debe sujetarse a ciertas restricciones que tienen por objeto velar por el respeto de derechos fundamentales de los trabajadores que pueden verse afectados por este tipo de control

Cómo ejercer este control en forma eficiente respetando los derechos de los trabajadores, es una respuesta que debe dar cada empresa. Al efecto puede optarse por la autorregulación o por otros convenios con los trabajadores, pero deberán seguirse los dictámenes de la Dirección del Trabajo que hemos citado (y uno en particular que analizaremos mas adelante) y considerar las nuevas normas que incorpora la reforma laboral, las cuales son aplicables en esta materia.

Estos sistemas de control pueden permitir al empleador detectar que el trabajador ha incurrido en alguna causal de despido. Proceder al despido en estos casos requiere evaluar la suficiencia de la prueba considerado que la conducta del trabajador por la cual se le despide consta generalmente en un medio virtual. Sin perjuicio de lo anterior, lo más importante es que el empleador previo al despido revise si su sistema de control cumple o no con la legalidad vigente. En caso de no cumplirlo, el despido puede acarrear para el empleador consecuencias más allá de una demanda laboral por despido injustificado, como son multas administrativas, recursos de protección e incluso una querella criminal por violación al derecho de privacidad.

4) Legislación Chilena

A Grosso modo podemos encontrar algunas normas fundamentales relativo a la protección laboral de la privacidad por el uso de las Tecnologías de la Información y las Comunicaciones.

- Constitución Política de la República de Chile

Artículo 19. La Constitución asegura a todas las personas:
5°. La inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley.
24°. El derecho de propiedad en sus diversas especies sobre toda clase de bienes corporales e incorporales.
26°. La seguridad de que los preceptos legales que por mandato de la Constitución regulen o complementen las garantías que ésta establece o que las limiten en los casos en que ella lo autoriza, no podrán afectar los derechos en su esencia, ni poner condiciones, tributos o requisitos que impidan su libre ejercicio.

De estas normas se desprenden lo relativo a protección de la privacidad, tal como lo abordamos en los primeros capítulos de la presente memoria. Sin embargo hacemos referencia además al concepto de derecho de propiedad y garantías de un debido proceso.

- Código Penal

Artículo 146. El que abriere o registrare la correspondencia o los papeles de otro sin su voluntad, sufrirá la pena de reclusión menor en su grado medio si divulgare o se aprovechare de los secretos que ellos contienen, y en el caso contrario la de reclusión menor en su grado mínimo. Esta disposición no es aplicable entre cónyuges, ni a los padres, guardadores o quienes hagan sus veces, en cuanto a los papeles o cartas de sus hijos o menores que se hallen bajo su dependencia. Tampoco es aplicable a aquellas personas a quienes por leyes o reglamentos especiales, les es lícito instruirse de correspondencia ajena.

Artículo 161-A. Inciso Primero: Se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500 Unidades Tributarias Mensuales al que, en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado; sustraiga, fotografíe, fotocopie o reproduzca documentos o instrumentos de carácter privado; o capte, grabe, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público.

Estas normas hacen referencia a la ilicitud en que podría encontrarse un empleador que violente estas mínimas garantías reguladas en estas normas, asimilando lo que es correspondencia con correo electrónico, cuestión que se debate en la doctrina de los autores, llegando a un concenso de hacer iguales ambos conceptos.

- Código del Trabajo

Art 5.° inciso 1° El ejercicio de las facultades que la ley reconoce al empleador, tiene como límite el respeto a las garantías constitucionales de los trabajadores, en especial cuando pudieran afectar la intimidad, la vida privada o la honra de éstos.

Art. 153. Inciso 1° Las empresas, establecimientos, faenas o unidades económicas que ocupen normalmente diez o más trabajadores permanentes, contados todos los que prestan servicios en la distintas fabricas o secciones, aunque estén situadas en localidades diferentes, estarán obligadas a confeccionar un reglamento de orden, higiene

y seguridad que contenga las obligaciones y prohibiciones a que deben sujetarse los trabajadores, en relación con sus labores, permanencia y vida en las dependencias de la respectiva empresa o establecimiento.

Art. 154. El reglamento interno deberá contener, a lo menos, las siguientes disposiciones:
5.- las obligaciones y prohibiciones a que estén sujetos los trabajadores.

Inciso final: Las obligaciones y prohibiciones a que hace referencia el número 5 de este artículo, y, en general, toda medida de control, sólo podrán efectuarse por medios idóneos y concordantes con la naturaleza de la relación laboral y, en todo caso, su aplicación deberá ser general, garantizándose la impersonalidad de la medida, para respetar la dignidad del trabajador.

5) Dictámenes de la Dirección del Trabajo y Jurisprudencia.

Para poder entender la real aplicación de la escasa legislación Chile en cuanto al Uso de las Tecnologías de la Información y las Comunicaciones en el ámbito laboral, relativas a su vez con el control del trabajador y sus límites, es que veremos en un punto diversosdictámenes de la Dirección del Trabajo, analizando uno de ellos que hace referencia a la materia de la presente memoria y verificaremos una jurisprudencia de traibunales.

La mayoría de las situaciones y prácticas que han planteado conflicto en materia de derechos fundamentales y relaciones laborales, se presentan a propósito de la concreción de las facultades que tiene el empleador para dirigir, organizar y administrar su empresa.

De esta forma, podemos apreciar como el amparo que le otorga el ordenamiento jurídico laboral a los derechos fundamentales de los trabajadores, se ha ido construyendo sobre la base de la casuística y de la creación dogmática elaborada a propósito de ésta.

Por lo cual, en esta materia reviste una importancia manifiesta repasar los criterios contenidos en los dictámenes de la Dirección del Trabajo y conocer de esta forma la extensión que nuestra jurisprudencia administrativa le ha otorgado a los distintos derechos fundamentales de los trabajadores.

Esta revisión, sin embargo debe efectuarse desde la óptica del análisis "a contrario sensu", esto es que la Dirección del Trabajo no se pronuncia directamente sobre la extensión y el contenido de los derechos fundamentales del trabajador en el ámbito de las relaciones laborales, sino que por el contrario, la jurisprudencia administrativa de ese Servicio se pronuncia y dictamina respecto de los límites de la actividad directiva de la empresa, estableciendo en definitiva requisitos para que resulten procedentes ciertas actuaciones del empleador en relación con los referidos derechos fundamentales: las medidas de revisión y control deben incorporarse en Reglamento Interno de Higiene y Seguridad; deben ser idóneas a los objetivos perseguidos; no deben tener un carácter prepolicial, investigatorio o represivo; y deben tener un carácter despersonalizado y por último, las acciones sólo pueden ser aquellas contempladas en la legislación laboral para estos efectos.[157]

• Ord. Nº 4.842/300, 15.09.93

"Resulta lícito que el empleador plantee medidas de control y revisión pero es necesario que tales medidas se integren en sistemas que sean compatibles con el respeto de la honra y dignidad de los trabajadores y en función de este objetivo se requiere que los sistemas de prevención sean técnicos y despersonalizados, y que, por ende, se apliquen mediante mecanismos automáticos y de sorteo, que eviten que su operación o funcionamiento se produzca frente a presunciones de actos o conductas ilícitas concretas".

• Ord. Nº 8.273/337, 19.12.95

"Las medidas de control que la ley autoriza, e incluso impone al obligar a ciertos empleadores a dictar un Reglamento Interno de Higiene y Seguridad, deben cumplir con

[157] Las infracciones a las obligaciones contenidas en el Reglamento Interno sólo pueden ser sancionadas, de conformidad al artículo 157 del Código del Trabajo, con multas de hasta un 25% de la remuneración diaria del trabajador.

las siguientes condiciones:

a) Las medidas de revisión y control de las personas, de sus efectos privados o de sus casilleros, al importar un límite a la privacidad de las personas, debe necesariamente incorporarse en el texto normativo que la ley establece para el efecto, esto es, el Reglamento Interno de Higiene y Seguridad de la empresa, dictado en conformidad a la ley.

b) Las medidas de revisión y control deben ser idóneas a los objetivos perseguidos como son el mantenimiento del orden, la higiene y la seguridad de la persona y sus trabajadores, no debiendo importar actos ilegales o arbitrarios por parte del empleador, según lo señala la Constitución en su artículo 20, como por ejemplo la selección discrecional de las personas a revisar o la implementación de medidas extrañas e inconducentes a los objetivos ya señalados.

c) Las medidas, además, no deben tener un carácter prepolicial, investigatorio o represivo frente a supuestos o presuntos hechos ilícitos dentro de la empresa, sino un carácter puramente preventivo y despersonalizado, siendo requisito "sine qua non" para la legalidad de estas medidas de revisión y control, que sean operadas a través de un mecanismo o sistema de selección, cuyas características fundamentales son la universalidad y la despersonalización de las revisiones".

• Ord. Nº 2.309/165, 26.05.98

"... una medida de control de "alcotest" sólo se ajustará a derecho cuando se establece, atendido el número de trabajadores de la empresa, en el Reglamento Interno de Orden, Higiene y Seguridad de la empresa, debiendo señalarse el mecanismo de selección y las garantías de éste para no vulnerar ni debilitar la protección a las garantías constitucionales de los trabajadores revisados".

• Ord. Nº 8.005/323, 11.12.95

"No se ajusta a derecho medida de control del personal denominada "Alcotest" por no estar incorporada a Reglamento Interno y no señalar mecanismo de selección".

• Ord. Nº 252/15, 13.01.88

"No se ve inconveniente para que un empleador recurra a su elección a la utilización de cualquier dispositivo de detección o medida de revisión, siempre que se aplique con ciertas precauciones tendientes a no causar menoscabo de la dignidad y honra de la persona del trabajador".

• Ord. Nº 8.381/191, 16.11.90

"No existe inconveniente para que una empresa, en casos justificados, adopte medidas de prevención destinadas a evitar la comisión de actos que atenten contra la propiedad, seguridad o salubridad, tanto de los trabajadores como del establecimiento, siempre que con ellas no se cause menoscabo a la honra y dignidad del trabajador".

• Ord. Nº 7.572/255, 15.11.91

"El sistema de prevención de hechos delictuales que se desea implantar por la Industria resulta ilegal si se establece en la forma indicada en la consulta, puesto que al pasar el detector de metales por el cuerpo de cada trabajador implica un registro material de su persona que es atentatorio contra la dignidad de aquéllos".

• Ord. Nº 4.958/219, 28.08.92

"El empleador no se encuentra legalmente facultado para ordenar, por sí y ante sí, de acuerdo a sistemas internos de control, la revisión corporal, casilleros y efectos personales de sus dependientes, sin perjuicio del derecho que le asiste de adoptar medidas de prevención que no atenten contra la dignidad y honra de aquéllos, debiendo en tal caso incorporar las obligaciones y prohibiciones en que dichas medidas se traduzcan, en el respectivo reglamento interno de orden, higiene y seguridad, de acuerdo a lo dispuesto en los artículos 149 y siguientes del Código del Trabajo".

• Ord. Nº 1.936/124, 22.04.93

"La instalación de un sistema de circuito cerrado de televisión en las secciones o talleres de una empresa, no infringe ninguna disposición legal vigente, siempre que con ello no se cause menoscabo a la honra y dignidad de la persona y en el Reglamento Interno se

regulen las posibles obligaciones o prohibiciones que de ella deriven".

• Ord. N° 2328/130 de 19.07.2002

1) El reconocimiento del carácter de límites infranqueables que los derechos fundamentales, en particular del derecho a la intimidad, vida privada u honra de los trabajadores, poseen respecto de los poderes empresariales (inciso primero, del artículo 5 del Código del Trabajo), así como la prevalencia que la dignidad de los trabajadores tiene respecto de los mecanismos de control empresarial (inciso final, del artículo 154 del Código del Trabajo), lleva necesariamente a concluir que la utilización de mecanismos de control audiovisual (grabaciones por videocámaras) en los vehículos de la locomoción colectiva urbana, sólo resulta lícita cuando ellos objetivamente se justifican por requerimientos o exigencias técnicas de los procesos productivos o por razones de seguridad de los conductores o de los pasajeros, debiendo ser el control de la actividad del trabajador sólo un resultado secundario o accidental del mismo.
2) Por el contrario, su utilización únicamente como una forma de vigilancia y fiscalización de la actividad del trabajador no resulta lícita, toda vez que supone un control ilimitado, que no reconoce fronteras y que se ejerce sin solución de continuidad, lo que implica no sólo un control extremada e infinitamente más intenso que el ejercido directamente por la persona del empleador o su representante, sino que en buenas cuentas significa el poder total y completo sobre la persona del trabajador, constituyendo una intromisión no idónea y desproporcionado en su esfera íntima, haciendo inexistente todo espacio de libertad y dignidad.
3) Es condición esencial para la implementación de estos mecanismos de control audiovisual, en las circunstancias que ello resulte lícito, el cumplimiento de los requisitos generales de toda medida de control laboral y específicos del medio en análisis.

- Ordinario 0260/0019, de fecha 24 de enero de 2002.

Mediante Ordinario 0260/0019, de fecha 24 de enero de 2002, la Dirección del Trabajo (la "Dirección"), a través de su directora doña María Ester Feres Nazarala, se pronunció sobre si el empleador puede tener acceso al contenido de los correos electrónicos enviados y recibidos por el empleado, a través de un sistema de correo

electrónico de la empresa.

Antes de llegar al pronunciamiento final, la Dirección reconoce la existencia de conflicto entre dos garantías constitucionales. Por un lado, la garantía constitucional de la inviolabilidad de toda forma de comunicación privada, que respaldada por el inciso 1° del artículo 5° del CT, protege al empleado, y por el otro, la garantía constitucional del derecho de propiedad, que otorga al empleador la facultad de organizar, dirigir y administrar su empresa.

Se compara el uso del correo electrónico con el uso de la línea y el aparato telefónico, en el sentido que no por ser el empleador dueño del teléfono, éste pretenderá enterarse del contenido de las llamadas telefónicas de sus dependientes.

Sin perjuicio de lo anterior, la Dirección reconoce el derecho del empleador de regular las condiciones, frecuencia y oportunidad de uso de sus bienes, pero siempre que no se infrinja la garantía constitucional de inviolabilidad de toda forma de comunicación privada. En este sentido, la Dirección no ve inconvenientes en que el uso del correo electrónico sea regulado al interior de una empresa a través del reglamento interno, respetando lo dispuesto en el inciso final del artículo 154, o en empresas de menos de diez trabajadores, a través del contrato individual o el instrumento colectivo, siempre que no se afecte la mencionada garantía constitucional.

La Dirección, por ejemplo, autoriza que se establezca la exigencia que todo envío de correo electrónico por el personal se efectúe con copia a alguna gerencia, privando de esta manera del carácter privado a la comunicación. Sin embargo, deja constancia que dicha regulación no es practicable en el caso de la recepción de correspondencia electrónica, la que conserva siempre su carácter de privada, y por lo tanto es amparada por la garantía en comento.

La Dirección concluye que “de acuerdo a las facultades con que cuenta el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, pero en ningún caso podrá tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores”.

- Análisis de este dictamen:

Podemos concluir diversos razonamientos:

a) La Dirección concluye que en ningún caso el empleador podrá tener acceso a la

correspondencia electrónica privada enviada y recibida por los trabajadores. Por supuesto, si existe correspondencia electrónica privada, debe existir correspondencia electrónica no privada. Por lo tanto, la Dirección no considera a toda comunicación electrónica como privada. Es más, señala claramente que los correos enviados por el empleado con copia a alguna gerencia pierden su calidad de privados, pero los correos recibidos por el empleado serán siempre privados. En conclusión, y de acuerdo a la Dirección, todos los correos electrónicos recibidos por el empleado y aquellos enviados que no deban ser copiados a alguna unidad de la empresa, se encuentran protegidos por la garantía constitucional de inviolabilidad de toda forma de comunicación privada.

b) Entre líneas, lo que la Dirección señala es que aceptará que el reglamento o el contrato individual prohiba al empleado usar el correo electrónico para fines personales, pero no permitirá al empleador poder fiscalizar, es decir, revisar el contenido de los correos, salvo por los correos enviados por el empleado con copia a la empresa.

c) Debido a que esta materia deberá finalmente ser resuelta por nuestros tribunales y/o legisladores, cabe preguntarse si las comunicaciones a través de correos electrónicos son, al amparo del artículo 19 N°5 de la Constitución Política de la República, una comunicación privada per se (como parece ser el caso de las comunicaciones telefónicas), o dicha calificación dependerá del análisis particular del contenido de los mismos. Nadie puede pretender que un sobre dirigido a la empresa con atención al empleado sea una comunicación privada. Igualmente, un correo electrónico que tiene por encabezado alguna referencia a la empresa tampoco podría ser privado. Por lo menos, privar en estos casos al empleador del derecho a revisar ese sobre o correo no parece muy sensato.

Tampoco convence la posición de algunos autores que consideran al correo electrónico como una forma de comunicación no privada, en el sentido de equiparlo a una postal, debido a que el administrador de un servidor de correos puede fácilmente acceder al contenido de los mismos. La facilidad para acceder al contenido no puede ser el elemento que determine el carácter de privado de un correo electrónico, documento, etc.

d) Por otro lado, el artículo 146 del Código Penal sanciona al que abriere o registrare la correspondencia de otro sin su voluntad, por lo cual distingue entre correspondencia

propia y ajena. La correspondencia física enviada con indicaciones claras de guardar relación respecto a la Empresa S.A. pero enviada a nombre del empleado no es correspondencia del empleado, sino de la Empresa S.A., por lo cual no cabría aplicar el tipo del artículo 146 del CP.

e) Finalmente, la conducta de interceptar comunicaciones de carácter privado, en recintos particulares o lugares que no sean de libre acceso al público (la oficina de un empleado en principio no tendría que ser por lo general un lugar de libre acceso al público) no es subsumible en el tipo del artículo 161-A del CP si concurre la autorización del afectado. O sea, con autorización del afectado, podrían interceptarse las comunicaciones privadas. Entonces, concurriendo la voluntad del empleado podría el empleador revisar el contenido de los correos electrónicos?

f) Según el parecer de la Dirección del Trabajo, es admisible regular el empleo que los trabajadores hacen del correo electrónico que les ha sido asignado por la empresa para el desarrollo de sus tareas. Dicha regulación debe contenerse en el reglamento interno de la empresa, que están obligadas a tener aquellas que cuentan con 10 o más operarios; en caso de no estar obligada a contar con reglamento interno, la empresa debía incorporar tal reglamentación en el texto de los contratos de trabajo, con el propósito de informar de antemano a los trabajadores del control que la empresa realiza sobre el correo electrónico que les ha asignado para el desarrollo de sus tareas.

En cuanto a las facultades de que dispondría el empleador para imponerse del uso que el trabajador está dando al correo electrónico, sostiene la Dirección del Trabajo que en ningún caso podrá el empleador tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores. De esta manera, la intromisión del empleador en la correspondencia electrónica privada del trabajador queda resguardada por las acciones civiles y penales del caso, junto con constituir una infracción a las obligaciones que impone el contrato de trabajo, cuya gravedad podría autorizar al trabajador a poner término al contrato con derecho a las indemnizaciones laborales que sean del caso.

De esta manera, la Dirección del Trabajo ha procurado dar los primeros pasos en el medio nacional para establecer un criterio que permita conjugar, entre otros bienes jurídicos, la seguridad requerida por las empresas en el empleo del correo electrónico por sus dependientes y la privacidad de estos en sus comunicaciones personales .

- Ordinario 1147/34, de fecha 21 de marzo de 2005.

Ahora bien, a pesar de la claridad con que se resolvió y aclaró esta situación, con posterioridad, se solicitó a la Dirección del Trabajo la reconsideración de la doctrina contenida en el dictamen Nº 260/019, de fecha 24.01.2002.

La respuesta a esta solicitud, es el ORD.: Nº 1147/34 de 21.03.2005 que en definitiva señala que se niega reconsideración de dictamen Nº 260/019, del 24.01.2002, que estableció las facultades de que disponen los empleadores en materia de control de los correos electrónicos de sus trabajadores y cuyo dictamen dice en resumidas cuentas que del análisis de su solicitud, no se aprecia ningún elemento de juicio que haga, precisamente, apartar a este Servicio de la consideración de que los mensajes electrónicos enviados o recibidos corresponden a correspondencia privada, y por lo tanto, protegidos por la inviolabilidad constitucional de la correspondencia (artículo 19 numero 5 de la Constitución Política del Estado).

Se confirma por tanto la protección desde el punto de vista laboral de la privacidad por el uso de las Tecnologías de la Información y las Comunicaciones /a través del correo electrónico) de los trabajadores.

6. Derecho Comparado.

El año 2001 se publicó en los medios de comunicación la noticia relativa a la aprobación en el Reino Unido de una norma que permitía a los empresarios, entre otras facultades, tener acceso al correo electrónico de los trabajadores.

Dicha noticia reavivó el debate sobre la licitud o ilicitud por parte del empresario de examinar los mensajes de correo electrónico enviados o recibidos por parte de sus trabajadores, cuestión que todavía no ha sido solucionada por parte del legislador.

La implantación de las nuevas tecnologías de la información en las empresas (Internet, correo electrónico, etc.) tiene una doble vertiente ya que si bien se considera indispensable para el correcto y competitivo funcionamiento de cualquier empresa y conlleva muchas ventajas, también comporta unos "usos y comportamientos laborales" de determinados trabajadores que pueden ir en contra de los intereses de la compañía y

considerarse desleales e incluso delictivos.

Es obvio que nos encontramos ante un nuevo marco laboral en el que el uso abusivo del correo electrónico o de Internet puede comportar ciertas actividades por parte de los trabajadores consideradas como situaciones de absentismo laboral, en el supuesto de que el correo electrónico no sea utilizado por el trabajador para tareas exclusivamente relacionadas con la actividad profesional, amén de provocar un potencial riesgo en cuanto a responsabilidades de la empresa frente a terceros.

Pese a la importancia de la cuestión, nos encontramos en la actualidad con un vacío legal dependiendo de la legislación del derecho comparado a considerar, ya que la cuestión sobre si el empresario puede o no puede examinar los correos electrónicos de sus trabajadores no se haya regulada expresamente en los textos legales.

- Caso de España

En este sentido, recientemente tanto la Asociación de Internautas (AI) como Comisiones Obreras (CC OO) (ambas entidades españolas) han pedido la reforma del Estatuto de Trabajadores para que se incluya el requisito previo de autorización judicial para que una empresa pueda examinar los mensajes de correo electrónico de un trabajador.

A falta de una regulación expresa, la respuesta al debate, debemos buscarla en el equilibrio existente entre las facultades que le son reconocidas al empresario en el artículo 20.3 del Estatuto de los Trabajadores "el empresario podrá adoptar las medidas más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana...:", y los derechos que le son reconocidos al trabajador, contrastando lo manifestado con el artículo 4.2 e) del Estatuto de los Trabajadores, que dispone que el trabajador tiene derecho "al respeto de su intimidad y a la consideración debida a su dignidad".

Asímismo, la Constitución Española establece en su artículo 18.3 la garantía constitucional de secreto de las comunicaciones, en particular, las telegráficas, postales y telefónicas; evidentemente se encuentran incluidos los mensajes de correo electrónico.

Pese a que la Ley otorga al empresario capacidad de dirección y control sobre la actividad laboral que realizan sus trabajadores, mediante la adopción de determinadas medidas, ello no puede confundirse con lo que sería una persecución indiscriminada y

absoluta de carácter feudal llevada a cabo por los empresarios, vulnerando sistemática la intimidad de los trabajadores, por ello deben examinarse las particularidades de cada caso.

En este sentido, es interesante la Sentencia de la Sala 2ª de la Sala de lo Social del Tribunal Superior de Justicia de Madrid de fecha 16 de octubre de 1998 dispone en su Segundo Fundamento de Derecho: (vid. Aranzadi AS 1998\3780):

Pasando a los motivos jurídicos, en el primero se denuncia la infracción de los arts. 14 de la Constitución (RCL 1978\2836, ApNDL 2875) y 17.1 del Estatuto de los Trabajadores (RCL 1995\997), si bien luego no se invoca ninguno de los móviles represivos que tipifican estos preceptos sino que simplemente se alega que el actor fue una mera «cabeza de turco» con la que la empresa de modo ejemplarizante decidió combatir una práctica generalizada en la empresa. El motivo ha de rechazarse. La supuesta «práctica» no se desprende del relato histórico de la sentencia. No se puede alegar además tolerancia empresarial cuando la empresa ya había manifestado un año antes su intención de sancionar disciplinariamente las navegaciones irregulares en la red de internet que efectuaron los trabajadores. Las imputaciones que basan el despido por otra parte no se ciñen a las meras «navegaciones» sino que comprenden también el uso del ordenador por el actor para actividades relacionadas con sus propios negocios en otra mercantil. Finalmente hemos de tener en cuenta que el principio de no discriminación sólo juega en los específicos supuestos de los arts. 14 de la Constitución y 17 del Estatuto de los Trabajadores sin que sea posible reconocer un imposible derecho a la igualdad en la ilegalidad como ha tenido oportunidad de establecer el Tribunal Constitucional -S. 21/1992 (RTC 1992\21) y AATC 118/1986 (RTC 1986\118 AUTO) y 27/1991 (RTC 1991\27 AUTO)-.

En la citada Sentencia se pone de manifiesto que la compañía disponía de una red interna a la que se conectaban los ordenadores de la empresa, red que se conectaba con Internet a través de los Proxys que se encontraban en Holanda, donde se registraban todas las conexiones, y se observó pérdida de calidad de la red de la empresa, entre otros motivos "por el elevado tráfico de conexiones, habiendo por ello solicitado datos a los 'Proxis' de los usuarios que más tiempo pasaban conectados a Internet y procediendo a analizar los destinos de las conexiones".

El despido fue motivado debido a que el trabajador se conectaba habitualmente en horas de trabajo a páginas de Internet de diferentes diarios, visitaba páginas web de ocio, charlas de caza o páginas de contenido sexual o pornográfico, etc. Así mismo el

despido también fue motivado porque el trabajador utilizó el ordenador de la empresa para asuntos y negocios particulares, almacenando correspondencia y documentación particular

La más reciente Jurisprudencia entiende como justificado el despido de un trabajador derivado del excesivo y abusivo uso del correo electrónico e Internet para usos particulares y no en cambio para usos exclusivamente profesionales, máxime teniendo en cuenta que la propietaria de los sistemas informáticos es la compañía, evitando de esta forma un bajo rendimiento del trabajador; ahora bien, esta no es la cuestión conflictiva del debate ni la que debe ser analizada o clarificada, lo que realmente debe clarificarse es si el empresario puede o no examinar e inspeccionar el correo electrónico de sus empleados, cuestión esta que no ha sido solucionada, y que es objeto de diferentes opiniones y puntos de vista por parte de la Doctrina.

Con posterioridad, y en el mismo sentido anunciado se pronunció la Sentencia del Tribunal Superior de Justicia de Cataluña, Sala de lo Social, de 14 de noviembre de 2000, caso Deutsche Bank, en el que se calificó como despido disciplinario el uso abusivo y no profesional realizado por un trabajador del correo electrónico de la empresa, si bien cabe destacar que en dicha Sentencia no se analizó cuestión alguna sobre la privacidad o intimidad del trabajador, pese a lo publicado en los medios de comunicación que aseguraban que una Sentencia del TSJC autorizaba al empresario a inspeccionar el correo electrónico de sus empleados.

El derecho que puede tener el empresario a examinar el correo electrónico del trabajador, siempre que previamente se haya advertido al trabajador de dicha facultad, encuentra su justificación diversos aspectos.

Obviamente, tratándose el correo electrónico corporativo de una herramienta cuya propiedad es del empresario y siendo los sistemas informáticos propiedad de la empresa, puede considerarse lícito su examen, si bien no puede olvidare (debido a la falta de regulación expresa actual al respecto) el riesgo que asume el empresario, que puede ser denunciado con posterioridad por parte del trabajador por la comisión de un delito contra la intimidad tipificado en el artículo 197 del Código Penal, tal como ocurrió en el conocido caso "Deutsche Bank".

Otro punto de vista interesente es el siguiente: frente al derecho a la intimidad cabe considerar el artículo 2.2. de la Ley Orgánica de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen "no se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere

expresamente autorizado por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso"

El empresario puede perfectamente implantar en el seno de la empresa una normativa relativa al uso de los sistemas informáticos, en especial el uso de Internet y de correo electrónico. No hay que olvidar que el empresario puede llegar a ser considerado responsable civil por culpa "in vigilando" por determinadas actividades de sus empleados en el uso de los sistemas informáticos, hecho que también justifica un control de los medios de trabajo propios de la compañía, entre los que destacan Internet y el correo electrónico. Entre otras muchas razones el control del empresario sobre el correo electrónico de sus empleados también puede estar motivado por posibles comportamientos delictivos consistentes en la revelación de secretos y en definitiva del Know-how, fugas de información valiosa propia de la compañía, delitos contra la propiedad intelectual, etc.

Se entiende que el debate debe ceñirse únicamente al caso de cuentas de correo electrónico propiedad de las empresas o las denominadas corporativas, ya que en el caso de cuentas de correo electrónico que no los son de la compañía sino del trabajador, parece unánime la opinión de que no puede el empresario controlar dichas cuentas, por ejemplo una cuenta privada, como "hotmail".

Recientemente, un grupo de trabajo de la Unión Europea, ha realizado un informe derivado de determinadas cuestiones de la Directiva 95/46/CE (protección de datos), relativo a vigilancia y control de las comunicaciones en el lugar de trabajo, parece ser que los estados van a involucrarse en legislar tan delicada cuestión en el futuro.

En dicho informe se formulan una serie de recomendaciones a tener en cuenta por parte de los empresarios sobre dichas cuestiones, el trabajador debe estar avisado de las posibles medidas de vigilancia futuras, siendo la finalidad de la observación determinada y legítima.

- Caso de Estados Unidos

Las condiciones y limitaciones impuestas al uso por los trabajadores del correo electrónico suministrado por la empresa, así como las facultades de que dispone el empleador para ejercer control sobre ello se han constituido en un problemas jurídico recurrente en aquellos países donde la penetración de las nuevas tecnologías ha dado pie

a su aplicación empresarial.

En Estados Unidos, donde no existe una adecuada protección legal para el uso de e-mail por los trabajadores[158], se han planteado numerosos casos jurisprudenciales sobre despidos fundados en el uso inapropiado de la red[159], los que han sentado doctrina en orden a salvaguardar la privacidad del trabajador, en tanto este disponga de una "expectation of privacy" o "esperanza razonable de privacidad" y no se encuentren comprometidos intereses públicos[160]. Al efecto, se ha estimado que una simple comunicación escrita al trabajador del empleador, en orden a que su correo electrónico puede estar controlado, rebaja las expectativas de intimidad y legitima la intromisión de éste en la correspondencia de sus empleados[161]. Tal doctrina ha sido objeto de duras críticas por la corrosión que importa para las libertades individuales, la falta de consideración hacia la dignidad del trabajador y las desventajas competitivas que origina para la actividad empresarial[162].

- Caso de Inglaterra

En Inglaterra, la Regulation of Investigatory Powers Act 2000 facultó al gobierno inglés para elaborar una regulación sobre la interceptación de las comunicaciones de los trabajadores, lo que llevó a la publicación de la controvertida Lawful Business Practice Regulations, que consagra la regla general de que no se debe interceptar las comunicaciones sin consentimiento de estos; no obstante, la regulación admite numerosas hipótesis que legitimarían tal control empresarial, prescindiendo del consentimiento del trabajador, que van desde razones que abogan por la seguridad nacional hasta asegurar el buen funcionamiento del sistema informático de la empresa, y aun para comprobar el cumplimiento de normas de conducta en el seno de ésta[163]. Con posterioridad, the Information Commissioner, autoridad de control para el tratamiento de datos personales, ha emitido un código de conducta, mediante el cual se procura mitigar los efectos de la regulación antedicha.

En el caso de los correos electrónicos, En el Reino Unido, la regulación del uso

[158] Castells, Manuel, "La Galaxia Internet", Areté editorial, España, 2001. Página 200.
[159] Howe, Jeff, "Big boss is watching", Yahoo¡ Internet Life, Octubre 2000
[160] Winters, Steven. "The New Privacy Interest: Electronic Mail in the Workplace", en Berkeley Technology Law Journal, volumen 8 (Spring 1993).
[161] Rosen, Jeffrey, "The erodel self", New York Times Sunday Magazine, 2000, cit. por Manuel Castells.
[162] Winters, Steven, op. cit.
[163] Jeffery, Mark, "¿Carta blanca para espiar a los trabajadores? Perspectivas inglesas sobre poder informático e intimidad, en http://www.uoc.es/web/esp/art/uoc/0109042/jeffery.html (15.07.2002)

de las comunicaciones internas durante el horario laboral ha sufrido un cambio radical. El consentimiento del trabajador ya no es necesario para realizar un barrido de los mensajes que éste haya enviado utilizando los medios puestos a su disposición por la empresa.

Un amplio abanico de posibilidades que los sindicatos británicos rechazan rotundamente y que llevarán ante el Tribunal de Justicia de las Comunidades Europeas por considerarlo una violación de la Convención Europea de los Derechos Humanos, transpuesta al cuerpo legal del Reino Unido .

Esta nueva regulación ha generado un intenso debate en el Reino Unido acerca de hasta donde puede llegar el empresario en su poder de control de las comunicaciones, planteándose su posible confrontación tanto con el artículo 8 (derecho a la privacidad) de la Convención Europea de Derechos Humanos, que entró a formar parte de su ordenamiento jurídico en octubre de 2000 (Human Rights Act), como con la normativa vigente de protección de datos (Data Protection Act).

Ahora bien, cuando analizamos la regulación legal en distintos países en lo relativo al correo electrónico y cuya violación podría atentar directamente contra la privacidad por el uso de las Tecnologías de la Información y las Comunicaciones, tenemos:

- Regulación del Correo Electrónico en Europa

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, viene a derogar la Directiva 97/66/CE, de 15 de diciembre de 1997, relativa al tratamiento de datos personales. Esta nueva Directiva, a través de su artículo 5, impone a los Estados miembros la obligación de garantizar la confidencialidad de las comunicaciones, ("Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el

consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad"). La coletilla de "salvo cuando", viene matizada algo más adelante, en el artículo 15, cuando establece que "1.Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6,en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea."). Se aprecia, por tanto, la supremacía del interés general frente al particular, sobre lo que nada hay que objetar en democracia.

- PORTUGAL

Al igual que otros países, la Constitución de Portugal regula en su artículo 34 la inviolabilidad de la correspondencia ("Artigo 34.º (Inviolabilidade do domicílio e da correspondência) 1. O domicilio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis. 2. A entrada no domicilio dos cidadãos contra a sua vontade só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstos na lei. 3. Ninguém pode entrar durante a noite no domicilio de qualquer pessoa sem o seu consentimento. 4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal"). En el mismo texto legal en su artículo 26 se regula el derecho a la intimidad ("A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à

capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação."). Y en el artículo 32.8 de la Constitución se declaran nulas todas las pruebas obtenidas mediante abusiva intromisión en la correspondencia.

Respecto al control de la forma en que el trabajador utiliza los instrumentos de trabajo disponibles por el Empresario, como teléfono u ordenador, es necesario ponderar varios factores. El Empresario es el titular del derecho de propiedad sobre los instrumentos de trabajo y puede y debe determinar a los trabajadores de los términos de utilización del correo electrónico, sobre todo de las formas de control que implantará.

La Ley portuguesa criminaliza el acceso indebido a las comunicaciones y ya que los mensajes de correo electrónico debemos comprenderlas dentro de las comunicaciones privadas, existen unas disposiciones legales que impiden el acceso a su contenido. La Ley 109/91 sobre Criminalidad Informática regula la interceptación ilegítima de las comunicaciones ("Artigo 8º . Intercepção ilegítima. 1- Quem, sem para tanto estar autorizado, e através de meios técnicos, interceptar comunicações que se processam no interior de um sistema ou rede informáticos, a eles destinadas ou deles provenientes, será punido com pena de prisão até três anos ou com pena de multa. 2- A tentativa é punível."). Por tanto, el Empresario no podrá interceptar las comunicaciones electrónicas de sus trabajadores ni abrir o acceder a los mensajes de correo electrónico, cuando estos mensajes sean de naturaleza privada y no tengan el consentimiento del trabajador.

Con la entrada en vigor el 1 de diciembre de 2003 de la Ley 99/2003, de 27 de agosto, fue aprobado el nuevo Código del Trabajo, que reúne de forma sistemática legislación laboral que estaba diseminada en cerca de cincuenta disposiciones legales de diferentes épocas y concepciones políticas y sociales. En su artículo 21 consagra expresamente, en el contexto laboral, el derecho de confidencialidad del trabajador relativo al contenido de los mensajes electrónicas de naturaleza personal.

- FRANCIA

El Tribunal Supremo francés ha marcado un importante precedente, que "un empresario no puede tener conocimiento de los mensajes personales enviados por un empleado y recibidos por éste a través de una herramienta informática puesta a su disposición para su trabajo" sin violar el secreto de correspondencia. Ni siquiera en los

casos en que el empleador "haya prohibido la utilización no profesional de la computadora". "El trabajador tiene derecho, incluso en su tiempo y lugar de trabajo, al respeto a su intimidad y su vida privada".

En el caso Tareg Al Baho, Ministere Public/ Francoise V, Merc F. et Hans H. El Tribunal de París condenó a los demandados (Directores de una Escuela Superior de Física y Química Industrial de París) por violación del secreto de correspondencia del demandante, porque sospechaban que el mismo estaba siendo usado para fines personales, mas la Justicia francesa entiende que las cuentas de correo electrónico están amparadas por el secreto de correspondencia.

Sobre el despido por parte de Nikon France de un empleado, en octubre de 2001, el Tribunal Supremo Francés equiparó el correo electrónico del empleado, no a su taquilla, sino a la correspondencia, por lo que consideraba ésta inviolable: "un empresario no puede tener conocimiento de los mensajes personales enviados por un trabajador y recibidos por éste a través de un útil de informático puesto a su disposición para su trabajo sin violar el secreto de correspondencia, aunque el patrón haya prohibido la utilización no profesional del ordenador". (Arrêt 02.10.01 Cour de Cassation. SA Nikon France / Frédéric O.)

- ALEMANIA

Alemania tiene una legislación rígida y muy respetuosa con la privacidad y los sindicatos han instado al gobierno a actualizar la protección en la era Internet. Cada lander (estado federal) es el encargado de nombrar a una comisión para la protección de datos, que es la responsable de controlar las actividades del gobierno y de las propias compañías privadas.

- ITALIA

En el artículo 15 de la Constitución se regula que la libertad y el secreto de la correspondencia y de cualquier otra forma de comunicación son inviolables. Su limitación puede venir motivado por un acto motivado de la autoridad judiciaria con la garantía de la ley. ("La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge").

- BÉLGICA

El Convenio colectivo de trabajo n ° 81 del 26 de abril de 2002 relativo a la protección de la vida privada de los trabajadores y al respeto del control de los datos electrónicos de las comunicación en red (Convention collective de travail n° 81 du 26 avril 2002 relative a la protection de la vie privée des travailleurs a l'égard du contrôle des données de communication électroniques en réseau).

El Tribunal de trabajo de Bruselas dictó sentencia el 2 de mayo de 2000, basado en el artículo 8 del Convenio Europeo de Derechos Humanos, entendiendo que el envío de correo electrónico por un trabajador pertenece a su vida privada.

- HOLANDA

La Ley de Protección de Datos Personales de 2001, permite el monitoramiento de las actividades electrónicas de los trabajadores, siempre que haya participación de los Sindicatos o Representantes de los Trabajadores acompañando en la elaboración del control.

- BRASIL

El artículo 5.XII de la Constitución de la República Federativa de 1988 nos dice que es inviolable el secreto de la correspondencia, de las comunicaciones telegráficas, de las informaciones y de las comunicaciones telefónicas, salvo, en el último caso, por orden judicial, en las hipótesis y en la forma que la ley establezca para fines de investigación criminal o instrucción penal; ("é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;")

El artículo 482 de la Consolidación de las Leyes de Trabajo ("Consolidation das Leis Trabalhistas") regula los incumplimientos de las obligaciones por parte del trabajador frente a la facultad de dirección de la empresa.

Por otra parte, el Código Penal en su artículo 151 impone la pena de 1 a 6 meses, o multa al que intervenga indebidamente el contenido de la correspondencia cerrada,

dirigida a otra persona ("Devastar indebidamente o conteúdo de correspondencia fechada, dirigida a outrem") .

En base a esta legislación algunos profesionales del derecho opinaban que estaba prohibido el monitoriamento de los correos electrónicos, exceptuándose los casos en que existe consentimiento del empleado o una orden judicial, según nos indica Lobato de Paiva . Existiendo, sin embargo, como en todos los temas polémicos algunos profesionales que opinaban de diferentes maneras, hasta que se publica la Sentencia del Tribunal Regional de Trabajo TRF-DF-RO 0504/2002. Acordão 3º Turma, en la que el juez Douglas Alentar Rodrigues en su voto no reconoce la existencia del derecho a la privacidad en la utilización de equipos de trabajo concebidos para ejecutar funciones generadas por contrato de trabajo y que la herramienta de correo electrónico concedido por la empresa para el ejercicio de las actividades laborales no hay que equipararla con las correspondencias postales o telefónicas, que son objeto de tutela constitucional del artículo 5º inciso XII de la Constitución.

Pero según la reciente sentencia del Tribunal Superior de Trabajo de 18 de mayo de 2005 publicada el 10 de junio de este mismo año (NÚMERO ÚNICO PROC: rr-613/2000-013-10-00 PUBLICAÇÃO : DJ - 10/06/2005 PROC. Nº TST-RR-613/2000-013-10-00.7 ACÓRDÃO 1ª Turma. Joa Oreste Dalazen, Ministro Relator del Proceso. JOD/rla/jc PORVA ILÍCITA. "E-MAIL" CORPORATIVO. JUSTA CAUSA. DIVULGAÇÃO DE MATERIAL PORNOGRÁFICO) las empresas brasileñas tienen derecho a vigilar el correo electrónico de sus empleados .

Las empresas brasileñas tienen derecho a vigilar el correo electrónico de sus empleados, según una sentencia del Tribunal Superior de Trabajo (TST) de Brasil, de la que informa una revista especializada en asuntos jurídicos.

El trabajador utilizaba su correo electrónico para enviar fotografías de mujeres desnudas a sus compañeros y la empresa lo despidió. En su reclamación el trabajador alegó que la empresa obtuvo de forma ilegal las pruebas para justificar su despido invadiendo su intimidad. Argumento que fue aceptado por un juez de primera instancia, que consideró que la empresa había obtenido las pruebas de forma ilegal. Esta decisión fue anulada por el Tribunal Superior de Trabajo que dio la razón a la Empresa.

El Tribunal Superior de Trabajo consideró que los principios constitucionales que garantizan el secreto de la correspondencia y el derecho a la privacidad se refieren a comunicaciones estrictamente personales y no a comunicaciones empresariales. ("Os sacrosantos directos do cidadão à privacidade e ao sigilo de correspondencia,

constitucionalmente asegurados, concernem à comunicação estritamente pessoal, ainda que virtual ")

Argumenta el juez que la cuenta de correo electrónico ofrecida por la empresa puede ser definida jurídicamente como "una herramienta de trabajo", admite que pueda utilizar el correo electrónico para fines particulares pero en forma "comedida" y observando la moral y las buenas costumbres. ("Solução diversa impõe-se em se tratando do chamado "e-mail" corporativo, instrumento de comunicação virtual mediante o qual o empregado louva-se de terminal de computador e de provedor da empresa, bem assim do próprio endereço eletrônico que lhe é disponibilizado igualmente pela empresa. Destina-se este a que nele trafeguem mensagens de cunho estritamente profissional. Em princípio, é de uso corporativo, salvo consentimento do empregador. Ostenta, pois, natureza jurídica equivalente à de uma ferramenta de trabalho proporcionada pelo empregador ao empregado para a consecução do serviço").
En relación con el código secreto que el empleado tienen para entrar en su correo, opina el juez que no sirve para garantizar el sigilo de su correspondencia, sino para evitar que terceros tengan acceso a informaciones de la empresa.
Ante la ausencia de normas específicas para el uso del correo electrónico de empleados en Brasil, el juez citó casos de otros países como EE.UU. y el Reino Unido.

- ARGENTINA

La Ley 20.744 de Contrato de Trabajo contempla en su capítulo VII los derechos y deberes de las partes en su artículo 62 ("Las partes están obligadas, activa y pasivamente, no sólo a lo que resulta expresamente de los términos del contrato, sino a todos aquellos comportamientos que sean consecuencia del mismo, resulten de esta ley, de los estatutos profesionales o convenciones colectivas de trabajo, apreciados con criterio de colaboración y solidaridad"). Impone un principio de buena fe del empleador y del trabajador en su artículo 63 ("Las partes están obligadas a obrar de buena fe, ajustando su conducta a lo que es propio de un buen empleador y de un buen trabajador, tanto al celebrar, ejecutar o extinguir el contrato o la relación de trabajo") y determina las facultades de organización del empleador en su artículo 64 ("El empleador tiene facultades suficientes para organizar económica y técnicamente la empresa, explotación o establecimiento") y vela por los derechos personales del trabajador en su artículo 65 ("Las facultades de dirección que asisten al empleador deberán ejercitarse con carácter

funcional, atendiendo a los fines de la empresa, a las exigencias de la producción, sin perjuicio de la preservación y mejora de los derechos personales y patrimoniales del trabajador")

Existe un Anteproyecto de Ley de Protección del Correo Electrónico, encomendado por la Cámara Argentina de Comercio Electrónico (CACE) a su Comité Asesor. (Consulta Pública. Resolución S.C. Nº 333/2001 -10/09/2001)

- ECUADOR

La Constitución Política de la República de Ecuador, aprobada en 1998, reconoce el derecho a la inviolabilidad de la correspondencia en su artículo 23.13 "23 Sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes: 13. la inviolabilidad y el secreto de la correspondencia. Esta sólo podrá ser retenida, abierta y examinada en los casos previstos en la ley. Se guardará el secreto de los asuntos ajenos al hecho que motive su examen. El mismo principio se observará con respecto a cualquier otro tipo o forma de comunicación" ("Artigo 23.- Sem prejuízo dos direitos estabelecidos em sua constituição e em seus instrumentos internacionais vigentes, o Estado reconhecerá e garantirá as pessoas o seguinte: 13- A inviolabilidade e o segredo da correspondência. Esta só poderá ser retida, aberta e examinada nos casos previstos na lei. Será guardado em segredo os assuntos alheios ao feito que motivem seu exame. O mesmo princípio será observado com respeito a qualquer outro tipo de forma de comunicação").

La transmisión de datos a través del correo electrónico se halla amparada por el derecho fundamental a la intimidad y a la inviolabilidad y al secreto de las correspondencia establecidos en el artículo 23 nº 8 y nº 13 de la Constitución ecuatoriano, y en el artículo 11 nº 2 y 3 de la Convención Americana sobre Derechos Humanos.

Al igual que en la mayoría de los países, se configura una posible confrontación entre el derecho a la intimidad del trabajador sobre el contenido y el uso del correo electrónico y la potestad que tiene todo empresario o empleador a proteger sus medios organizativos patrimoniales y a dirigir y controlar la actividad laboral de sus trabajadores.

En la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos,

no se regula expresamente el uso del correo electrónico en las empresas, si bien de la lectura de los artículos 3 (confidencialidad y reserva) y 9 (protección de datos) interpretaríamos que la transmisión de mensajes electrónicos están protegidos por la confidencialidad y la reserva, sin embargo la misma ley establece varias excepciones, siendo una de ellas la existencia de una relación laboral. Esta excepción pueda dar lugar a una mala interpretación y conferir a empresarios y empleadores la peligrosa potestad de intervenir y revisar el correo electrónico de sus empleados sin su previo consentimiento.

- COLOMBIA

La Constitución de Colombia modificada en 1991 dispone en su artículo 15: "La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley". ("A correspondência e demais formas de comunicação privada são invioláveis. Só podem ser interceptadas ou registradas mediante ordem judicial, e nos casos e com as formalidades estabelecidas em lei").

- PERÚ

La Constitución Política de Perú de 1993 en su artículo 2.10 consagra el derecho a la inviolabilidad de la correspondencia: "Toda persona tiene su derecho: Al secreto y a la inviolabilidad de sus comunicaciones y documentos privados. Las comunicaciones, telecomunicaciones o sus instrumentos sólo pueden ser abiertos, incautados, interceptados o intervenidos por mandamiento motivado del juez, con las garantías previstas en la ley. Se guarda secreto de los asuntos ajenos al hecho que motiva su examen.".("10. O segredo e a inviolabilidade de suas comunicações e documentos privados. As comunicações, telecomunicações e seus instrumentos só podem ser abertos, incautos, interceptados ou sofrerem intervenção através de ordem judicial motivada do juiz, com as garantias previstas em lei").

- VENEZUELA

La Constitución de la República Bolivariana de Venezuela de 1999 regula en su articulo 48 la garantía del secreto e inviolabilidad de las comunicaciones privadas: "Se garantiza

el secreto e inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso". ("Será garantido o direito ao segredo e inviolabilidade das comunicações privadas em todas as suas formas. Não poderão ser interferidas sem ordem de um Tribunal competente, com o cumprimento das disposições legais e preservando-se o segredo privado que não guarde relação com o correspondente processo").

- BOLIVIA

El artículo 20 de la Constitución Política del Estado regula la inviolabilidad de la correspondencia: "I. Son inviolables la correspondencia y los papeles privados, los cuales no podrán ser incautados sino en los casos determinados por las leyes y en virtud de orden escrita y motivada de autoridad competente. No producen efecto legal los documentos privados que fueren violados o substraídos. II. Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones y comunicaciones privadas mediante instalación que las controle o centralice."

La Ley de Modificación del Código Penal nº 1768 de 10 de marzo de 1997 en su capítulo XI. Delitos informáticos, artículo 363 bis nos indica que: "El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días". Artículo 363 ter.: "El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días".

CAPITULO VIII Protección de los datos y privacidad en Internet.

"En Microsoft estamos firmemente convencidos de que el único y más importante uso de la tecnología de la información es mejorar la educación".
Bill Gates

1. Conceptos generales, introducción

Resulta ya obvio hacer referencia a la revolución que ha supuesto la informática y la tecnología, y las posibilidades de digitalización de la información (ya sea en forma de textos, imágenes, animaciones o sonidos), para su posterior almacenamiento, manipulación o transmisión, de cara al tratamiento de datos de carácter personal.

Internet ha incrementado las posibilidades anteriores gracias a la interconexión de equipos informáticos y de bases de datos, la descentralización y crecimiento de redes, y, especialmente, por el hecho de reunir, en un instrumento interactivo y multidireccional, el mayor número de usuarios que puede englobar un medio. Los avances en Internet han obligado a aumentar la capacidad de los ordenadores, han permitido el desarrollo de nuevas vías de negocio así como de nuevas formas de Marketing1, si bien a la vez se han puesto de manifiesto también vulnerabilidades y faltas de seguridad importantes.

Junto a esto, el carácter transnacional de Internet (multitud de servidores desperdigados por el globo) y los problemas de jurisdicción y competencia judicial, dificultan el control y aplicación de gran parte de las garantías legales que pretenden, de algún modo, regular los contenidos o el flujo de datos a través de la red.

2) Protección de usuarios de Internet en los servicios de comunicaciones electrónicas.

En la actualidad nos encontramos ante una nueva situación tecnológica, social, económica y jurídica, que ha sido denominada comúnmente como "Sociedad de la Información", que abre múltiples posibilidades y va unida a importantes cambios en las conductas de los operadores jurídicos. Ahora bien, la implantación y desarrollo de este nuevo fenómeno tropieza con algunas incertidumbres jurídicas, producto de la aparición de un nuevo escenario, una nueva realidad social no contemplada en la normativa vigente y que, sin embargo, es necesario incorporar, estableciendo un nuevo marco jurídico que ofrezca claridad y seguridad a los diferentes actores intervinientes, al tiempo que la confianza necesaria para lograr una práctica equiparación del mundo real y el mundo virtual. En este sentido, las normas de cualquier ordenamiento jurídico en materia de protección de datos de carácter personal se proyectan sobre los servicios de la Sociedad de la Información, ya que el uso de Internet implica riesgos para el derecho a la protección de datos, en el sentido de que se generan importantes datos que sin el consentimiento de los afectados pueden ser almacenados por terceros.

La protección de la privacidad y el secreto de las comunicaciones son derechos constitucionalmente reconocidos, cuya relevancia nadie pone en duda. Pues bien, la protección de la intimidad y de los derechos a ella ligados plantea retos cada vez más novedosos, en la medida en que las nuevas tecnologías de la información permiten no sólo nuevas formas de comunicación, sino también, paralelamente, más modos de interceptar las comunicaciones.

Como señala el profesor ÁLVAREZ CIVANTOS[164], hay veces en las que uno piensa perderse en un lugar en el que nadie pueda localizarle, sin dar más explicaciones. Esto que pudiera parecer cosa fácil, hoy día puede calificarse de prácticamente imposible, aún cuando creamos que no le hemos comentado a nadie nuestro paradero.

Más allá de nuestra familia, novia o amigos de confianza, siempre hay alguien que conoce donde estamos, aunque nosotros no seamos conscientes de ello. Ese alguien es nuestro banco. Sea cual fuere el lugar del mundo en el que nos encontremos nuestro banco conocerá nuestra situación desde el mismo momento en que utilicemos nuestra

[164] ÁLVAREZ CIVANTOS, Oscar Jo sé, "Normas para la implantación de una eficaz protección de datos de carácter personal en empresas y entidades", Ed. Comares, Granada, 2001, pp. 1-3

tarjeta de crédito, medio de pago que más que usual se ha convertido en imprescindible compañero de viaje. Al hacer un cargo con nuestra tarjeta, nuestro banco conocerá no sólo en que lugar del mundo nos encontramos, sino también lo que hacemos; eso sí, nosotros seguiremos creyendo que nadie lo sabe, pues en muchas ocasiones, nos falta conciencia de que estamos suministrando nuestros datos, lo cual no nos importará ya que en el cambio ganaremos en calidad de vida y comodidad.

En efecto, nuestro banco conoce más de nosotros que la mayor parte de nuestros amigos y familiares. Conocerá nuestros hábitos en cuanto a compras, nuestra suscripción a una revista de una u otra tendencia ideológica, el colegio al que van nuestros hijos, nuestro partido político, nuestra salud, y en general todo lo que, de una forma u otra, comporte una implicación económica.

Si toda la información que nuestro banco tiene de nosotros fuera utilizada de forma incontrolada, podríamos decir que nuestra intimidad habría pasado a dominio de personas ajenas a nosotros mismos.

El caso de los bancos no es el único en el que cedemos datos sin darnos cuenta. Hoy día, la proliferación de las nuevas tecnologías permite tratamientos de datos que apenas podemos imaginar y que permitimos, a veces, de manera inadvertida. El simple hecho de hacernos con una cuenta de correo electrónico o convertirnos en usuarios de un proveedor de servicios de Internet, requerirá que con carácter previo el cumplimiento de un formulario en el que insertaremos datos como nuestro nombre, dirección, profesión o aficiones. De forma inocente, llegaremos a pensar que dicho servicio se nos concede de forma gratuita, pero en realidad estaremos pagando un precio más alto que el que pagaríamos, en dinero, por dicho servicio. Estaremos vendiendo una parte de nuestra intimidad.

Los formularios de recogida de datos en Internet, además, levarán aparejada de forma casi accesoria una o varias cláusulas por las que aceptaremos que nuestros datos sean tratados con fines publicitarios o cedidos a terceras empresas. A esto se puede unir el seguimiento que por medios técnicos pueda hacer el proveedor de servicios de las páginas y contenidos a los que accedemos. Con toda esta información, el proveedor de servicios además de nuestros datos personales podrá extraer un perfil exacto de nuestros gustos y aficiones, a los que podrá dar un uso sobre el que no tendremos control alguno.

La era de las nuevas tecnologías nos exige la máxima prudencia en el uso que de nuestros datos hagamos y requiere la adopción de medidas que permitan el control del uso de los mismos por terceras personas, empresas y corporaciones. Las empresas y

entidades tienen como reto adaptarse a las necesidades de intimidad de sus clientes y empleados, encontrando en la adopción de medidas de seguridad y en el respeto de los derechos de toda persona, no una obligación sino una oportunidad de mejorar el producto o servicio respecto del de sus competidores y de lograr un beneficio de imagen.

En esta línea, la Comisión Europea publicó, el pasado 2 de marzo de 2004, los resultados del último eurobarómetro sobre protección de datos en la Unión Europea, centrado en la visión que los ciudadanos europeos tienen en relación con el tratamiento de sus datos personales por organizaciones públicas y privadas.

Así, el 60 % de los ciudadanos europeos se manifiestan preocupados en cierta medida por la protección de su privacidad. En el caso español, sólo un 13 % afirman estar muy preocupados por el tema, frente a más del 50 % en Grecia y Suecia.

Las organizaciones consideradas más fiables en relación con el tratamiento de datos personales son las sanitarias, policiales, agencias de recaudación de impuestos y entidades financieras. En el lado opuesto se situarían las empresas de comercio por correspondencia, emisores de tarjetas de crédito y compañías de seguros.

Igualmente, nueve de cada diez europeos afirman su deseo de ser informados sobre el tratamiento de sus datos personales y las cesiones que de los mismos se pueden realizar, y dos tercios desconocen la existencia de autoridades independientes para el control de los tratamientos de datos personales.

- Formas de Vulneración del Derecho a la Protección de los Datos de carácter Personal en Internet..

Como señala la profesora LLÁCER MATACÁS[165], el tratamiento informático de aspectos parciales de nuestra persona, como los gustos y aficiones, los hábitos de compra o el poder adquisitivo, es una fuente de información que, en manos de terceros, puede perjudicar el libre desarrollo de la personalidad o provocar la denegación de derechos; así, p. ej., la Carta de Derechos Fundamentales de la Unión Europea, firmada en Niza, el 7 de diciembre de 2000, ha individualizado en su artículo 8, el derecho a la protección de datos de carácter personal que pasa a formar parte del orden público europeo y de los derechos de sus ciudadanos. La privacidad ha entrado en la categoría

[165] LLÁCER MATACÁS, Mª Rosa, "La Protección de los Datos Personales en Internet", en "La regul@ción del comercio electrónico", Dykinson, Madrid, 2003, pp. 158-190.

de los derechos humanos en la medida que garantiza libertades ulteriores como la de obtener trabajo, un crédito o de optar o acceder a determinados servicios: en definitiva, devuelve al individuo el control sobre su entorno y garantiza la sostenibilidad del desarrollo; si bien es cierto que el propio Tribunal Constitucional español, en su Sentencia 292/2000, de 30 de noviembre, indicaba el objeto y contenido propios del derecho fundamental a la privacidad –derecho fundamental que como tal es inherente a la persona e indisponible–, señalando que protegía un conjunto de datos de carácter personal, no necesariamente íntimos o incluso públicos, que por su capacidad de ser tratados por medios informáticos arrojan un perfil de la persona y cuyo uso puede lesionar los derechos de los ciudadanos.

En Internet el deber de información que corresponde al responsable del fichero se manifiesta por medio de la política de privacidad que se debe de incluir en un lugar visible del sitio web. En dicha política de privacidad el responsable del fichero deberá informar a los afectados a los que se soliciten datos de carácter personal de modo expreso, preciso e inequívoco:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
- De su Política en cuanto a la cesión o no de los datos a terceras personas y de la solicitud del afectado de su consentimiento para tal menester.
- De la destrucción de los datos almacenados para el caso de extinción de la entidad responsable del fichero.
- De las cláusulas que aclaren cómo debe realizar el afectado la prestación de su consentimiento para la recogida de sus datos de carácter personal.
- Del uso de mecanismos complementarios de recogida de datos o información de sus visitas, como, por ejemplo, puede ser la efectuada por medio de las cookies.
- De las cláusulas eximentes de responsabilidad por el tratamiento de datos que

efectúen otros sitios web a las que pueda acceder desde la del responsable de los ficheros al cliquear sobre un link, un banner o sobre cualquier otro enlace ubicado en la web con esta finalidad.

- De las cláusulas que determinen el plazo de vigencia de la política de privacidad y de la forma en que se habrá de producir y comunicar el cambio de la misma.
- De la mención de los derechos de los menores en el tratamiento de sus datos de carácter personal y de la necesidad de que el consentimiento para que él mismo sea concedido por sus padres o tutores.

- Aplicaciones de Internet susceptibles de revelar datos de carácter personal

Cuando se habla de aplicaciones de Internet nos estamos refiriendo a todas aquellas herramientas de Internet en las que se recoge información del usuario, con o sin su consentimiento y, debemos distinguir entre los tratamientos visibles – herramientas de Internet en las que se recoge información de los usuarios con su consentimiento, esto es, aquellos elementos donde se recoge información sobre los usuarios claramente en la red– y, los tratamientos invisibles –tratamiento de datos personales sin conocimiento por parte del usuario, ya que más allá de los datos nominativos que circulan en la red, hay otros que el usuario normal no puede aprehender directamente, a pesar de que su valor de información y los riesgos que representan para la vida privada son importantes. En este sentido, existen diferentes dispositivos técnicos muy útiles para asegurar la protección de la vida privada del usuario; así, p. ej. el usuario podría fijar los parámetros en su ordenador de acuerdo a su propia sensibilidad y la utilización de estos datos personales por las webs visitadas o por el proveedor de acceso que deben someterse a las opciones indicadas. También cabría la posibilidad de la utilización de las técnicas del anonimato, esto es, la posibilidad de que el individuo quiera pasearse y actuar libremente como en su vida cotidiana real, ya que él debe poder conservar el anonimato en la Red para ir y venir, realizar pagos, enviar cartas, etc.[166] Siendo necesaria, en todo caso, la necesidad de una educación de los usuarios a partir del conocimiento de los usos y de los riesgos, que vaya más allá de la simple formación del individuo sino traduciéndose en la posibilidad de elección por parte del individuo del modo de

[166] Un sondeo reciente organizado en los EEUU llegaba a la conclusión de que un 82 % de los usuarios está a favor del anonimato –que podría realizarse a través de un pseudónimo-, pero sólo el 52 % para los pagos anónimos.

protección de sus propios datos, ya sea a través de dispositivos técnicos de autoprotección, denuncias, etc.

- Los tratamientos visibles de los datos

Los tratamientos visibles o herramientas de Internet en las que se recoge información de los usuarios –que permiten extraer el perfil del usuario– son, básicamente, los siguientes:

- Los grupos de noticias.
- El correo electrónico.
- Las guías web.
- Los formularios y cuestionarios.

- Los grupos de noticias

Los grupos de noticias, newsgroups o simplemente news, es un servicio de Internet que le permite al usuario participar voluntariamente en intercambios de opiniones acerca de los temas más dispares, con personas de todo el mundo. Un grupo de noticias es como un tablón de anuncios acerca de un tema, donde los usuarios que están suscritos a él pueden recibir los mensajes que hay en él y enviar los suyos propios para expresar sus opiniones.

La información de los usuarios puede ser capturada de diferentes formas:

a.- Captura de datos identificativos del usuario (nombre del usuario, dirección electrónica, servidor del grupo de noticias, nombre de usuario y contraseña, nombre de la cuenta o tipo de conexión) a través de software de búsqueda.

b.- A través de motores de búsqueda (por ejemplo, el motor de búsqueda X 500) que permiten localizar al suscriptor e incluso los mensajes que ha enviado (que pueden estar disponibles durante meses o años).

- El correo electrónico

La World Wide Web (WWW) y la Transmisión de archivos (FTP) son, junto con el correo electrónico (e-mail), los tres servicios principales de Internet. El correo electrónico es una forma de enviar y recibir mensajes entre usuarios de Internet, de

forma parecida a la correspondencia postal, utilizando para ello una dirección única para cada uno de los usuarios. El correo electrónico presenta algunas ventajas con respecto al correo postal, ya que es mucho más rápido y también más barato.

De un tiempo a esta parte el e-mail se ha convertido en una importantísima herramienta de marketing.[167] Todos los usuarios de Internet hemos recibido en alguna ocasión mensajes de correo electrónico no solicitados de alguien que no conocíamos, la mayoría de las veces con anuncios y publicidad.[168] Este tipo de mensajes enviados de forma masiva e indiscriminada es lo que denominamos "correos basura", "chatarra" o "spam".

Los internautas de todo el mundo padecen desde hace diez años el correo basura que inventaron casi sin querer Laurence Canter y su esposa, y que se ha convertido en

---

[167] En este sentido, el pasado 17-4-2004 leíamos en la prensa que Google, el primer buscador del mundo, tenía la intención de lanzar un email gratuito con capacidad de un gigabite, cien veces mayor que el que ofertan sus principales competidores, como Microsoft y Yahoo!. Esta prestación permitiría a los internautas conservar todos sus mensajes durante años, sin necesidad de borrar por limitaciones de espacio. El secreto de esta oferta, actualmente en pruebas, consiste en que la compañía está dispuesta a explotar comercialmente el envío de publicidad a los usuarios de su correo, de acuerdo con las palabras clave que estos escriban en sus mensajes. Por ejemplo, si un internauta comenta sus vacaciones de Semana Santa con un amigo, ambos serán incluidos en una base de datos como potenciales clientes de agencias de viajes, compañías aéreas u hoteleros. La ambiciosa oferta ha provocado la reacción instantánea de asociaciones de consumidores, que interpretan la estrategia de Google como una actividad próxima al espionaje, ya que husmea en los mensajes de los particulares para enviarles publicidad. Los fundadores de Google, Sergey Brin y Larry Page, han recibido una carta pidiendo la suspensión del lanzamiento hasta que se aclare o cambie su política de privacidad. No obstante, ellos argumentan que el sistema se limita a escanear los mensajes de forma automatizada, donde en ningún momento interviene la participación de las personas. En cualquier caso, la controversia está servida. Por un lado, el super email gratuito sería una oferta muy interesante para los usuarios, pese al precio que se cobre a través de publicidad teledirigida. Por otro, los reguladores procurarán preservar la legalidad y los derechos de los usuarios, esto es, podría darse el caso de que "el consumidor no tenga la última palabra", como presuponen los promotores de la iniciativa, al suponer una amenaza a los derechos fundamentales de las personas, y un peligroso antecedente que otras empresas o instituciones podrían utilizar en el futuro. En todo caso, este sistema vulneraría la LOPD, que reconoce el derecho de los usuarios a oponerse al tratamiento de sus datos con fines publicitarios, independientemente de que éste se realice de forma automatizada o no. También indica que esta práctica atentaría contra el derecho de los usuarios a oponerse al tratamiento de sus datos con fines publicitarios, también atentaría contra la prohibición de enviar publicidad no autorizada y la catalogación como datos especialmente protegidos de toda información que revele cualquier aspecto relativo a la ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual. No obstante, desde Google apuntan que la ida de permitir a los usuarios de Gmail optar por entrar o no en el servicio de publicidad era una idea todavía en estudio

[168] Recientemente la compañía Internet Net Value destaca que, desde enero a diciembre de 2001, el promedio de correos recibidos por internauta en España pasó de 31.6 a 42.5, con un contenido publicitario creciente (del 15.2 al 20.3 %). En cuanto a la fuente de los correos promocionales, se encuentran en primer lugar los emitidos por Proveedores de acceso a Internet (ISP), seguido de Portales de Internet, telecomunicaciones y software.

Menos mal que el e-mail no ocupa un lugar físico, porque en caso contrario estaríamos inundados de papeles. La firma investigadora Júpiter Media Metrix señala que, en 2006, los usuarios recibirán 206 mil millones de mensajes de este tipo, un promedio de 1.400 por persona, muy por encima de los 700 de 2001. Este volumen preocupa a las empresas, habida cuenta del tiempo de trabajo que estiman que se pierde en abrir y/o borrar estos documentos. En Estados Unidos han tomado medidas al respecto y algunas empresas prohíben a sus empleados todo e-mail desconocido proveniente de regiones enteras de Asia, desde donde operan servidores no regulados que se dedican a retransmitir mensajes "chatarra".

un grave problema para la red. A “la pareja más odiada de la Red” como la llamó en un reportaje de portada la revista Time, se le atribuye el dudoso honor de haber enviado diez años atrás lo que se considera el primer correo electrónico basura, posteriormente conocido como spam. El despacho de Arizona Canter & Siegel de los abogados Canter y su entonces esposa, la fallecida Martha Siegel, destapó la caja de los truenos cuando lanzó publicidad sobre la lotería que da acceso a un permiso para trabajar en EE.UU., también conocido como la green card en inglés. El anuncio, que después pasaría a los anales de la ciber-historia como el green card spam, se difundió entre más de 5.000 grupos de noticias y enfadó a muchos internautas que contestaron al correo no solicitado con airadas respuestas. La idea que nació como un experimento, según el propio Canter, cambió el espíritu de la Red para siempre: Internet pasó de ser una herramienta utilizada sobre todo en círculos académicos a una potente arma que los vendedores de crecepelo y de hipotecas a bajo interés comenzarían a utilizar sin ningún reparo. Mientras, la pareja de abogados autores del libro Cómo hacer una fortuna con la súper autopista de la información, publicado en 1996, vio su negocio incrementarse en 100.000 ó 200.000 dólares gracias a la tremenda difusión del anuncio. Diez años después, el spam causa pérdidas anuales de unos 200.000 millones dólares en recursos y tiempo malgastados, sin que se hayan encontrado respuestas definitivas a la plaga. Gigantes informáticos de la talla de America Online, Microsoft o Yahoo buscan soluciones de tipo técnico al problema, complementarias a la primera ley federal para frenar a los spammers, la denominada Can spam, que entró en vigor el pasado enero.

Unos 7.300 millones de correos basura –un email que no suele ir personalizado, que es masivo, cuyo destinatario no es conocido y que no se ha solicitado– circularon a diario por la Red en 2003, lo que supone entre el 45 % y el 60 % de los email enviados cada día en todo el mundo. Y este año se mandarán 9.000 millones de spam diarios. Se trata de una lacra que el año pasado provocó pérdidas económicas por valor de 8.000 millones de dólares a las empresas de EE.UU., 2.500 millones a las europeas y otros 500 millones a los proveedores de servicios de la Sociedad de la Información. Tecnología anti-spam para filtrar emails, listas de identificación de spammers y proveedores, medidas legales e incluso cobrar por enviar emails, en determinadas condiciones se han planteado como propuestas para mejorar el servicio.

Dado que el spam tiene un modelo económico que funciona –no tiene costes de impresión, de distribución, de envío, es fácil acceder a listas de emails y con un pequeño índice de éxito resulta rentable– hay que hacer que no sea rentable. La idea parece que

no es cobrar a los spammers para hacer dinero, sino que al obligarles a pagar o hacerles perder tiempo mediante un proceso de confirmación de envíos, no les sea rentable enviar spam, que es un delito. Se busca combatir el correo basura desde el origen y no eliminarlo sólo en el buzón del usuario con software como el MSN, Trend Micro, Symantec o Network Associates, entre otros. En el mejor de los casos parece que estas técnicas podrían reducir el spam, como mucho, en un 95 %, porque siempre habrá spammers nuevos, técnicas mejores o el riesgo de considerar spam correos que no lo son.

En España, el frente anti-spam está representado por la Ley de Servicios de la Sociedad de la Información –LSSI– que prevé multas graves de entre 30.000 y 150.000 euros por el "envío de más de tres comunicaciones comerciales no solicitadas en un año"[169], y la iniciativa "PePi-II.com"[170] avalada por la Asociación de Usuarios e Internet – AUI–, un intento oficial para identificar los envíos masivos de correos y erradicarlos. Tiene el apoyo del Ministerio de Ciencia y Tecnología y de diferentes empresas informáticas con el fin de tratar de identificar al remitente del spam y, una vez detectado, poner en marcha un sistema de alarma entre las compañías. En definitiva, el objetivo es que la gente no deje de usar el correo electrónico por el spam, porque el email es el motor de Internet.

- Las guías web

Se trata de páginas web dedicadas total o parcialmente a la difusión en Internet de guías de alumnos, miembros de asociaciones profesionales, abonados o de personas, que figuraban con más frecuencia sobre otros soportes, papel o telemático.

[169] La LSSI ha tomado como referencia la Directiva 2002/58/CEE que prohíbe el envío de comunicaciones comerciales no solicitadas a personas físicas en toda la UE, salvo en el marco limitado de las relaciones entre clientes y empresas. La normativa se basa en el principio de consentimiento previo y de que es lícito camuflar o disimular la identidad del emisor, además de que todos los correos deben mencionar una dirección de respuesta válida donde el abonado pueda oponerse al envío de mensajes posteriores. De hecho, todos los correos enviados a direcciones conseguidas sin conocimiento de los destinatarios son considerados ilegales y cada Estado miembro puede imponer multas por ello. Bruselas se ha visto obligada a abrir en diciembre pasado procedimientos d infracción contra países como Francia, Bélgica, Holanda, Luxemburgo, Portugal, Finlandia, Suecia y Alemania por no cumplir los plazos previstos en esta normativa, por lo que ahora urge a los Estados miembros a tomar las decisiones oportunas ante este fenómeno

[170] Se trata de un Consejo para luchar contra el spam y buscar soluciones para evitar los problemas que provoca la recepción de mensajes no deseados a las empresas y particulares. El Consejo se reunirá mensualmente y tiene por objeto debatir y encontrar propuestas para luchar contra los abusos del correo electrónico de forma consensuada, establecer procedimientos y canales de información que agilicen la resolución de incidencias y tener voz y representatividad en los foros internacionales

Las guías web quedan dentro de lo que podríamos denominar "fuentes accesibles al público"(censos promocionales,[171] repertorios telefónicos y listas de personas pertenecientes a grupos profesionales) y, el problema sigue siendo el tratamiento que se dé a esos datos personales de los internautas.

- Los formularios de Internet

Nos estamos refiriendo a los formularios que rellena el internauta inscribiendo su dirección de correo electrónico, identidad, número de teléfono, dirección, profesión, ingresos, etc. Así, por ejemplo, el formulario a cumplimentar en páginas web que hacen sorteos entre sus clientes (el objetivo de la empresa es hacerse con los datos del cliente e introducirlos en una base de datos que pueden ser utilizados con fines de promoción y comercialización de los servicios de la compañía) o los Portales de Internet (Terra-Telefónica, Navegalia-Vodafone, etc.) que ofrecen servicios gratuitos (acceso, correo electrónico, alojamiento de páginas web, etc.) que exigen cantidad de datos personales sin una política clara de protección de los mismos.

- CONCLUSIONES FINALES

En resumen, parece evidente que las nuevas tecnologías permiten no sólo nuevas, más fáciles y más sofisticadas formas de comunicación, sino también, y como contrapartida, la posibilidad técnica de que se produzcan más injerencias en las mismas. Ahora bien, como ya hemos comprobado, si bien es cierto que Internet no es un vacío jurídico en materia de tratamiento informatizado de datos de carácter personal y la protección de la intimidad, no es menos cierto que: a) La protección efectiva de la intimidad en Internet necesita de una acción combinada entre poder público y actores privados; b) Es necesaria la combinación de la regulación y la autorregulación por parte de los actores de Internet; c) En la medida en que las respuestas nacionales son insuficientes, en ocasiones, se pone de manifiesto la necesidad de cooperación internacional.

La realidad empieza a parecerse peligrosamente a la ficción. En mayo de 2001, David Brin, prolífico autor de novelas de ciencia-ficción, pronosticaba que "la

[171] ORTEGA GIMÉNEZ, Alfonso, "Censo promocional y consentimiento del afectado ", en IURIS. Actualidad y Práctica del Derecho, núm. 68, La Ley, Madrid, Enero 2003.

tecnología podrá vencer cualquier barrera que establezcamos para proteger nuestra intimidad. En el futuro, será posible, por ejemplo, camuflar un cámara en una mosca artificial". Ni siquiera cuando nos encontramos tranquilamente navegando por Internet desde el ordenador de casa estamos libres de la prospección y el cotilleo ajenos. Algunos hábitos de conducta ante el ordenador nos convierten en fáciles víctimas del mirón cibernético. Una de las más recientes modalidades de ataque es el llamado spoofing, que consiste en engañar a un usuario de correo electrónico haciéndole creer que recibe un mensaje de una persona conocida. En algunos casos, como uno reciente entre usuarios de Yahoo! es solicitar datos secretos, como el número de tarjeta de crédito, haciéndose pasar por gentes autorizados de una compañía de la que se es cliente. En otros casos, lo que se pretende es sabotear determinadas actividades, como en el caso del Comité Español de Solidaridad con la Causa Árabe que vio como un spoofer se hacía pasar por su presidente para desacreditar sus actividades, o bien aquellos usuarios que recibieron mensajes supuestamente enviados desde las oficinas del Foro de Ermua para solicitar fondos solidarios que debían ingresarse en una cuenta corriente.

El uso de Internet implica riesgos para el derecho a la protección de datos de carácter personal, en el sentido de que se generan importantes datos que sin el consentimiento de los afectados pueden ser almacenados por terceros. Como ha quedado comprobado el mundo en Red no es símbolo de vacío jurídico en materia de datos de carácter personal, sin embargo, la protección efectiva de estos derechos necesita una acción combinada del poder público y de los actores privados, pues, en definitiva, ninguna solución nacional es plenamente eficaz. Así, por ejemplo, una posible solución al spam podrían ser, por ejemplo las Listas Robinson[172], en las que se podrían inscribir aquellos ciudadanos que no quieran recibir publicidad vía email o aquellos que, por el contrario, estén dispuestos a que a diario le bombardeen el buzón de correo electrónico, teniendo en cuenta que, como ha señalado la propia AEPD en numerosas ocasiones, "el primer defensor de nuestros derechos debe ser el propio ciudadano". Además, no olvidemos que "el consumidor español es poco exigente pues

[172] En el mundo real la Lista Robinson más numerosa fue creada en 1992 por la FECEMD, donde se agrupa más del 90 % de las empresas del sector. También es una paradoja que las empresas que se dedican al marketing directo y al comercio electrónico sean las primeras interesadas en promover estas listas de personas poco receptivas a los mensajes promocionales, ya que evitan que la publicidad que envían se pierda con consumidores que no tienen el más mínimo interés por ella. Ahora bien, las Listas Robinson no eliminan el buzoneo de impresos sin dirección, revistas gratuitas y, en general, la publicidad de empresas no adheridas a este servicio.

todavía no hay conciencia consolidada de la importancia que tiene hacer valer el derecho a la intimidad, a la privacidad y a la protección de datos, ya que todavía se facilitan datos con demasiada frecuencia, sin demasiadas cautelas, a veces incluso con cierta ingenuidad".

Respecto de las aplicaciones de Internet susceptibles de revelar datos de carácter personal, a algunas conclusiones podríamos llegar: Primera, el riesgo que plantean los grupos de noticias es doble: por un lado, la posible venta de datos identificativos a empresas y, por otro lado, la elaboración de perfiles de usuarios. En este sentido, las recomendaciones a seguir serían las siguientes: primera, el Principio de auto-responsabilidad, esto es, hay que tener cierta cautela a la hora de dar nuestros datos personales cuando nos suscribimos a un grupo de noticias y ser consciente de a quién facilitamos nuestros datos personales y con qué finalidad; y, segunda, el uso de medidas de seguridad como el cifrado de datos para proteger los mismos de accesos no deseados; Segunda, respecto del contenido de los mensajes enviados o recibidos con el correo electrónico es texto, aunque se puede añadir archivos que pueden almacenar cualquier tipo de información (sonidos, imágenes, animaciones, programas, etc.). Además de la posible captura de estos datos identificativos del usuario a través de softwares de búsqueda, se pueden plantear otros problemas: a) La vulneración del derecho al secreto de las comunicaciones –derecho que aunque se suele presentar por la doctrina como una manifestación del derecho a la intimidad goza de cierta autonomía hasta alcanzar la consideración de derecho independiente–; y, b) La seguridad en las transmisiones, en la medida en que el problema que se puede plantear es la interceptación del correo electrónico por terceros; Tercera, parece claro que respecto de las guías web, los abonados pueden oponerse –previamente a la difusión de datos en Internet así como posteriormente en cualquier momento– gratuitamente y sin tener que justificarse a la difusión en una red internacional abierta de los datos que los atañan; Cuarta, la solución respecto de los formulario y cuestionarios pasaría por establecer la necesidad de informar previamente de modo expreso, preciso e inequívoco a los interesados a los que se soliciten datos personales cuando se utilicen cuestionarios u otros impresos para la recogida. No obstante, el riesgo sigue siendo la creación de perfiles de usuarios y, la solución pasa, entonces, por no dar datos improcedentes o innecesarios (ideología, religión o creencias, etc.), o bien, como "solución de andar por casa" cumplimentar esos formularios o cuestionarios con datos falsos; Quinta, los datos recogidos en un "archivo log" no pueden ser desvelados sin el consentimiento del interesado, aunque, en la

práctica suponen un cierto peligro aquellos Proveedores de acceso de Internet que ofrecen una cuenta de correo electrónico a cambio de datos personales, siendo, en todo caso, una posible solución la consideración de esos contratos entre Proveedores de acceso Internet y usuarios contrarios al orden público; y, Sexta, las cookies son útiles para agilizar la navegación pues permiten reconocer un mismo usuario durante su sesión con un mismo sitio o en sus consultas posteriores sin tener que reiterar datos. Pueden ser cookies de sesión o permanentes si permanecen y se conservan en el ordenador, no identifican necesariamente a una persona pero existen grados de acotación, y pueden colocarse a criterio de los sitios web o destinarse a terceros, empresas de cybermarketing, mediante hipervínculos invisibles. En este sentido, las recomendaciones a tener en cuenta serían las siguientes: 1ª) Ser consciente de que los servidores que visitamos pueden registrar las páginas web a las que accedemos, la frecuencia y las materias por las que buscamos, aunque no nos informen de ello; y, 2ª) Utilizar las últimas versiones de los programas navegadores, que incorporan las mejores medidas de seguridad.

No obstante, parece conveniente abrirle en esta materia la puerta a la autorregulación. Es positiva la regulación de la Red pues se deben fijar las "reglas de juego" pero, no debemos olvidar que la normativa que regule este fenómeno debe estar en permanente construcción porque la propia realidad de Internet así lo requiere. Es obvio que es necesaria una regulación mínima y flexible pero, al mismo tiempo, que garantice la libertad de la Red y, le aporte el grado de confianza que demanda la sociedad. En este sentido, a la hora de enfrentarnos a la regulación de Internet, las recomendaciones que podríamos hacer serían las siguientes: a) No se hace necesario crear un Derecho específico de Internet; b) Se debe combinar la regulación estatal con la Autorregulación; c) Debemos desarrollar la cooperación interestatal para hacer respetar el Derecho sobre las redes digitales; d) Se deben definir orientaciones estratégicas comunes que aseguren la presencia española en las negociaciones internacionales referentes a Internet y a las redes digitales; y, e) Hay que hacer todo lo posible para poner en marcha un dispositivo de vigilancia y de observación jurídica de las redes digitales. En cuanto a la intervención de los Estados para regular la Autorregulación, teniendo en cuenta el perfil más regulador de la UE y, la apuesta decidida de los EE.UU. por la Autorregulación, parece que en ambos continentes se habla de corregulación, esto es, de cooperación entre la "regulación pública" y la "autorregulación privada". Aunque parece claro que, en general, los Estados y, en

particular, las empresas, actualmente, reconocen, en mayor o menor medida, la utilidad de la autorregulación, pues sin confianza no hay negocio en la Red. Es evidente que, hoy por hoy, los empresarios son conscientes de que todavía no hay suficiente confianza en estas nuevas formas de comercio y, la consecución de un entorno de seguridad para los consumidores es imprescindible para el desarrollo del comercio electrónico.

3) El anonimato en Internet como Utopía

"Para gozar íntimamente y para amar se necesita soledad, mas para salir airoso se precisa vivir en el mundo". Estas palabras escritas por Stendhal en el siglo XIX, presentan un conflicto en el que permanentemente nos encontramos: el respeto de la privacidad vs. la exposición pública de nuestra vida. Por esa razón, las consideramos válidas para describir, en el siglo XXI, la situación que experimentan los usuarios de servicios de Internet, en particular, cuando buscan información diversa navegando por los contenidos de la web.

Si observamos lo que a diario nos presenta la publicidad, los estudios que se han escrito, los medios de comunicación y, principalmente, nuestra propia experiencia encontraremos que la mayoría de los cibernautas sólo desarrollan su actividad en la red de forma realmente libre y espontánea dentro de un marco de individualismo –de "soledad"-, que les permita ir de vínculo en vínculo, de página en página, de contenido en contenido, diseñando un camino virtual personal en Internet que, a su vez, les lleve a conectarse con otros, a convivir en el mundo, siendo así fieles a su propia naturaleza social.

Esa necesaria soledad –usando la expresión del novelista francés-, ha llevado a que la doctrina propugne el reconocimiento de un derecho específico emergente para los usuarios de Internet: un derecho al anonimato, en cuya virtud se permita no dejar indicios electrónicos en la comunicación por la red, por ejemplo mediante el uso de seudónimos, procedimientos criptográficos o el empleo de filtros. Además, atendida su estrecha vinculación, se le considera como un elemento esencial en el sistema de

protección de datos personales en Internet[173].

Se trata, entonces, de reconocer de forma jurídica que el anonimato en un entorno en línea - a diferencia de las comunicaciones en persona (off-line)-, aparece espontáneamente natural al cibernauta que lo pretende en su calidad de tal porque, al menos en un principio, el esfuerzo radica en el establecimiento de la real identidad del usuario de Internet[174]. Así, la anonimia puede ser concebida como una facultad que exige ser respetada para que, consecuencialmente, haga frente a las desigualdades de trato que se dan en ciertos contextos, basadas en criterios raciales, sexuales o de apariencia física. Además, pretende facilitar la participación de personas que en ciertas actividades pueden ser más propensas a no decir lo que piensan, a menos que el sistema les garantice la ocultación de sus señas.

En tal sentido, el anonimato de las comunicaciones aparece como un tema relevante, ya que está vinculado no sólo a la vida privada y la protección de datos, sino también a otros derechos como la libertad de expresión de los usuarios y el derecho a la inviolabilidad de las comunicaciones privadas. En el primer caso, el anonimato facilita el participar libremente en la red sin temor a ser seguido por las opiniones que se emitan; y en el segundo, permite mantener la confidencialidad, sin interceptación o vigilancia, a menos que esté autorizada por ley.

Sin embargo, lograr una navegación anónima por la web no es del todo posible y a ratos parece algo utópico, no sólo por los intentos políticos de intervenir las comunicaciones electrónicas por razones de seguridad y defensa nacional, persecución de delitos, y primacía del interés público[175], sino porque técnicamente esta red abierta permite investigar el camino seguido por un usuario, debido a los rastros accesibles que

[173] Corripio Gil-Delgado, María de los Reyes. Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet. Premio de la Agencia de Protección de Datos, Madrid, 2000, pp. 20; 183-1 97.

[174] Johnson, Deborah G., Ética On-line. La ética en las redes informáticas. Moralia Nº20, 1997, pp. 77-78; 81-82.

[175] Dicha intervención se ve justificada por estos intereses superiores a los individuales, siempre que guarde proporcionalidad, tenga un carácter excepcional y esté limitada temporalmente, situación que no se admite, en cambio, en las interceptaciones realizadas por el sector privado, incluso sancionadas penalmente en el artículo 2 de la ley Nº 19.223 ("El que con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio"). Lamentablemente, la intervención estatal se ha visto agudizada por los atentados terroristas sufridos por Estados Unidos, quien ha involucrado a importantes países desarrollados en lo que, a nuestro juicio, es una maniquea, contradictoria y violenta campaña contra el terrorismo, que en el plano de las comunicaciones electrónicas se traduce en fuertes restricciones a los derechos individuales de los cibernautas, como la privacidad, y más aún de derechos emergentes como el del anonimato

va dejando en los nodos[176] por los que pasa[177].

Lo anterior ha llevado a que los usuarios de Internet se vuelvan transparentes como el cristal sin proponérselo y sin poder evitarlo por mucha resistencia que ofrezcan, ya que dichas huellas permiten conocer las conexiones que han establecido, los contenidos seleccionados, con quienes se comunican, a qué hora, por cuánto tiempo, desde dónde, en qué lugar se encuentran físicamente los terminales que utilizan, cuáles son sus gustos, sus necesidades, qué escriben, qué compran, qué piensan... en fin, sin duda, mucho más de lo que se desearía al navegar por la web[178].

A esta traba técnica que afecta al anonimato se suman las razones económicas que van detrás, ya que para hacer efectivo este derecho se requiere como primer paso, que la industria se anime a desarrollar y usar tecnologías y estándares que minimicen la necesidad de procesar datos personales, permitiendo convertir en anónimas las huellas electrónicas[179]. Sin embargo, este cambio en las empresas no se ve muy claro y auspicioso dado el valor que presenta la información nominativa utilizada por el marketing relacional o one to one, actividad clave para el comercio electrónico, pero en ocasiones, realizada de modo excesivo.

En efecto, esta legítima y necesaria actividad puede llevar a la realización de algunas conductas que consideramos abusivas de la libertad de información y vulneradoras de la vida privada. Por ejemplo, mediante la utilización de los almacenes de datos o datawarehouse y, particularmente, a través de las técnicas de análisis como la

[176] Un nodo es, en general, cualquier computador, periférico o dispositivo –como un teléfono celular- conectado directamente a una red.

[177] Cada vez que un cibernauta visita un sitio web se registra un dato en un archivo log del servidor. Ellos tienen programas para transformar esa cantidad de archivos en una información clara, analizando, por ejemplo, el orden por el cual las páginas web han sido visitadas, dando cuenta así de los intereses y decisiones adoptadas durante las visitas. Esta acción puede no lesionar la privacidad en la medida en que se utilicen los datos disociadamente, es decir, no puedan asociarse a una persona determinada o determinable. Sin embargo, en otras ocasiones lo que realmente interesa es conocer la identificación de quienes acceden, por ejemplo, para marketing directo y ahí es necesario aplicar un sistema de protección de datos nominativos.

[178] La Agencia de Protección de Datos de España en su memoria de 2000 indica que, sobre la base de su experiencia, las actividades que utilizan Internet como medio de recogida o tratamiento de datos personales son el comercio electrónico, los portales de contenidos diversos, los prestadores de servicios de telecomunicaciones, la recopilación de direcciones, la gestión de anuncios, las páginas web de temas diversos, las empresas convencionales que han instalado algún tipo de servicio en la red, y la gestión de moneda virtual. Agrega que los tipos de datos de carácter personal que se recogen en las actividades recién mencionadas son datos de mera identificación (nombre, apellidos, dirección de correo electrónico), datos de características personales (fecha de nacimiento, sexo, nacionalidad), datos académicos y profesionales (formación, titulaciones), datos de circunstancias sociales (aficiones y estilo de vida), datos de detalles de empleo (profesión, datos no económicos de remuneraciones, historial del trabajador), datos económico-financieros (tarjeta de crédito, datos bancarios), y datos de transacciones (bienes y servicios recibidos por el usuario).

[179] USER'S DECLARATION. European Ministerial Conference. Bonn, 1997. Forum Information Society Report 1997, p.66

minería de datos o datamining se explota una enorme cantidad de datos desordenados obtenidos de fuentes diversas -de acceso público, del tráfico y la facturación por el uso de dichos servicios de telecomunicaciones, de la relación comercial establecida entre las partes, de tratamientos invisibles u otras-, lo que permite descubrir relaciones sutiles u ocultas entre elementos que constituyen la información de las bases de datos, y luego generar modelos predictibles derivados de ellos.

Por lo tanto, nos adentramos en una problemática circunscrita al respeto de derechos de los cibernautas que se ven fácilmente desconocidos en el ambiente on-line, a causa de la dificultad técnica, política y económica para mantener una situación que permita la navegación libre, espontánea y personal por la web, como podría acontecer si existiera un anonimato efectivo en la red.

En ese contexto, el respeto a los derechos de los cibernautas lo abordaremos en relación con el momento en que un tercero recoge datos de un navegante en Internet, especialmente cuando ello ocurre de modo oculto al usuario, sin su conocimiento ni consentimiento, a través de dispositivos técnicos que operan automáticamente al navegar, operación denominada como tratamientos invisibles.

- La recolección de Información a la luz de los principios de la protección de datos.

El problema del tratamiento de datos en Internet y, en especial, cuando no se realiza de un modo transparente al usuario radica en la cantidad de información nominativa de éste que otros pueden conocer cuando utiliza servicios de la red. No sólo nos referimos a los datos que directamente conciernen a una persona natural identificada, como su nombre o su dirección, sino también a aquellos que pueden vincularse indirectamente a un individuo mediante un simple cruce de datos con los archivos de clientes de los proveedores de acceso, por ejemplo.

En efecto, no hay que olvidar que al comenzar una sesión en Internet[180], el ISP (Proveedor de Servicios de Internet) asigna a cada usuario un número único (conocido como IP dinámico) y anota los tiempos de conexión en unión con este número, formando una base de datos. En otro listado almacena la identificación de los usuarios y

[180] Una sesión comienza cuando se solicita una página en un sitio web determinado y termina cuando el usuario decide cerrar el programa de navegación, apagar el computador o solicitar una página de otro sitio web

su número. Esta dirección IP dinámica aparece en todas las páginas que se visitan en la web, permitiendo deducir el proveedor y el país del cibernauta, e incluso analizando los logs es posible localizar desde qué número de teléfono llamó, el día y hora, o qué terminal es. Por lo tanto, cuando se cruza la base que contiene datos de conexión con los números IP y se les vincula con los usuarios, se revelan datos de carácter personal.

En tales circunstancias, la protección de la privacidad en Internet necesita fortalecerse principalmente al momento de la recolección de datos, sean estos recabados del propio titular, de fuentes accesibles al público o del procesamiento de "información persistente del cliente", es decir, de datos relacionados con el computador del usuario y que permanecen más de una sesión en el equipo informático –denominado "cliente"-. La razón de este refuerzo estriba en que una vez reunidos los datos personales de los cibernautas, aquellos quedan fuera del control de su titular y, por aplicación del principio de territorialidad de la ley, si circulan transfronterizamente –como suele ocurrir en Internet-, el marco jurídico del país de origen podría no tener fuerza totalmente vinculante. No obstante, este último es un tema que, pese a su importancia e interés, no desarrollaremos en este trabajo porque escapa del objeto central de nuestra investigación.

Nos parece relevante propender hacia una recogida respetuosa de los principios básicos reconocidos en los sistemas de protección de datos personales. Al respecto, la ley Nº 19.628, sobre protección de la vida privada, pese a todas sus imperfecciones[181], reconoce que el tratamiento sólo puede efectuarse cuando el titular consienta expresamente en ello (artículo 4 inciso primero); se le informe debidamente del propósito del almacenamiento de sus datos y su posible comunicación al público (artículo 4 inciso segundo); se utilicen los datos sólo para los fines para los cuales hubieren sido recolectados (artículo 9 inciso primero); y siempre que la información sea exacta, actualizada y responda con veracidad a la situación real del titular de los datos (artículo 9 inciso segundo). En definitiva, las disposiciones precedentes contienen un deber de información y los principios que la doctrina denomina como calidad de los datos, consentimiento del titular y finalidad del tratamiento.

Dichos principios, vinculados con un tratamiento leal y legítimo, se encuentran reconocidos en el Convenio 108, de 1981, suscrito en Estrasburgo por el Consejo de Europa, relativo a la protección de las personas con respecto al tratamiento

[181] Críticas que ya fueron analizadas en el capítulo IV de esta memoria.

automatizado de datos de carácter personal, uno de los primeros pilares jurídico-positivos de carácter internacional sobre la materia. En su artículo 5 dispone que los datos de carácter personal que sean objeto de un tratamiento automatizado se obtendrán y tratarán leal y legítimamente; se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con éstas; serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; serán exactos y si fuera necesario puestos al día; y se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Catorce años después la misma norma se repite, ahora en la Directiva[182] 95/46/CE del Parlamento Europeo y del Consejo, sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en cuyo artículo 6.1 establece lo siguiente:

Art. 6.1. Los Estados miembros dispondrán que los datos personales sean:

a) tratados de manera leal y lícita.

b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; [...]

c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.

d) exactos y, cuando sea necesario, actualizados; [...]

e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. [...]

Además, la Directiva agrega en el artículo 7, como principio relativo a la legitimación del tratamiento de datos, que el interesado haya dado su consentimiento de forma inequívoca.

Finalmente, nos parece interesante mencionar como demostración de un criterio que ha permanecido por los años lo dispuesto en la Carta de Derechos Fundamentales

[182] La Directiva es un tipo de norma comunitaria que obliga al Estado miembro destinatario, en cuanto al resultado a obtener, dejando a éste la elección de la forma y medios a emplear. Su objetivo principal es la aproximación entre las legislaciones de los distintos Estados de la Unión. En virtud de las mismas los Estados miembros deben adecuar su legislación a las normas comunitarias, suprimiendo, modificando o generando normas adecuadas. Lo vinculante es el objetivo comunitario a alcanzar, no la forma y medios. Una Directiva puede ser de efectos directos para los ciudadanos del Estado. Ull Pont, Eugenio. Derecho público de la informática (Protección de datos de carácter personal). UNED Ediciones, Madrid, 2000. pp. 295-296.

de la Unión Europea, la cual, en diciembre de 2000 estableció en su artículo 8 que toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan; que estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley.

De conformidad con lo anterior, una recogida leal de datos en Internet supone que quien los colecte despliegue toda la diligencia necesaria para cumplir las condiciones de licitud, los obtenga de forma totalmente transparente y prevenga los riesgos que ese acto puede conllevar para el titular de los datos. En particular, la lealtad debe venir referida a los medios utilizados para la recogida, a la entrega de información previa al interesado y a contar con su consentimiento libre, inequívoco, específico e informado[183].

La lealtad también se manifiesta al limitar la recogida sólo a aquellos datos necesarios para alcanzar las finalidades propuestas, y al cancelarlos una vez cumplidos dichos fines. Por eso, una colecta leal exige la definición lo más precisa posible de la finalidad que se persigue, no siendo correcta una descripción vaga del objeto del tratamiento, como por ejemplo, al señalar "fines comerciales".

Por otra parte, cabe destacar la directa conexión que presenta el deber de información al titular con el principio del consentimiento, sea que los datos se recaben de él mismo o no. En la Unión Europea se sigue el criterio contenido en el artículo 10 de la Directiva 95/46/CE antes mencionada, según el cual se debe explicitar a lo menos la identidad del responsable del tratamiento[184], los fines a que van a ser objeto los datos, sus destinatarios o categorías de éstos, el carácter obligatorio o no de la respuesta del titular, las consecuencias que tendría para él su negativa a responder, la existencia de derechos de acceso y rectificación que puede ejercer y, habida consideración de las circunstancias específicas en que se obtienen los datos, toda información suplementaria necesaria para garantizar un tratamiento leal.

En Chile, la ley Nº 19.628, en los artículos 4 y 5 ha dispuesto que la autorización escrita del titular al tratamiento de sus datos debe haber estado debidamente informada respecto del propósito del almacenamiento y su posible comunicación. En este último caso, frente a requerimientos de datos personales que un tercero haga mediante una red

[183] Hemos destacado estas características del consentimiento basados en la definición que de él realiza la ley española 15/1 999, sobre protección de datos de carácter personal, en su artículo 3, letra h).
[184] El legislador chileno emplea la denominación responsable del registro o banco de datos, para referirse al responsable del tratamiento.

electrónica, se debe dejar constancia de la individualización del requirente; el motivo y el propósito del requerimiento, y el tipo de datos que se transmiten. En este supuesto, el receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

Cabe advertir que aunque la misma ley establece que la necesidad de consentimiento y el deber de información no son aplicables cuando se trate de datos personales accesibles al público en general, es decir, cuando provengan de registros o recopilaciones de datos nominativos, públicos o privados, de acceso no restringido o reservado a los solicitantes, ello no significa necesariamente que esa información no tenga un titular o que éste renuncie a sus derechos.

En virtud de lo anterior, una situación en la que se podría considerar leal la recogida de datos desde el punto de vista del deber de información se presentaría cuando la página web en donde se solicitan datos personales indica la política de privacidad de la empresa, señalando su identificación precisa; un correo electrónico y una dirección postal para el ejercicio de los derechos de acceso, rectificación, cancelación y para especificar las finalidades para las que se autoriza el uso de los datos; el que la captación de información sea almacenada en el equipo informático y el tipo de datos que recoge; la finalidad o finalidades a que se destina la información obtenida; y la intención de comunicar los datos a terceros.

- ¿Cúando hay un tratamiento invisible de datos personales?

Como hemos visto, navegar por Internet deja tras de sí un sinnúmero de datos que quedan registrados en los nodos por los que pasa un cibernauta cada vez que ingresa a una página web, por lo que es necesario garantizar un tratamiento leal, principalmente al momento de la recogida de éstos, mediante el respeto de un conjunto de principios básicos de los sistemas de protección de datos de carácter personal.

Sin embargo, en Internet no siempre se reúnen datos con consentimiento del titular; incluso hay ocasiones en las que ni siquiera se cuenta con su conocimiento, privándole de la posibilidad de ejercitar sus derechos.

Precisamente este caso se presenta en el denominado “tratamiento invisible y automatizado de datos personales”, que consiste en un conjunto de operaciones y procedimientos técnicos efectuados por programas y equipos capaces de procesar los datos de los usuarios y ponerlos a disposición de terceros sin conocimiento o

consentimiento de sus titulares.

Ahora bien, ¿cuándo se realiza este procesamiento tan particular? Sus manifestaciones son múltiples, algunas más conocidas que otras. Lo encontramos en los hipervínculos o enlaces automáticos a sitios de terceros que se incluyen en las páginas web, o cuando el servidor envía contenido activo, como Javascript[185] o ActiveX[186].

También puede haber un tratamiento invisible a partir de la actuación que realiza un "agente inteligente", es decir, un programa informático configurado por una persona para cumplir una misión y tomar una decisión. En estas aplicaciones se observa una triple función: filtran información en función de los parámetros fijados; personalizan el interfaz adaptándolo automáticamente a las necesidades del usuario; y recogen información autónomamente porque estos agentes son capaces de actuar incluso aunque el usuario no esté conectado a la red; todo lo cual implica que no exista un control o supervisión directo del usuario para el que actúa[187].

Los programas navegadores o browsers –como Internet Explorer, Navigator u Opera, por ejemplo- constituyen otro caso en el que se realiza tratamiento invisible. Estos programas destinados, entre otras cosas, a visualizar gráficamente el material disponible en Internet y a comunicar el cliente (computador del usuario) con el servidor web (computador remoto donde está almacenada la información), envían automáticamente a éste más información de la estrictamente necesaria para establecer la comunicación, por ejemplo, el tipo y la lengua del navegador, el nombre de otros programas instalados en el computador y el sistema operativo del usuario, entre otros. A esto se suma la posibilidad de que el navegador, también de manera invisible, transmita sistemáticamente esos datos a terceros.

Por otra parte, la manifestación de tratamiento invisible más conocida es, sin duda, la conformada por archivos denominados cookies, que se envían desde un servidor al computador de un usuario con el objeto de identificar en el futuro ese equipo

[185] JavaScript es un lenguaje de programación desarrollado por Netscape para hacer más conveniente la animación y otras formas de interacción. Estos programas se encuentran en archivos HTML y les permiten a éstos controlar al browser o navegador. En cuanto a los ataques a la privacidad cabe advertir que, como el código de JavaScript descargado corre dentro del navegador, potencialmente tiene acceso a cualquier información que este tenga. Por lo tanto, el problema de JavaScript pasa más que por el tener acceso a información sensible, por el que ésta pueda salir del computador del usuario. Véase Garfinkel, Simson y Spafford, Gene. Seguridad y comercio en el Web. Ed. McGraw-Hill, México, 1999.

[186] ActiveX es un conjunto de tecnologías, protocolos e interfaces de programación desarrolladas por Microsoft que sirven para descargar código ejecutable de Internet. Como riesgo destaca la posibilidad de apoderarse de información privada y confidencial. Véase Garfinkel, Simson y Spafford, Gene. Op. Cit.

[187] En el comercio electrónico los agentes inteligentes tienen aplicaciones particulares destinadas a buscar la oferta de un producto, comparar precios y ofrecer información clasificada por las preferencias del usuario.

en sucesivas visitas al mismo sitio web. La función básica de un cookie es permitir a un servidor almacenar y, más adelante, recuperar una pequeña cantidad de información en la máquina cliente, guardando aquellos datos que expresamente determine en un archivo de texto. Esos datos que contiene –dentro de los que podría incluir alguna información personal, como códigos de usuario y contraseñas- están asociados a un sitio web y a un programa navegador en particular, lo cual implica que un cookie creado por un servidor en un momento dado sólo será accesible en el futuro si el visitante regresa al sitio web usando el mismo computador y el mismo navegador[188].

Sin embargo, no todos los cookies son iguales, los hay locales y remotos. Los cookies locales son los que señalamos precedentemente y pueden ser tan necesarios que algunos sitios dependen de ellos para trabajar correctamente, por ejemplo, para acceder a cuentas de correo webmail como Yahoo o Hotmail, o para comprar libros o música en sitios como Amazon. En cambio, los cookies remotos son los que hacen posible el funcionamiento de redes de seguimiento de la navegación que realiza un usuario. Suelen guardarse cuando el sitio web que se visita despliega publicidad de terceros, a través de banners o applets Java, es decir, mensajes comerciales que poseen la capacidad de ejecutar un código que puede grabar el cookie en un cliente, y recuperarlo posteriormente. Así, analizando los datos que va dejando registrado el usuario en los cookies remotos técnicamente es posible vigilar las acciones de los usuarios en la red.

Por tanto, lo anterior nos lleva a concluir que frente a la existencia de técnicas que permiten crear registros a partir de los vínculos por los que ha pasado el usuario y que están almacenados en el servidor -que contienen información sobre el comportamiento, la identidad, el recorrido efectuado o las elecciones expresadas por la persona al visitar el sitio web-, quienes navegan por Internet deben morigerar el resguardo celoso de su vida privada y volverse tolerantes, permitiendo que otros traten dicha información. Sin embargo, la justa medida de ello se encuentra en un equilibrio suficiente que permita que esa tolerancia del individuo para con el medio pueda transformarse legítima y eficazmente en firme oposición allí donde el exceso y el abuso dañen su dignidad y conculquen sus derechos.

- Presupuestos recomendados para un tratamiento invisible de datos invisibles

[188] Es frecuente almacenar la fecha de la última visita, o bien algunos datos que permitan "recordar" lo que el usuario hizo o adquirió en esa oportunidad. Así, en el momento en que la persona regresa al sitio, su navegador envía el contenido del cookie al servidor, para que lo interprete y use de un modo preestablecido, por ejemplo, mostrando un saludo personalizado al usuario.

nominativos leal y lícito

Como los cibernautas no son conscientes de que constantemente se está recopilando información que les concierne y desconocen los fines a que se destinan sus datos, el tratamiento invisible que no se realiza de forma totalmente transparente al usuario contraviene el principio de lealtad en la recogida de datos e impide el ejercicio de los derechos que le asisten, especialmente, el de acceso, incluso si pese a saber la existencia de dicho tratamiento, no está en condiciones de entender el significado de las informaciones grabadas en el cookie, por ejemplo. Por esa razón, finalizaremos este trabajo planteando algunas recomendaciones para que el tratamiento invisible sea informado, consentido y, en definitiva, lícito y leal.

Según hemos señalado precedentemente, la legitimidad de estas operaciones y procedimientos técnicos descansa sobre dos pilares básicos: información y consentimiento. El primero de ellos consiste en el deber de suministrar información suficiente sobre los datos que se pretende recopilar, almacenar o transmitir, la finalidad del tratamiento y los derechos a oponerse al registro de ciertas categorías de servicios consultados cuando sean capaces de mostrar, además del perfil del consumidor potencial, sus hábitos, tendencia sexual, opiniones políticas o religiosas, es decir, datos sensibles. Recordemos que ese tipo de información cuenta con una protección reforzada en la ley Nº 19.628, antes anotada, la cual prohíbe su tratamiento a menos que una ley lo autorice, sean datos necesarios para determinar u otorgar beneficios de salud a sus titulares, o cuenten con el consentimiento escrito del titular.

Además, una información de buena fe no debe limitarse sólo a indicar que se generará un cookie o que los datos serán conservados con fines de promoción comercial, sino que será preciso que el usuario tenga noticia clara de la identidad del responsable del tratamiento, de los fines perseguidos, las categorías de datos, los destinatarios de éstos, y la existencia de derechos de acceso y rectificación.

Lo anterior, llevado a la práctica, significa que los browsers deberían señalar al momento de establecer una conexión con el servidor web, qué datos se pretende transferir y con qué objetivo. Tratándose de los cookies , el usuario tendría que ser advertido cuando esté previsto que el software de Internet los reciba, almacene o envíe, especificando en un lenguaje comprensible qué información se pretende guardar en el

cookie, su finalidad y el período de validez[189].

Como consecuencia de ello, estos dispositivos no deberían estar configurados para que por defecto se recopile, almacene o remita "información persistente del cliente", que como explicamos es la que permanece más de una sesión en el equipo informático del usuario. En tal sentido, la opción por defecto del navegador sólo debería permitir el tratamiento de la mínima cantidad de información necesaria para establecer una conexión y, en el caso de los cookies no deberían ser enviados ni almacenados de forma oculta[190].

El segundo pilar es, obviamente, el consentimiento expreso y facilitado desde los propios programas de navegación. Los productos de Internet tanto de software como de hardware deberían permitir al interesado decidir libremente sobre el tratamiento de sus datos personales ofreciéndole instrumentos de fácil manejo para filtrar la recepción, el almacenamiento o el envío de la información persistente del cliente según unos criterios determinados, tales como perfiles, dominio o identidad del servidor, o el tipo y duración de la información recopilada, almacenada o enviada.

En ese sentido, un browser debería brindar la opción para que el usuario lo configure especificando el tipo de información que debe o no recopilar y transmitir. En el caso de los cookies, el usuario debería contar siempre con la opción de aceptar o rechazar su envío o almacenamiento, junto con disponer de alternativas para determinar los elementos de información que se van a conservar o eliminar de un cookie, considerando, por ejemplo, el período de validez o los sitios web de envío y recepción.

Además, se recomienda establecer en los programas la posibilidad de eliminar la información persistente del cliente de manera simple para el usuario e inocua para el remitente. Incluso cuando no sea posible eliminar dicha información tendría que existir una forma fiable para evitar su transferencia y lectura, todo lo cual se logra en la medida que los cookies y demás información persistente del cliente se almacenen de forma normalizada que permita borrarla selectivamente en el cliente.

En definitiva, frente a un tratamiento invisible y automático necesario para

[189] Véase la Recomendación 1/99 de 23 de febrero de 1999, sobre el tratamiento invisible y automático de datos personales en Internet, adoptada por el Grupo de trabajo del artículo 29 (Grupo europeo especializado en protección de datos personales, creado por el artículo 29 de la Directiva 95/46/CE).

[190] Recientemente el Consejo de Ministros de Telecomunicaciones de la Unión Europea ha alcanzado un acuerdo sobre la Directiva referente a la privacidad en las comunicaciones electrónicas, norma que compromete a organismos públicos y privados a destruir o hacer anónimos los datos personales que obtengan a través sus comunicaciones en Internet, excepto si consideran que éstos afectan a la seguridad pública o del Estado. En relación con los cookies, a propuesta de Francia, la Directiva obliga que no puedan activarse sin que el usuario lo haya autorizado al menos en una ocasión

mejorar los servicios ofrecidos por la red, personalizándola o volviéndola más interactiva, la lealtad que lo legitima debe cumplir con prácticas generalmente aceptadas que consistan en la entrega de información clara y completa sobre el procesamiento de datos nominativos que se recopilan; en el ofrecimiento de opciones para los cibernautas relacionadas con el tratamiento de su información personal; la facilidad para que el titular acceda de forma razonable a ésta, incluyendo la posibilidad de revisarla, corregir inexactitudes o borrarla; y con la adopción de medidas pertinentes para preservar la seguridad de los datos que recolectan de los usuarios.

Son exigencias mínimas para lograr que los usuarios de Internet confíen en el comercio electrónico, para que la tecnología no avasalle los derechos de las personas y para que no se opte, tampoco, por prohibir este tipo de recogida de información ya que ello podría afectar el interés comercial en la red. Sin embargo,... ¿existirá la voluntad suficiente para corregir el estado actual de las cosas? Es una interrogante que debe ser resuelta en parte por los propios usuarios, los principales defensores de sus derechos.

4) Derecho a la privacidad y cookies. un ejemplo práctico y real

A pesar de ser una de las herramientas informáticas más usadas actualmente en la Internet, lo cierto es que las cookies[191] son también de las más incomprendidas, convirtiéndolas frecuentemente en objeto de mitos y medias verdades. Este desconocimiento no sólo afecta al público en general sino -de manera más preocupante aún- a los juristas, legisladores y muchas otras personas con poder de decisión en lo que se refiere al enunciado de políticas de telecomunicaciones y tecnología de la información.

Desde el punto de vista estrictamente técnico, el potencial benéfico de las cookies es muy grande. Ofrecen la posibilidad de brindar a los usuarios de la red una serie de servicios y ventajas que de otro modo no tendrían. Desde la óptica jurídica, sin embargo, pesa sobre ellas la sombra de servir como un instrumento maligno para

[191] La palabra cookie significa, literalmente, "galleta". Se trata de típica jerga informática angloparlante. Sin embargo, preferimos no traducirla aquí al castellano por la misma razón por la que no se suele hacerlo tampoco con otras expresiones como "hardware" o "CD-ROM", cuya usanza literal se ha difundido ampliamente a nuestro vocabulario informático

invadir la intimidad de las personas; característica que, como veremos, es sólo parcialmente cierta. Es por ello que, para los estudiosos del derecho informático, una adecuada comprensión de lo que las cookies son (e, igualmente importante, de lo que no son), nos parece fundamental para dar al tema del derecho a la intimidad en la red -uno de los más candentes y apremiantes de hoy- el tratamiento que corresponde y merece.

Comenzaremos por examinar brevemente en qué consiste esta herramienta y para qué se usa, desde el punto de vista informático. Luego repasaremos las críticas que le han sido dirigidas desde la perspectiva de la temática de la intimidad, intentando establecer cuáles son ciertas y cuáles meramente fruto de la ficción o de la candidez. Finalmente analizaremos algunas de las soluciones propuestas para los problemas reales que derivan del empleo de las cookies, en el plano tanto técnico como jurídico.

- ¿Qué es una cookie?

La "World-Wide Web" (WWW), el componente multimedial de la Internet, fue diseñada, construida y funciona hoy bajo un modelo llamado de cliente-servidor. En él, las computadoras de los usuarios son los "clientes", que mediante un programa visualizador o navegador[192], envían peticiones a otras computadoras (los "servidores"), para que éstas les envíen de regreso los documentos y demás componentes que conjuntamente conforman una "página web".

Estas interacciones entre clientes y servidores se conocen técnicamente como conexiones sin estado. A diferencia de lo que ocurre, por ejemplo, durante una conversación telefónica (en la que el vínculo entre el aparato telefónico de la persona que llama y el de la persona llamada se mantiene de modo continuo durante el transcurso de la conversación), las conexiones en la WWW tienen un carácter más bien intermitente: una vez que el servidor termina de enviar al cliente la información solicitada, el enlace entre ambos se quiebra. Si se quiere, podríamos decir que, a partir de ese momento, el servidor "olvida" al cliente. Si éste formula un nuevo requerimiento (de otra o incluso de la misma página web enviada anteriormente), ambas máquinas deben establecer una nueva conexión, identificándose una a otra de nuevo, como si nunca se hubiesen comunicado antes.

Esta arquitectura nos puede parecer curiosa, pero no obstante es la responsable

[192] Tales como el Netscape Navigator, Microsoft Internet Explorer, Opera, Lynx, Mosaic, etc

de la gran versatilidad de la WWW. Sin ella, los servidores web no podrían atender a la gran cantidad de usuarios de Internet que ingresan simultáneamente a los sitios más populares. En efecto, si las conexiones fuesen permanentes, ocurriría de algún modo lo mismo que pasa cuando intentamos llamar por teléfono a una persona, cuando ésta se encuentra conversando en el mismo momento con otra: no recibiríamos la información deseada y tendríamos que esperar a que el servidor se libere.

Pero esa misma característica de las conexiones sin estado, tan eficiente desde el punto de vista telemático, comporta un serio inconveniente desde la perspectiva humana. La intermitencia de las conexiones, a medida que el visitante navega de una página a otra dentro de un mismo sitio web o cuando regresa a él después de un tiempo, se convierte en un obstáculo a la sensación de continuidad que se podría querer ofrecer al usuario.

Las personas por lo general no nos avenimos bien a la fría eficiencia de las máquinas. Por ello, a medida que la WWW ha avanzado y madurado, las empresas y organizaciones han percibido la importancia de tratar de implementar mecanismos que contribuyan a crear la sensación de un trato más "personalizado" para sus visitantes.

Esto es particularmente cierto tratándose de los sitios de comercio electrónico, que -como cualquier otra empresa- dependen en gran medida de atraer y retener la lealtad de sus clientes mediante la excelencia de su servicio. Por ejemplo, dichos sitios querrían aprovechar algunos datos personales sobre sus clientes, así como tomar nota de sus particulares preferencias, con el fin de brindarles una más enriquecedora experiencia durante sus sucesivas visitas. Se querría también simular lo más estrechamente posible la visita a un comercio del "mundo real", en el que los consumidores pueden recorrer las estanterías, examinar los diversos productos e ir colocando sus selecciones en un "carrito" de compras antes de dirigirse a la caja para pagar. Justamente para llenar esta necesidad es que se ha dado paso a la creación y empleo de las cookies.

La función básica de una cookie es simple: permitirle a un servidor almacenar y más adelante recuperar una pequeña cantidad de información en la máquina cliente. Esos datos siempre están asociados a un sitio web y a un programa navegador en particular, lo cual implica que una cookie creada por un servidor en un momento dado sólo le será accesible en el futuro si el visitante regresa al sitio web usando la misma computadora y el mismo navegador. La información es guardada en un archivo de texto, y puede contener sólo aquellos datos que la aplicación servidora expresamente determine. Eso, desde luego, podría incluir alguna información personal, así como

códigos de usuario y contraseñas.[193] También es frecuente almacenar la fecha de la última visita, o bien algunos datos que permitan "recordar" lo que el usuario hizo o adquirió en esa oportunidad. En el momento en que la persona regresa al sitio en cuestión, su programa navegador envía el contenido de la cookie al servidor, que puede entonces interpretarlo y usarlo de un modo preestablecido, como, por ejemplo, mostrando un saludo personalizado al visitante.

Expuesto así someramente lo que una cookie es, analicemos ahora lo que no es, en procura de desterrar algunos de los mitos que las rodean. En primer término, es importante subrayar que no pueden capturar información personal de un usuario que no esté dispuesto a cederla voluntariamente. Además, no pueden transmitir un virus informático, porque no contienen más que texto estático. No sólo por sus características intrínsecas sino además por su muy reducido tamaño, estas estructuras no tienen la posibilidad de almacenar código ejecutable que pueda actuar como un virus. Finalmente, un servidor no tiene acceso más que a los datos contenidos en la cookie creada por él. En especial, no pueden hurgar por el disco fijo, extrayendo documentos u otros archivos sensibles de la computadora del usuario. De hecho, algunas cookies ni siquiera son almacenadas en disco; existen solamente en la memoria de la computadora y por el término de la actual sesión del programa navegador, desapareciendo tan pronto éste se descarga.[194]

Para concluir este aparte, se debe recalcar que la mayoría (si no todas) las aplicaciones recientes de navegación en la web, permiten que el usuario elija una opción que impedirá el almacenamiento de cookies en su computadora, o que por lo menos lo alerte cuando esté por ocurrir. Esto se puede activar o desactivar fácilmente como parte de sus preferencias de uso de la respectiva aplicación.

- Afectaciones al derecho a la privacidad por el uso de cookies

A muchas personas molesta el mero hecho de que un servidor web tenga la capacidad de almacenar información, por poca que sea, en su computadora. Lo

[193] Esto es lo que ocurre cuando se automatiza el ingreso a un sitio web protegido por medio de una clave. El servidor grabará el dato en la computadora cliente, de manera que en las visitas futuras se recuperará automáticamente la clave, ahorrando al visitante la molestia de tener que reescribirla cada vez que regresa a ese sitio web. A pesar de la evidente comodidad de este mecanismo, no es menos obvio que no debe ser empleado en computadoras accesibles a más de una persona (muy especialmente las de las populares cabinas públicas de acceso a la Internet o cibercafés), ya que en tal caso todos los usuarios podrían acceder al servicio en cuestión como si fueran el legítimo titular.
[194] Así es como suelen funcionar los llamados "carritos de compras".

consideran una especie de invasión de su propiedad y de su espacio personal. Sin embargo, como se dirá, la verdadera amenaza a la intimidad que puede derivar del uso (más bien, del abuso) de la tecnología de cookies es mucho mayor de lo que esas personas posiblemente siquiera imaginen.

Como ha quedado claro de la sección precedente, el empleo de cookies es de evidente provecho para la empresa u organización que opera un sitio web, no sólo en cuanto permite ofrecer el grado de personalización del que hablábamos arriba, sino también -y quizás de mayor importancia- porque le permite realizar ciertos análisis de mercadotecnia y así conocer más acerca del perfil y los hábitos de consumo de sus clientes. Dependiendo del punto de vista de cada quien, esto podría parecer bueno o malo. Por ejemplo, la información contenida en una cookie puede ser empleada para la aplicación de publicidad dirigida: si se sabe que el visitante de un sitio web ha adquirido, digamos, libros sobre el cuidado de bebés, esto podría dar lugar a que en la misma o futuras visitas le sean presentados una serie de mensajes publicitarios sobre bienes o servicios asociados a ese mismo tema, con la esperanza de despertar su interés e intención de compra. Y, desde luego, el conocimiento así adquirido del consumidor también puede ser vendido o cedido a terceros. A través de técnicas de esta índole, es claro que eventualmente podríamos encontrarnos en presencia de la problemática que se examina a propósito de los grandes temas del derecho a la autodeterminación informativa y su instrumento aparejado, el recurso de hábeas data.

Si bien, como se explicó antes, se tiene siempre a mano la posibilidad de desactivar la creación de cookies en nuestra computadora, lo cierto es que esto no siempre es deseable y, de hecho, podría resultar perjudicial. En efecto, al hacerlo, se bloquearía tanto su empleo pernicioso como el benéfico.[195] Para entender mejor la cuestión, es importante establecer una distinción entre lo que podríamos denominar cookies locales y remotas.

* Una cookie local es aquella clase que hemos venido analizando hasta ahora: la que crea en nuestra computadora el servidor del sitio web que estamos visitando, con cualquiera de los fines ya señalados. Algunos sitios dependen de ellas al punto de que no trabajar correctamente si se deniega su creación. [196]

[195] Y la opción de aceptar selectivamente las cookies tampoco resuelve el problema, no sólo por lo tedioso que resulta sino porque, de todos modos, los usuarios no sofisticados carecen de criterio para determinar cuáles autorizar y cuáles no

[196] Por ejemplo, los diversos sitios que ofrecen correo electrónico gratuito vía una interface web, como los populares Yahoo, Hotmail, etc.

* También es posible la creación y recuperación remota de cookies. Cuando el sitio web que visitamos despliega publicidad de terceros, vía los llamados "banners" o "applets" Java, esos mensajes comerciales también poseen la capacidad de ejecutar código que puede grabar una cookie en nuestra computadora, y recuperarla posteriormente.

Desde la óptica del tema de la privacidad, interesa destacar que es justamente a través del uso de cookies remotas que se posibilita el funcionamiento de las llamadas "redes de seguimiento".[197] Estas funcionan cuando una empresa de mercadeo coloca mensajes publicitarios suyos en múltiples sitios populares de Internet con el fin de crear y luego recuperar cookies en las computadoras de los visitantes. Analizando estos datos, les es posible "seguir" a un usuario a medida que navega por esos sitios, vigilando sus acciones, acumulando información personal, controlando cuales bienes o servicios adquiere, etc. Es obvio que la posibilidad de crear perfiles sobre hábitos de consumo y recolectar datos personales crece así exponencialmente. Con solo navegar algunos minutos por estos lugares, ignorando por completo lo que sucede, la persona va dejando un clarísimo rastro electrónico, a la vez que cede -valga reiterar que involuntariamente- un tesoro de información a las empresas comercializadoras.

Las implicaciones jurídicas para el derecho de autodeterminación informativa y la privacidad en general son más que obvias.

- ¿Cómo enfrentar el problema?

- Soluciones tecnológicas

La tecnología frecuentemente tiene la capacidad de contrarrestar los problemas que ella misma crea. La primera solución, ya mencionada, fue la posibilidad que se ofreció a los usuarios de desactivar selectiva o totalmente el almacenamiento de cookies. Sin embargo, tal como se explicó también, esta vía es bastante radical y a la postre más bien puede coartar las posibilidades del consumidor de recibir las ventajas y beneficios del uso correcto y ético de las cookies.

Por esta razón, otras posibilidades han ido apareciendo paulatinamente. Por ejemplo, ya hay aplicaciones capaces de distinguir entre el acto de creación de una

[197] "Tracking network".

cookie local y una remota. Se puede elegir así, a discreción del usuario, si bloquear la segunda, ambas o ninguna.[198] También se ha propuesto un estándar denominado P3P ("Platform for Privacy Preferences"). Esta iniciativa sería incorporada dentro de los principales programas navegadores, con el propósito de permitir a los usuarios decidir cuánta información personal desean entregar a un sitio web. A través de P3P, el consumidor puede aprobar o improbar la transferencia de información personal, de acuerdo con preferencias fijadas de antemano. Por ejemplo, se podría establecer que no se transmitan datos de esta naturaleza a sitios que los venden a terceros. [199]

Está claro que el empleo de soluciones técnicas de este tipo, aparejado al incentivo de las alternativas de autorregulación que mucha de la industria informática responsable viene propugnando, ofrece una vía idónea para al menos minimizar el problema. Sin embargo, es igualmente indudable que no todas las empresas y organizaciones poseen esta buena disposición. En esa medida, un conjunto claro y completo de regulaciones normativas debe entrar a llenar los espacios restantes.

- Soluciones jurídicas

Desde la perspectiva de la mayoría de los ordenamientos jurídicos, nada de lo que se haga con las cookies, bueno o malo, posee mayor regulación legal. Sin embargo, diversas personas y entidades de tutela de los derechos civiles en países como los Estados Unidos ya han comenzado a preocuparse por el problema y a requerir la intervención de las autoridades para poner alguna clase de freno al "cosechado" de datos personales por medio de cookies.

En la medida en que, como se sabe, el ciberespacio no conoce fronteras políticas ni barreras geográficas, es evidente que el ideal sería que este tema forme parte de las diversas iniciativas para la creación de regulaciones de ámbito internacional en materia de comercio electrónico. Después de todo, la intimidad es un derecho fundamental, reconocido y tutelado internacionalmente en los diversos instrumentos sobre derechos humanos. La autodeterminación informativa, como corolario suyo que es, está siendo incorporada también cada vez más en los diversos textos normativos. Por ende, no se ve

[198] Nos referimos en particular al "Privacy Companion", que la empresa IDcide ha puesto gratuitamente a disposición del público. Nótese, sin embargo, que al momento de escribir estas líneas, se encuentra disponible solamente para el Internet Explorer de Microsoft. Es probable que más adelante sea ofrecido para otras aplicaciones.

[199] Puede verse un análisis de P3P desde el punto de vista jurídico, elaborado por el World Wide Web Consortium (W3C) en http://www.w3.org/TR/P3P-analysis

por qué no pueda y deba existir también un enfoque global del tema del abuso en el empleo de las cookies, en procura de soluciones integrales.

5) Legislación extranjera. Caso de España

La legislación española en materia de protección de datos se contiene básicamente[200] en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal, y en el Real Decreto 1332/1994, de 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Pese a la relativa novedad de esta normativa, las obligaciones y requerimientos legales que se establecen no se ajustan adecuadamente al tratamiento de datos a través de Internet, y ni siquiera existe previsión alguna en cuanto a la publicación de datos personales en páginas web[201].

En cuanto a esto último, a pesar de que la normativa no lo contempla expresamente, la Agencia de Protección de Datos considera[202] que la difusión de datos a través de Internet, en la medida en que se comunican datos a una pluralidad -indefinida- de personas distintas del interesado, constituye una cesión o comunicación a efectos de la LOPD.

Por otro lado, la prestación del consentimiento en los casos en que se efectúe por un simple clic o incluso por correo electrónico puede plantear problemas en el caso de que dicho consentimiento se exige de forma expresa y por escrito[203], dadas las dificultades de identificación inequívoca de quien manifiesta su voluntad, así como las

[200] Existe, junto a esta, legislación específica que se ocupa, en mayor o menor medida, del tratamiento de datos de carácter personal en los ámbitos de las telecomunicaciones, sanitario, registral y catastral, electoral o en la legislación de régimen local.

[201] De acuerdo con el artículo 3 i) de la LOPD, se entiende por cesión o comunicación de datos "toda revelación de datos realizada a una persona distinta del interesado", por lo que la publicación de datos de carácter personal a través Internet se considerará como cesión o comunicación a efectos de la normativa sobre protección de datos, debiéndose aplicar, en consecuencia, las previsiones establecidas en la misma en cuanto a la cesión de datos a terceros y a la prestación del consentimiento por parte del afectados (arts. 7 y 8 de la LOPD para datos especialmente protegidos, y arts. 11 y 27 con carácter general).

[202] Véase la Memoria de la Agencia de Protección de Datos del año 1999, que comenta dicha cuestión al analizar la posibilidad de publicación a través de Internet de datos de Sentencias condenatorias por negligencia médica

[203] Para el tratamiento de los datos relativos a ideología, afiliación sindical, religión o creencias (art. 7.2 LOPD).

dudas que existen acerca del valor jurídico de estas acciones o comunicaciones.

En relación con el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, la práctica habitual, y así lo demuestra la Agencia de Protección de Datos6, es requerir al interesado la aportación de una fotocopia del Documento Nacional de Identidad, por lo que, a pesar de las previsiones que realiza tanto la LOPD (art. 15) como el Real Decreto 1332/94 (art. 12) de poder cumplir con este deber por medio otros medios fuera del soporte papel, como la visualización en pantalla de los datos, lo cierto es que no van a tener gran aplicabilidad, a menos que la firma electrónica experimente el despegue que no parece va a tener a medio plazo.

Con todo, parece ser que, en cierto modo, se aceptan este tipo de prácticas[204], ya sea el uso del correo electrónico para el ejercicio de los derechos o para comunicaciones entre el responsable del fichero y el afectado, o la utilización de mecanismos via web, previo registro del interesado, que se identifica y autentica por medio de su nombre de usuario y contraseña.

- Cookies

Al hablar de protección de datos e Internet necesariamente hay que hacer referencia a las cookies, cuya definición ya la comentábamos con anterioridad. Consisten en pequeños ficheros que se almacenan en el disco duro del ordenador del usuario, y proporcionan información sobre los sitios web visitados, las preferencias y enlaces seleccionados, pero también almacenan otros datos más importantes, si cabe, como el nombre de usuario y clave de acceso a un sitio web o el número de la tarjeta de crédito, todo ello en relación con la dirección IP asignada a un equipo, generalmente para una sesión, por el proveedor de acceso a Internet. Por tanto, en principio, las cookies no serían datos de carácter personal en la medida en que no identificarían a una persona física sino a una máquina. No obstante, ello no es así. En primer lugar, porque las cookies vienen bajo la forma nombre de usuario configurado en el navegador@nombre del servidor web que envía la cookie, con lo que ya se podría identificar a una persona física, pero es que, además, el proveedor de acceso a Internet puede identificar, en todo momento, una dirección IP con su correspondiente usuario, y la LOPD, al definir el concepto de datos de carácter personal se refiere a ellos[205] como

[204] Véase la Recomendación de la Agencia de Protección de Datos al sector del comercio electrónico, disponible a través de su sitio web.
[205] Art. 3 a) de la LOPD.

"cualquier información concerniente a personas físicas identificadas o identificables", con lo cual no cabe ninguna duda de que las cookies son datos de carácter personal. En consecuencia, habrá que aplicar la normativa sobre la materia, con las correspondientes obligaciones: deber de información en la recogida de los datos, solicitud del consentimiento para su tratamiento y, en su caso, cesión[206], creación del correspondiente fichero y notificación a la Agencia de Protección de Datos, implantación de medidas de seguridad informática,...

La práctica habitual indica que lo anterior no se hace, limitándose los titulares de sitios web a informar, en el mejor de los casos, de que su sitio web utiliza cookies, para qué sirven y la información que recogen.

Pero las implicaciones entre Internet y la regulación de los datos de carácter personal son mucho más que eso. La generación de datos transaccionales y los logs que almacenan los proveedores de acceso a Internet también es importante desde este punto de vista, ya que contienen información personal sobre las visitas de los navegantes a los sitios que, al igual que con las cookies, se relaciona con una dirección IP. Por otro lado, y tal como señala María de los Reyes Corripio[207], podemos equiparar los datos transaccionales a los "datos sobre el tráfico" a que se refiere la Directiva sobre Protección de Datos[208], y considerarse, por tanto, datos de carácter personal.

Lo mismo puede decirse con los llamados clickstream data, que se recogen tanto por proveedores de acceso como por los servidores de páginas web, y contienen información sobre los sitios y páginas web visitadas, el tiempo que se ha estado en cada una, el orden en que se han visitado, los foros en los que ha participado el usuario y las direcciones de correo electrónico enviadas o recibidas por éste.

Todos estos datos se utilizan para finalidades asociadas al Marketing one to one (ajustado al cliente), lo que requiere la elaboración de contenidos personalizados de acuerdo con el perfil del cliente. En este sentido, y de acuerdo con lo que establece el artículo 4.4 del Reglamento de Medidas de Seguridad, las entidades que realicen el

---

[206] Téngase en cuenta que, determinadas *cookies* pueden ser leídas por servidores distintos del que la origina, con lo cual existe una comunicación de los datos que contiene o, cuando menos, se posibilita el acceso a los mismos por parte de terceros. No obstante, también es cierto que es el propio usuario de Internet quien permite ese conocimiento de los datos, ya que se almacenan en su ordenador, pudiendo eliminarlos en todo momento.

[207] Corripio Gil-Delgado, María de los Reyes, Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet, Premio Agencia Protección de Datos, Cuarta Edición

[208] Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Diario Oficial L 024 de 30/01/1998.

tratamiento de estos datos deberán aplicar las medidas de nivel medio establecidas en dicha norma.

- Correo electrónico

Las direcciones de correo electrónico constituyen, a juicio de la Agencia de Protección de Datos[209], datos de carácter personal. Distingue aquellas direcciones de correo electrónico que contienen información acerca del titular, como el nombre o apellidos (o sus iniciales), la entidad en la que trabaja (por el nombre de dominio de segundo nivel[210]) y el país en el que lleva a cabo su actividad (por el nombre de dominio de primer nivel), de aquellos en que la dirección de correo no muestra directamente datos relacionados con el titular de la cuenta, sino una denominación abstracta o un conjunto de caracteres alfanuméricos sin significado alguno.

El segundo caso es el que suscita más dudas. No obstante, también en este tipo de direcciones de correo puede llegar a identificarse al titular de la cuenta mediante una consulta al servidor que gestione dicho dominio[211], por lo que se concluye que la dirección de correo electrónico es un dato de carácter personal y se somete al régimen de la LOPD.

Por otro lado, en cuanto a los mensajes, conviene tener en cuenta que se transmiten en abierto[212], por lo que son susceptibles de ser interceptados y leídos utilizando los denominados sniffers, programas que monitorizan el tráfico a través de Internet y permiten interceptar las comunicaciones.

- Uso de foros y listas de correo

A través de los foros y listas de correo uno puede manifestar opiniones, preferencias o inquietudes, ya sea a través del web o del correo electrónico. Hay que tener en cuenta que, dadas las facilidades de la informática, estos datos pueden

[209] Véase Memoria de la Agencia de Protección de Datos del año 1999, que resuelve una consulta sobre el tema.
[210] Se distingue entre nombres de dominio de primer nivel (top level domain names), que pueden ser genéricos (.com, .net., .int, .edu,...) o geográficos (.es, .fr, .uk,...), y los de segundo nivel (second level domain names), ligados a los anteriores y referidos a la entidad titular. Junto a ellos, pueden coexistir nombres de dominio de tercer nivel, que aparecen entre ambos y añaden, a los nombres geográficos de primer nivel, otra indicación de tipo genérico.
[211] Debe tenerse en cuenta que no siempre será tan sencillo obtener los datos del titular de una cuenta de correo cuando el servidor que lo gestiona se encuentre establecido fuera de la Unión Europea, pues bien podría no estar obligado a dar dicha información conforme a su ley aplicable
[212] Salvo que se utilicen programas de cifrado. El más conocido es el PGP (Preety Good Privacy), que es gratuito.

almacenarse en servidores web sin dificultad durante varios años. Por tanto, un rastreo permitiría recopilar, sin que el afectado fuera consciente, una cantidad de información suficiente para el establecimiento de su perfil. En este sentido, tanto la Agencia de Protección de Datos como otros organismos, como el Consejo de Europa[213], el International Working Group on Data Protection in Telecommunications[214] o el Grupo de Trabajo sobre Protección de Datos de la UE aconsejan ser conscientes de que las opiniones vertidas en dichos foros y listas son públicas y pueden ser malinterpretadas. Se aconseja asimismo utilizar todos los mecanismos posibles para preservar el anonimato en la red.

- Herramientas de búsqueda

Lo anterior se relaciona con el uso de las herramientas de búsqueda de información en Internet, ya que por medio de éstas se puede acceder a los comentarios y opiniones de los foros y listas de correo.

Tal como señala María de los Reyes Corripio, se distinguen tres tipos de herramientas de búsqueda: los llamados genéricamente buscadores, que ofrecen direcciones o sitios de Internet relacionados con la búsqueda solicitada (www.terra.es, www.yahoo.com o www.ya.com los incorporan), los motores de búsqueda, que por su cuenta rastrean la red y crean bases de datos documentales que pueden ser consultadas por los usuarios (www.google.com, www.alltheweb.com), y los agentes inteligentes o netbots, que incorporan mecanismos que permiten el filtrado de contenidos, pueden informarnos de actualizaciones y cambios en páginas web, aprenden de las búsquedas anteriores, no sólo de las del propio usuario, sino de las realizadas por otros con las mismas preferencias que nosotros, e incorporan todo tipo de mecanismos que, procesando el lenguaje natural, ajustan los resultados de la búsqueda al máximo, a partir, eso sí, de un conocimiento muy completo de los intereses del usuario[215].

En comercio electrónico se suelen utilizar este tipo de programas para buscar productos que se ajusten a un margen de precios, utilidades o preferencias del usuario. Por ejemplo, la tienda virtual Amazon (www.amazon.com) propone, junto a los libros

[213] Anexo de la Recomendación nº R(99)5: Directrices para la protección de las personas respecto a la recogida y tratamiento de datos personales en las "autopistas de la información", adoptada por el Comité de Ministros el 23 de febrero de 1999.
[214] Posición Común sobre la Protección de Datos y los motores de búsqueda en Internet, adoptada en la 23 Reunión del IWG en Hong Kong SAR, China, el 15 de abril de 1998
[215] Ejemplos de aplicaciones de este tipo son el Netbot Jango (www.jango.com), o el Auction Bot (http://auction.eecs.umich.edu)

cuyo título o contenido se ajustan a la búsqueda, otros libros de la misma temática, otros que han comprado usuarios con un interés semejante, o incluso productos de música o vídeo que estén relacionados.

Otro ejemplo es el eService Center, desarrollado por al empresa norteamericana RightNow (www.rightnow.com) para gestionar de forma más eficiente los servicios de atención al cliente. Su novedad es que el sistema no tiene que anticiparse a las posibles preguntas de los usuarios sino que va aprendiendo con cada consulta hecha por estos y va clasificando las respuestas a medida que se van generando. La aplicación reconoce, en las consultas (por correo electrónico, por ejemplo), ciertas palabras clave por medio de las cuales puede llegar a comprender dichas consultas, realizar estadísticas y hasta generar respuestas personalizadas utilizando plantillas. Se calcula que estos sistemas pueden atender entre el 70% y el 90% de las consultas de este tipo.

Los riesgos para la privacidad del usuario medio, que no es consciente del funcionamiento de estas aplicaciones, son evidentes. Debemos tener en cuenta que, en el uso todas las herramientas que utiliza Internet[216] existen estos riesgos, y que al sector privado[217] puede recopilar y sistematizar, gracias al desarrollo de la informática, toda la información sobre sus potenciales clientes que esté a su alcance.

- Agencia de Protección de Datos.

Para finalizar analizaremos un órgano español especializado en la protección de los datos y en el tratamiento de los mismos, sus principales funciones y la estructura principal con sus características, todo esto, para darnos una visión de cómo podría constituirse en Chile un órganos de iguales condiciones.

Funciones

General

* Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

[216] Por ejemplo, también en el uso de *chats* o de programas de mensajería instantánea.

[217] Principalmente, porque se destinan a finalidades básicamente comerciales, pero nada impide que los organismos públicos puedan incorporar estas tecnologías para mejorar los servicios que ofrecen al ciudadano.

En relación con los afectados

* Atender a sus peticiones y reclamaciones.

* Información de los derechos reconocidos en la Ley.

* Promover campañas de difusión a través de los medios.

En relación con quienes tratan datos

* Emitir autorizaciones previstas en la Ley.

* Requerir medidas de corrección.

* Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.

* Ejercer la potestad sancionadora.

* Recabar ayuda e información que precise.

* Autorizar las transferencias internacionales de datos.

En la elaboración de normas

* Informar los Proyectos de normas de desarrollo de la LOPD.

* Informar los Proyectos de normas que incidan en materias de protección de datos.

* Dictar Instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD.

* Dictar recomendaciones en materia de seguridad y control de acceso a los ficheros.

En materia de telecomunicaciones

*

Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente.

Otras funciones

* Velar por la publicidad en los tratamientos, publicando anualmente una lista de los mismos (CD).

* Cooperación Internacional.

* Representación de España en los foros internacionales en la materia.

* Control y observancia de lo dispuesto en la Ley reguladora de la Función

Estadística Pública.

* Elaboración de una Memoria Anual, presentada por conducto del Ministro de Justicia a las Cortes.

- Estructura de la Agencia de Protección de Datos a diciembre de 2005

El Director
D. José Luis Piñar Mañas

Ostenta la representación de la Agencia, sus actos se considerarán como propios de la Agencia, es nombrado por Real Decreto de entre los miembros del Consejo Consultivo a propuesta del Ministro de Justicia, es Independiente y no sometido a mandato imperativo alguno, su Mandato es de cuatro años

* Causas de cese

A petición propia

Por separación en caso de incumplimiento grave, incapacidad, incompatibilidad o comisión de delito doloso

* Funciones del Director: Resoluciones (ponen fin a la vía administrativa; recurribles ante la Sala de lo Contencioso de la AN)

    o Sobre inscripción
    o Sobre códigos tipo
    o Sobre transferencias
    o Tutelas de derechos
    o Procedimientos sancionadores
    o Medidas cautelares
    o Instando la incoación de expedientes disciplinarios
    o Autorizaciones de entrada en locales
        + Coordinación con las autoridades autonómicas
        + Funciones de gestión

El Consejo Consultivo

- Dª Elisenda Malaret García, a propuesta del Congreso de los Diputados
- Dª María Rosa Vindel López, a propuesta del Senado
- D. Antonio Troncoso Reigada, Director de la Agencia de la Comunidad de Madrid, a

propuesta de la misma

- Dª. Esther Mitjans i Perelló, Directora de la Agencia Catalana de Protección de Datos
- D. Iñaki Vicuña de Nicolás, Director de la Agencia Vasca de Protección de Datos
- D. Gonzalo Brun Brun, como vocal de la Administración Local, a propuesta de la Federación Española de Municipios y Provincias
- D. Eloy Benito Ruano, a propuesta de la Real Academia de la Historia
- D. Antonio Pérez Prados, a propuesta del Consejo de Universidades
- D. Alejandro Perales Albert, como vocal de los consumidores y usuarios, a propuesta, en terna, del Consejo de Consumidores y Usuarios
- Dª Belén Veleiro Reboredo, como vocal del sector de ficheros privados, a propuesta, en terna, del Consejo Superior de Cámaras Oficiales del Comercio, Industria y Navegación

* Órgano Colegiado de asesoramiento del Director
* Emitirá informe en todas las cuestiones que le solicite el Director
* Formulará propuestas en materia de protección de datos
* Se reunirá al menos una vez cada seis meses
* El Director será elegido de entre sus miembros

El Registro General de Protección de Datos

Subdirectora General del Registro General de Protección de Datos

Dª María José Blanco Antón

* Función: Velar por la publicidad de los tratamientos de datos
* Expedientes que tramita
    - o Inscripción de tratamientos notificados
    - o Autorización de transferencias internacionales de datos
    - o Inscripción de Códigos Tipo
* Tratamientos inscribibles
    - o Ficheros Públicos
        - + Administración del Estado
        - + Administración de las CC.AA.
        - + Administración Local
        - + Entidades vinculadas o dependientes de esas Administraciones
        - + Administración 'corporativa' en el desempeño de potestades de derecho

público

Ficheros Privados

* Contenido de las inscripciones
    - o Responsable del fichero, ubicación y existencia de encargados del tratamiento
    - o Finalidad y usos
    - o Afectados
    - o Procedimiento de recogida
    - o Estructura del fichero y tipo de datos que contiene
    - o Cesiones y transferencias, indicando destinatarios
    - o Medidas de seguridad
    - o Forma de ejercicio por los afectados de sus derechos
* Si el fichero es de titularidad pública, debe aprobarse una disposición general en que se haga mención a estos extremos
* ProcedimientoNotificación del tratamiento al RGPD (previo a iniciar la recogida de los datos)
    - o Si hubiera que subsanar algún defecto: solicitud de subsanación en 10 días
    - o Si se aclara o no hizo falta subsanación, se inscribe el tratamiento
    - o Si no se ha aclarado suficientemente, se deniega la inscripción
    - o Si no se dice nada en 30 días desde la remisión (sin contar el plazo de subsanación), el fichero se considerará inscrito (silencio positivo)
* Efectos de la inscripción: la inscripción es necesaria para que el tratamiento sea lícito, pero la inscripción es meramente declarativa
    - o No inscribir es contrario a la LOPD
    - o Estar inscrito no implica una presunción de que el tratamiento es totalmente conforme a la Ley

La Inspección de Datos

Subdirector General de Inspección de Datos

D. Alvaro Canales Gil

* Función
    - o Comprobación de la legalidad de los tratamientos
* Organización
    - o Inspectores de datos
    - o Instrucción de procedimientos

+ Tutelas de derechos

+ Procedimientos sancionadores

+ Procedimientos de infracción por las Administraciones Públicas

* Funciones inspectoras

o Naturaleza de autoridad pública

o Deber de secreto de los inspectores

o Posibles actuaciones

+ Examen de soportes

+ Examen de equipos

+ Análisis de programas

+ Examen de los sistemas de transmisión

+ Auditoría informática

+ Requerimiento de información

o Potestades de entrada en locales

o Supuestos de actuación

+ Ante una denuncia de un afectado o en supuestos de 'alarma social'

+ Dentro de un plan de inspección de oficio

o Planes de Oficio Finalidad 'preventiva'.

+ Sólo se imponen sanciones en casos de extrema gravedad

+ Tiene por objeto conocer el modo en que se realizan los tratamientos por parte de un sector

+ Concluye con la preparación de unas 'recomendaciones' en que se detectan los problema

* Instrucción de procedimientos. Tutela de derechos.

o Presupuesto

+ Ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición

+ Denegación de este derecho por el responsable del Fichero

o Procedimiento

+ Reclamación por escrito a la APD

+ La APD requiere alegaciones al responsable en plazo de 15 día

+ Práctica de pruebas o inspección

+ Audiencia del responsable y el afectado

+ Resolución

+ Plazo máximo de tramitación: 6 meses. Silencio positivo

* Instrucción de procedimientos. Procedimiento sancionador.

o Causa de iniciación

+ Denuncia de un afectado

+ Conocimiento de un hecho presuntamente ilícito (por ejemplo, por los medios de comunicación o denuncia de un tercero)

o Procedimiento

+ Establecido por las normas generales de derecho administrativo (RD 1398/1993, de 4 de agosto, en desarrollo Título VI Ley 30/1992)

o Medidas cautelares específicas

+ En caso de hechos tipificados como infracción muy grave de utilización o cesión ilícita

+ Perjuicio para los derechos de los ciudadano y el libre desarrollo de la personalidad

+ Podrá requerirse el cese en el tratamiento

+ Si no se atiende, podrán inmovilizarse los ficheros

+ Instrucción de procedimientos

o Procedimiento sancionador. Contenido de la resolución sancionadora.

+ Ficheros de titularidad privada

+ Multa económica (criterios de cuantificación y atenuación previstos en la Ley)

+ Medidas complementarias

o Ficheros de titularidad pública

+ Declaración de la infracción

+ Imposición de medidas correctoras

+ Solicitud de medidas disciplinarias para el responsable de la actuación ilícita

+ Notificación de la resolución al Defensor del Pueblo

La Secretaría General de la Agencia

Subdirector General. Secretario General

D. Ignacio García-Belenguer Laita

* Misión

o Apoyo al adecuado funcionamiento de la Agencia

* Funciones

o De apoyo

o De gestión, por Delegación del Director

o Otras complementarias

+ Fondo de documentación

+ Edición de repertorios, Memoria y publicaciones

+ Preparación de conferencias...

o Atención al ciudadano en las cuestiones que plantee, relacionadas con la protección de datos

Capitulo IX Anexo: Legislación Chilena

Pero... ¿para qué sirve?
Ingeniero de IBM refiriéndose al microchip.

1) Ley 19628 sobre Protección de Datos de Carácter Personal.

Identificación de la Norma: LEY-19628
Fecha de Publicación : 28.08.1999
Fecha de Promulgación : 18.08.1999

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente Proyecto de ley:

"PROTECCION DE DATOS DE CARACTER PERSONAL

Título Preliminar
Disposiciones Generales

Artículo 1º.- El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley, con excepción del que se efectúe en ejercicio de las libertades de emitir opinión y de informar, el que se regulará por la ley a que se refiere el artículo 19, N° 12, de la Constitución Política. Toda persona puede efectuar el tratamiento de datos personales, siempre que lo haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico. En todo caso deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta ley les reconoce.

Artículo 2°.- Para los efectos de esta ley se entenderá por:

a) Almacenamiento de datos, la conservación o custodia de datos en un registro o banco de datos.

b) Bloqueo de datos, la suspensión temporal de cualquier operación de tratamiento de los datos almacenados.

c) Comunicación o transmisión de datos, dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas.

d) Dato caduco, el que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna.

e) Dato estadístico, el dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable.

f) Datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.

g) Datos sensibles, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.

h) Eliminación o cancelación de datos, la destrucción de datos almacenados en registros o bancos de datos, cualquiera fuere el procedimiento empleado para ello.

i) Fuentes accesibles al público, los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

j) Modificación de datos, todo cambio en el contenido de los datos almacenados en registros o bancos de datos.

k) Organismos públicos, las autoridades, órganos del Estado y organismos, descritos y regulados por la Constitución Política de la República, y los comprendidos en el inciso segundo del artículo 1º de la ley N° 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado.

l) Procedimiento de disociación de datos, todo tratamiento de datos personales de manera que la información que se obtenga no pueda asociarse a persona determinada o determinable.

m) Registro o banco de datos, el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos.

n) Responsable del registro o banco de datos, la persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal.

ñ) Titular de los datos, la persona natural a la que se refieren los datos de carácter personal.

o) Tratamiento de datos, cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

Artículo 3°.- En toda recolección de datos personales que se realice a través de encuestas, estudios de mercado o sondeos de opinión pública u otros instrumentos semejantes, sin perjuicio de los demás derechos y obligaciones que esta ley regula, se deberá informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información. La comunicación de sus resultados debe omitir las señas que puedan permitir la identificación de las personas consultadas. El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión.

Título I

De la utilización de datos personales

Artículo 4°.- El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello.

La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.

La autorización debe constar por escrito.

La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito.

No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, cuando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de

nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.

Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos.

Artículo 5º.- El responsable del registro o banco de datos personales podrá establecer un procedimiento automatizado de transmisión, siempre que se cautelen los derechos de los titulares y la transmisión guarde relación con las tareas y finalidades de los organismos participantes.

Frente a un requerimiento de datos personales mediante una red electrónica, deberá dejarse constancia de:

a) La individualización del requirente;

b) El motivo y el propósito del requerimiento, y

c) El tipo de datos que se transmiten.

La admisibilidad del requerimiento será evaluada por el responsable del banco de datos que lo recibe, pero la responsabilidad por dicha petición será de quien la haga.

El receptor sólo puede utilizar los datos personales para los fines que motivaron la transmisión.

No se aplicará este artículo cuando se trate de datos personales accesibles al público en general.

Esta disposición tampoco es aplicable cuando se transmiten datos personales a organizaciones internacionales en cumplimiento de lo dispuesto en los tratados y convenios vigentes.

Artículo 6°.- Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.

Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.

Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular.

Artículo 7°.- Las personas que trabajan en el tratamiento de datos personales, tanto en organismos públicos como privados, están obligadas a guardar secreto sobre los

mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.

Artículo 8°.- En el caso de que el tratamiento de datos personales se efectúe por mandato, se aplicarán las reglas generales.

El mandato deberá ser otorgado por escrito, dejando especial constancia de las condiciones de la utilización de los datos.

El mandatario deberá respetar esas estipulaciones en el cumplimiento de su encargo.

Artículo 9°.- Los datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público.

En todo caso, la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos.

Artículo 10.- No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Artículo 11.- El responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños.

Título II
De los derechos de los titulares de datos

Artículo 12.- Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.

En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen.

Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.

Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal.

En el caso de los incisos anteriores, la información, modificación o eliminación de los datos serán absolutamente gratuitas, debiendo proporcionarse, además, a solicitud del titular, copia del registro alterado en la parte pertinente. Si se efectuasen nuevas modificaciones o eliminaciones de datos, el titular podrá, asimismo, obtener sin costo copia del registro actualizado, siempre que haya transcurrido a lo menos seis meses desde la precedente oportunidad en que hizo uso de este derecho. El derecho a obtener copia gratuita sólo podrá ejercerse personalmente.

Si los datos personales cancelados o modificados hubieren sido comunicados previamente a personas determinadas o determinables, el responsable del banco de datos deberá avisarles a la brevedad posible la operación efectuada. Si no fuese posible determinar las personas a quienes se les hayan comunicado, pondrá un aviso que pueda ser de general conocimiento para quienes usen la información del banco de datos.

Artículo 13.- El derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales no puede ser limitado por medio de ningún acto o convención.

Artículo 14.- Si los datos personales están en un banco de datos al cual tienen acceso diversos organismos, el titular puede requerir información a cualquiera de ellos.

Artículo 15.- No obstante lo dispuesto en este Título, no podrá solicitarse información, modificación, cancelación o bloqueo de datos personales cuando ello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional.

Tampoco podrá pedirse la modificación, cancelación o bloqueo de datos personales almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva.

Artículo 16.- Si el responsable del registro o banco de datos no se pronunciare sobre la solicitud del requirente dentro de dos días hábiles, o la denegare por una causa distinta de la seguridad de la Nación o el interés nacional, el titular de los datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable, que se encuentre de turno según las reglas correspondientes, solicitando amparo a los derechos consagrados en el artículo precedente.

El procedimiento se sujetará a las reglas siguientes:

a) La reclamación señalará claramente la infracción cometida y los hechos que la configuran, y deberá acompañarse de los medios de prueba que los acrediten, en su caso.

b) El tribunal dispondrá que la reclamación sea notificada por cédula, dejada en el domicilio del responsable del banco de datos correspondiente. En igual forma se notificará la sentencia que se dicte.

c) El responsable del banco de datos deberá presentar sus descargos dentro de quinto día hábil y adjuntar los medios de prueba que acrediten los hechos en que los funda. De no disponer de ellos, expresará esta circunstancia y el tribunal fijará una audiencia, para dentro de quinto día hábil, a fin de recibir la prueba ofrecida y no acompañada.

d) La sentencia definitiva se dictará dentro de tercero día de vencido el plazo a que se refiere la letra anterior, sea que se hayan o no presentado descargos. Si el tribunal decretó una audiencia de prueba, este plazo correrá una vez vencido el plazo fijado para ésta.

e) Todas las resoluciones, con excepción de la indicada en la letra f) de este inciso, se dictarán en única instancia y se notificarán por el estado diario.

f) La sentencia definitiva será apelable en ambos efectos. El recurso deberá interponerse en el término fatal de cinco días, contado desde la notificación de la parte que lo entabla, deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

g) Deducida la apelación, el tribunal elevará de inmediato los autos a la Corte de Apelaciones respectiva. Recibidos los autos en la Secretaría de la Corte, el Presidente ordenará dar cuenta preferente del recurso, sin esperar la comparecencia de ninguna de las partes.

h) El fallo que se pronuncie sobre la apelación no será susceptible de los recursos de casación.

En caso de que la causal invocada para denegar la solicitud del requirente fuere la seguridad de la Nación o el interés nacional, la reclamación deberá deducirse ante la Corte Suprema, la que solicitará informe de la autoridad de que se trate por la vía que considere más rápida, fijándole plazo al efecto, transcurrido el cual resolverá en cuenta la controversia. De recibirse prueba, se consignará en un cuaderno separado y reservado, que conservará ese carácter aun después de afinada la causa si por sentencia ejecutoriada se denegare la solicitud del requirente.

La sala de la Corte Suprema que conozca la reclamación conforme al inciso anterior, o la sala de la Corte de Apelaciones que conozca la apelación, tratándose del procedimiento establecido en los incisos primero y segundo, si lo estima conveniente o se le solicita con fundamento plausible, podrá ordenar traer los autos en relación para oír a los abogados de las partes, caso en el cual la causa se agregará extraordinariamente a la tabla respectiva de la misma sala. En las reclamaciones por las causales señaladas en el inciso precedente, el Presidente del Tribunal dispondrá que la audiencia no sea pública.

En caso de acogerse la reclamación, la misma sentencia fijará un plazo prudencial para dar cumplimiento a lo resuelto y podrá aplicar una multa de una a diez unidades tributarias mensuales.

La falta de entrega oportuna de la información o el retardo en efectuar la modificación, en la forma que decrete el Tribunal, serán castigados con multa de dos a cincuenta unidades tributarias mensuales y, si el responsable del banco de datos requerido fuere un organismo público, el tribunal podrá sancionar al jefe del Servicio con la suspensión de su cargo, por un lapso de cinco a quince días.

Título III

De la utilización de datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial

Artículo 17.- Los responsables de los registros o bancos de datos personales sólo podrán comunicar información que verse sobre obligaciones de carácter económico, financiero, bancario o comercial, cuando éstas consten en letras de cambio y pagarés protestados; cheques protestados por falta de fondos, por haber sido girados contra cuenta corriente cerrada o por otra causa; como asimismo el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos, sociedades financieras, administradoras de mutuos hipotecarios, cooperativas de ahorros y créditos, organismos públicos y empresas del Estado sometidas a la legislación común, y de sociedades administradoras de créditos otorgados para compras en casas comerciales.

También podrán comunicarse aquellas otras obligaciones de dinero que determine el Presidente de la República mediante decreto supremo, las que deberán estar sustentadas en instrumentos de pago o de crédito válidamente emitidos, en los cuales conste el consentimiento expreso del deudor u obligado al pago y su fecha de vencimiento.

Artículo 18.- En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos siete años desde que la respectiva obligación se hizo exigible.

Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de transcurridos tres años del pago o de su extinción por otro modo legal.

Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes.

Artículo 19.- El pago o la extinción de estas obligaciones por cualquier otro modo no produce la caducidad o la pérdida de fundamento legal de los datos respectivos para los efectos del artículo 12, mientras estén pendientes los plazos que establece el artículo precedente.

Al efectuarse el pago o extinguirse la obligación por otro modo en que intervenga directamente el acreedor, éste avisará tal hecho, a más tardar dentro de los siguientes siete días hábiles, al responsable del registro o banco de datos accesible al público que en su oportunidad comunicó el protesto o la morosidad, a fin de que consigne el nuevo dato que corresponda, previo pago de la tarifa si fuere procedente, con cargo al deudor. El deudor podrá optar por requerir directamente la modificación al banco de datos y liberar del cumplimiento de esa obligación al acreedor que le entregue constancia suficiente del pago; decisiones que deberá expresar por escrito.

Quienes efectúen el tratamiento de datos personales provenientes o recolectados de la aludida fuente accesible al público deberán modificar los datos en el mismo sentido tan pronto aquélla comunique el pago o la extinción de la obligación, o dentro de los tres días siguientes. Si no les fuera posible, bloquearán los datos del respectivo titular hasta que esté actualizada la información.

La infracción de cualquiera de estas obligaciones se conocerá y sancionará de acuerdo a lo previsto en el artículo 16.

Título IV

Del tratamiento de datos por los organismos públicos

Artículo 20.- El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular.

Artículo 21.- Los organismos públicos que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias, no

podrán comunicarlos una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena.

Exceptúase los casos en que esa información les sea solicitada por los tribunales de Justicia u otros organismos públicos dentro del ámbito de su competencia, quienes deberán guardar respecto de ella la debida reserva o secreto y, en todo caso, les será aplicable lo dispuesto en los artículos 5º, 7°, 11 y 18.

Artículo 22.- El Servicio de Registro Civil e Identificación llevará un registro de los bancos de datos personales a cargo de organismos públicos.

Este registro tendrá carácter público y en él constará, respecto de cada uno de esos bancos de datos, el fundamento jurídico de su existencia, su finalidad, tipos de datos almacenados y descripción del universo de personas que comprende, todo lo cual será definido en un reglamento.

El organismo público responsable del banco de datos proporcionará esos antecedentes al Servicio de Registro Civil e Identificación cuando se inicien las actividades del banco, y comunicará cualquier cambio de los elementos indicados en el inciso anterior dentro de los quince días desde que se produzca.

Título V
De la responsabilidad por las infracciones a esta ley

Artículo 23.- La persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal.

La acción consiguiente podrá interponerse conjuntamente con la reclamación destinada a establecer la infracción, sin perjuicio de lo establecido en el artículo 173 del Código de Procedimiento Civil. En todo caso, las infracciones no contempladas en los artículos 16 y 19, incluida la indemnización de los perjuicios, se sujetarán al procedimiento sumario. El juez tomará todas las providencias que estime convenientes para hacer efectiva la protección de los derechos que esta ley establece. La prueba se apreciará en conciencia por el juez.

El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.

Título Final

Artículo 24.- Agrégase los siguientes incisos segundo y tercero, nuevos, al artículo 127 del Código Sanitario:

"Las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo.

Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos.".

Disposiciones transitorias

Artículo 1°.- Las disposiciones de esta ley, con excepción del artículo 22, entrarán en vigencia dentro del plazo de sesenta días, contados desde la fecha de su publicación en el Diario Oficial.

Los actuales registros o bancos de datos personales de organismos públicos se ajustarán a las disposiciones de este cuerpo legal, a contar de su entrada en vigencia.

Lo dispuesto en el artículo 22 comenzará a regir un año después de la publicación de esta ley. Sin perjuicio de lo anterior, los organismos públicos que tuvieren a su cargo bancos de datos personales deberán remitir los antecedentes a que se refiere dicho precepto con anterioridad, dentro del plazo que fije el reglamento.

Artículo 2°.- Los titulares de los datos personales registrados en bancos de datos creados con anterioridad a la entrada en vigencia de la presente ley tendrán los derechos que ésta les confiere.

Artículo 3°.- Las normas que regulan el Boletín de Informaciones Comerciales creado por el decreto supremo de Hacienda N° 950, de 1928, seguirán aplicándose en todo lo que no sean contrarias a las disposiciones de esta ley.".

Habiéndose cumplido con lo establecido en el N° 1º del artículo 82 de la Constitución Política de la República y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 18 de agosto de 1999.- EDUARDO FREI RUIZ-TAGLE, Presidente de la República.- José Miguel Insulza Salinas, Ministro Secretario General de la Presidencia.- María Soledad Alvear Valenzuela, Ministra de Justicia.- Germán Quintana Peña, Ministro de Planificación y Cooperación.

Lo que transcribo a Ud., para su conocimiento.- Saluda Atte. a Ud., Carlos Carmona Santander, Subsecretario General de la Presidencia de la República.
Tribunal Constitucional

Proyecto de ley sobre protección de datos de carácter personal

El Secretario del Tribunal Constitucional, quien suscribe, certifica que el Honorable Senado envió el proyecto de ley enunciado en el rubro, aprobado por el Congreso Nacional, a fin de que este Tribunal ejerciera el control de la constitucionalidad de su artículo 16; y que por sentencia de 4 de agosto de 1999, declaró:

1. Que los preceptos contenidos en el artículo 16, del proyecto sometido a control, son constitucionales en el entendido que deben interpretarse en conformidad con lo que se ha señalado en el considerando 7º de esta sentencia.

2. Que las disposiciones contempladas en el artículo 19 del proyecto sometido a control, son constitucionales.

Santiago, agosto 6 de 1999.- Rafael Larraín Cruz, Secretario.

2) Ley 19970 que crea el Sistema Nacional de Registros de ADN.

Identificación de la Norma: Ley-19.970
Fecha de publicación: 06.10.2004
Fecha de Promulgación: 10.09.2004

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

Proyecto de ley:

"Crea el Sistema Nacional de Registros de ADN
CAPITULO I
Disposiciones Generales

Artículo 1º.- Sistema Nacional de Registros de ADN. La presente ley regula un Sistema Nacional de Registros de ADN, constituido sobre la base de huellas genéticas determinadas con ocasión de una investigación criminal.

Por huella genética se entenderá, para estos efectos, el registro alfanumérico personal elaborado exclusivamente sobre la base de información genética que sea polimórfica en la población, carezca de asociación directa en la expresión de genes y aporte sólo información identificatoria.

La obtención de la huella genética se realizará por profesionales y técnicos que se desempeñen en el Servicio Médico Legal, o en instituciones públicas o privadas que se encontraren acreditadas para tal efecto ante dicho servicio.

La administración y custodia del sistema estará a cargo del Servicio de Registro Civil e Identificación, correspondiendo en general al Servicio Médico Legal el ingreso de la información, así como, previa acreditación especial al efecto y sólo respecto de las huellas que hubieren determinado, a las instituciones públicas o privadas aludidas en el inciso precedente.

Artículo 2º.- Principios. El sistema tendrá carácter reservado. La información en él contenida sólo podrá ser directamente consultada por el Ministerio Público y los tribunales. Las policías podrán tener acceso previa autorización del Ministerio Público, y los defensores públicos y privados, previa autorización del tribunal respectivo.

Bajo ningún supuesto el Sistema podrá constituir base o fuente de discriminación, estigmatización, vulneración de la dignidad, intimidad, privacidad u honra de persona alguna.

Artículo 3º.- Naturaleza de los datos y su titularidad. La información contenida en el Sistema y, en particular, las muestras biológicas y las huellas genéticas, se considerarán datos sensibles de sus titulares, según lo dispuesto en la ley Nº19.628, sobre protección de la vida privada.

CAPITULO II
De los Registros

Artículo 4º.- Registros. El Sistema estará integrado por el Registro de Condenados, el Registro de Imputados, el Registro de Evidencias y Antecedentes, el Registro de Víctimas y el Registro de Desaparecidos y sus Familiares.

Artículo 5º.- Registro de Condenados. El Registro de Condenados contendrá las huellas genéticas de las personas que hubieren sido condenadas en un proceso criminal por sentencia ejecutoriada, en los casos a que se refiere el artículo 17 de esta ley.

Las huellas genéticas incluidas en este Registro deberán ser integradas adicionalmente a los antecedentes que consten en el prontuario penal de los condenados. La eliminación de los antecedentes contenidos en el prontuario penal, realizada en conformidad a la ley y a los reglamentos correspondientes, no implicará la eliminación de la huella genética contenida en el Registro de que trata este artículo.

Artículo 6º.- Registro de Imputados. El Registro de Imputados contendrá las huellas genéticas de quienes hubieren sido imputados de un delito, determinadas sobre la base de muestras biológicas obtenidas en conformidad con lo dispuesto en el Código Procesal Penal y en el artículo 17 de esta ley.

Artículo 7º.- Registro de Evidencias y Antecedentes. En el Registro de Evidencias y Antecedentes se conservarán las huellas genéticas que hubieren sido obtenidas en el curso de una investigación criminal y que correspondieren a personas no identificadas.

Artículo 8º.- Registro de Víctimas. El Registro de Víctimas contendrá las huellas genéticas de las víctimas de un delito, determinadas en el curso de un procedimiento criminal.

En todo caso, no se incorporará al Registro la huella genética de la víctima que expresamente se opusiere a ello. Para tal efecto, quien tome la muestra biológica consignará el hecho de corresponder a una víctima. El Servicio Médico Legal o, en su caso, la institución especialmente acreditada que hubiere determinado la huella genética, se abstendrán de incorporarla en el Registro hasta recibir tal instrucción del Ministerio Público, el que previamente consultará a la víctima, informándola acerca de su derecho.

Las huellas agregadas a este Registro serán eliminadas en la forma prevista en el artículo 18.

Artículo 9º.- Registro de Desaparecidos y sus Familiares. El Registro de Desaparecidos y sus Familiares contendrá las huellas genéticas de:

a) cadáveres o restos humanos no identificados;

b) material biológico presumiblemente proveniente de personas extraviadas, y

c) personas que, teniendo un familiar desaparecido o extraviado, acepten voluntariamente donar una muestra biológica que pueda resultar de utilidad para su identificación.

CAPITULO III

De la toma de muestras, obtención de evidencias, determinación de huellas genéticas y cotejo de las mismas

Artículo 10.- Toma de muestras biológicas. Los casos y formas en que se procederá a la toma de las muestras biológicas se regularán por las disposiciones de la ley procesal penal que sean aplicables.

Artículo 11.- Reserva y custodia. Toda persona que intervenga en la toma de muestras, obtención de evidencias y determinación de huellas genéticas, deberá mantener la reserva de los antecedentes y la integridad de la cadena de custodia, de acuerdo con las exigencias que imponga el reglamento a que se refiere el artículo 21 de esta ley.

Artículo 12.- Remisión de informe y material biológico. El organismo que hubiere determinado la huella genética evacuará el informe que dé cuenta de la pericia y lo remitirá al fiscal del Ministerio Público o al tribunal respectivo, según correspondiere. Tratándose de las instituciones públicas o privadas acreditadas, deberán, además, remitir al Servicio Médico Legal la totalidad del material biológico y el resto del ADN extraído, a partir de los cuales se obtuvo la huella, la copia del aludido informe y los demás antecedentes que disponga el Reglamento.

Artículo 13.- Pericia de Cotejo y Remisión de Informe. El Servicio Médico Legal procederá a practicar el peritaje de cotejo de la huella genética en cuestión, contrastándola con las demás huellas contenidas en uno o más Registros del Sistema, según le hubiere sido específicamente requerido en un procedimiento penal.

Practicado el cotejo, el Servicio Médico Legal enviará al fiscal del Ministerio Público o al tribunal, según correspondiere, el informe que dé cuenta de la pericia y de sus resultados.

Artículo 14.- Conservación y destrucción del material biológico. Inmediatamente después de evacuado el informe de que trata el artículo precedente o de recibidos los antecedentes a que se refiere el artículo 12, el Servicio Médico Legal deberá proceder a la destrucción del material biológico que hubiere sido objeto de un examen de ADN.

Con todo, cuando la obtención del material biológico fuere calificada por el Servicio Médico Legal como técnicamente irrepetible, el Ministerio Público deberá ordenar la conservación de una parte de aquél, hasta por treinta años.

De la destrucción o conservación de las muestras biológicas se dejará constancia escrita por el funcionario encargado. Dicha constancia deberá contener los datos que

permitan identificar las muestras de que se trate, así como las razones que, en el caso concreto, hubieren justificado la medida de conservación.

Los funcionarios a cargo de la destrucción de las muestras biológicas deberán remitir mensualmente a su superior jerárquico las listas de muestras ingresadas, destruidas y conservadas en dicho período, incluyendo, en su caso, las razones a que se refiere el inciso precedente. Asimismo, un informe consolidado que contendrá la lista de las muestras biológicas ingresadas, destruidas y conservadas en el período respectivo, se remitirá semestralmente al Director Nacional del Servicio Médico Legal por los directores médicos regionales o, en el caso de la Región Metropolitana de Santiago, por el jefe del departamento competente.

Los funcionarios que, debiendo proceder a la destrucción del material biológico, no lo hicieren, incurrirán en responsabilidad administrativa.

Artículo 15.- Reembolso. El Ministerio Público, el querellante, la Defensoría Penal Pública o el defensor, según correspondiere, deberán reembolsar el importe del servicio a la institución que hubiere determinado la huella genética o realizado la pericia de cotejo, importe que constituirá ingreso propio de la institución. Lo anterior es sin perjuicio de lo que se resuelva sobre costas.

Con todo, tratándose de las huellas genéticas determinadas en cumplimiento de lo dispuesto en los incisos segundo y tercero del artículo 17, el importe de la pericia será de cargo del Servicio Médico Legal. En dichos casos la determinación de las huellas genéticas deberá siempre solicitarse al referido servicio.

Los aranceles a cobrar por las instituciones públicas serán fijados anualmente por resolución del director o jefe superior de la respectiva entidad.

CAPITULO IV

De la administración del Sistema Nacional de Registros de ADN

Artículo 16.- Incorporación de las huellas genéticas en los Registros del Sistema. Tratándose de huellas genéticas correspondientes a condenados o imputados, su incorporación en los respectivos Registros del Sistema se ejecutará por orden del tribunal.

Tratándose de huellas genéticas correspondientes a víctimas, evidencias o desaparecidos o sus familiares, su incorporación en los respectivos Registros del Sistema se ejecutará por orden del fiscal del Ministerio Público, sin perjuicio de lo dispuesto en el artículo 8º.

En los casos a que se refieren los incisos precedentes, la incorporación en los Registros será ejecutada por el organismo que hubiere determinado la huella genética. En todo caso, las instituciones públicas o privadas no especialmente acreditadas para el ingreso de información al Sistema, remitirán la huella genética al Servicio Médico Legal para que éste la incorpore en el Registro correspondiente.

Con todo, en los casos a que se refiere el inciso primero del artículo 17 de esta ley, la incorporación de la huella en el Registro de Condenados se llevará a cabo por el Servicio de Registro Civil.

Artículo 17.- Incorporación de huellas genéticas de imputados al Registro de Condenados. Cuando, por sentencia ejecutoriada, se condenare por alguno de los delitos previstos en el inciso siguiente a un imputado cuya huella genética hubiere sido determinada durante el procedimiento criminal, se procederá a incluir la huella genética en el Registro de Condenados, eliminándola del Registro de Imputados.

Si no se hubiere determinado la huella genética del imputado durante el procedimiento criminal, en la sentencia condenatoria el tribunal ordenará que se determine, previa toma de muestras biológicas si fuere necesario, y se incluya en el Registro de Condenados. Lo anterior sólo tendrá lugar cuando se condenare al imputado por alguno de los siguientes delitos:

a) los previstos en los artículos 141, 142, 150 A, 150 B, 296 Nºs. 1 y 2, 313 d, 315, 316, 348, 352, 395, 396, 397 Nº 1, 401, 403 bis, 433, 436 inciso primero, 440, 474, 475, 476, y 480 del Código Penal;

b) los previstos en los Párrafos 1º, 5º, 6º y 7º del Título VII y 1º y 2º del Título VIII del Libro Segundo del Código Penal, y

c) elaboración o tráfico ilícitos de estupefacientes o delito terrorista.

En todo caso, el tribunal competente, de oficio o a petición del fiscal, y en consideración a los antecedentes personales del condenado, así como a la naturaleza, modalidades y móviles determinantes del delito, podrá ordenar en la sentencia la práctica de las mismas diligencias de toma de muestras biológicas y determinación y registro de huellas genéticas respecto de un condenado a pena de crimen que no se encontrare en las situaciones previstas en el inciso precedente.

Artículo 18.- Eliminación de huellas genéticas contenidas en el Sistema. Las huellas genéticas contenidas en los Registros de Imputados y de Víctimas, serán eliminadas una vez que se hubiere puesto término al procedimiento criminal respectivo. Si hubo juicio,

procederá la eliminación desde que se falló por resolución ejecutoriada, sin perjuicio de lo previsto en el inciso primero del artículo precedente.

El Servicio de Registro Civil e Identificación deberá proceder a la eliminación o reingreso a que se refiere el inciso precedente en un plazo no superior a tres días, contado desde que le fuere comunicado el término del procedimiento por el fiscal. Dicha comunicación se efectuará por cualquier medio idóneo que permita dejar constancia fehaciente de su despacho y recepción. Igualmente procederá el Servicio de Registro Civil e Identificación a solicitud de la víctima o del imputado, cuando éstos acreditaren el término del procedimiento, mediante certificación expedida por el fiscal o el tribunal respectivo.

En cualquier caso, las huellas genéticas contenidas en los Registros de Imputados, de Víctimas y de Evidencias y Antecedentes, serán eliminadas una vez transcurridos treinta años desde la fecha de su incorporación a éstos.

De la eliminación y reingreso de los antecedentes de que trata este artículo se dejará constancia escrita por el funcionario encargado. Dicha constancia deberá contener los datos que permitan identificar las huellas genéticas de que se trate, así como la comunicación de término del procedimiento, si fuere el caso.

Los funcionarios a cargo de la eliminación de las huellas genéticas deberán remitir mensualmente a sus superiores jerárquicos las listas de huellas eliminadas y reingresadas en dicho período, incluyendo los datos a que se refiere el inciso precedente.

Los funcionarios que, debiendo proceder a la eliminación o reingreso de los antecedentes de los registros, no lo hicieren o lo hicieren extemporáneamente, incurrirán en responsabilidad administrativa.

CAPITULO V

De las responsabilidades y sanciones

Artículo 19.- Acceso, divulgación y uso indebido de la información genética. Quienes, interviniendo en alguno de los procedimientos regulados en la presente ley en razón de su cargo o profesión, permitieren el acceso a los registros o exámenes a personas no autorizadas, o los divulgaren o usaren indebidamente, serán sancionados con presidio menor en sus grados mínimo a medio y multa de seis a diez unidades tributarias mensuales.

En caso de que el acceso, la divulgación o el uso se efectuare respecto de las muestras biológicas o evidencias, se impondrá la pena de presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales.

Quienes, sin tener las calidades referidas en el inciso primero, accedieren a los registros, exámenes o muestras, los divulgaren o los usaren indebidamente, serán sancionados con la pena de presidio menor en sus grados mínimo a medio o multa de seis a diez unidades tributarias mensuales.

Artículo 20.- Obstrucción a la justicia. El que alterare las muestras biológicas que debieren ser objeto del examen de ADN; falseare el resultado de dichos exámenes o la determinación de la huella genética; faltare a la verdad en el informe pericial de examen o cotejo, o adulterare su contenido, será sancionado con la pena de presidio menor en su grado medio y multa de seis a diez unidades tributarias mensuales.

Con igual pena será sancionado el que indebidamente eliminare o alterare huellas genéticas o sus datos asociados, contenidos en el Sistema Nacional de Registros de ADN.

El que, teniendo el deber de intervenir en alguno de los procedimientos regulados en la presente ley en razón de su cargo o profesión, incurriere en cualquiera de las conductas previstas en los incisos precedentes, será sancionado con la pena de presidio menor en su grado máximo y multa de seis a diez unidades tributarias mensuales.

Con la misma pena será sancionado el que, teniendo el deber de incorporar una huella genética al Sistema Nacional de Registros de ADN, no lo hiciere.

CAPITULO VI

Disposiciones finales

Artículo 21.- Reglamento. Un reglamento, dictado por intermedio del Ministerio de Justicia, determinará las características del Sistema Nacional de Registros de ADN; las modalidades de su administración, y las normas técnicas que regulen los procedimientos aplicables a la toma de muestras, la conservación de evidencias, y su cadena de custodia.

Asimismo, regulará los requisitos y condiciones que deberán cumplir las instituciones públicas o privadas que deseen acreditar ante el Servicio Médico Legal su idoneidad para determinar huellas genéticas e incorporarlas en el sistema, de acuerdo a lo previsto en el artículo 199 bis del Código Procesal Penal.

Artículo 22.- Concordancia. Serán aplicables, en cuanto no se opusieren a lo previsto en esta ley, las normas contempladas en la ley Nº 19.628 sobre protección de la vida privada.

Artículo 23.- Modificaciones al Código Procesal Penal. Introdúcense las siguientes modificaciones al Código Procesal Penal:

1.- Agrégase el siguiente inciso tercero, nuevo, al artículo 198:

"Si los mencionados establecimientos no se encontraren acreditados ante el Servicio Médico Legal para determinar huellas genéticas, tomarán las muestras biológicas y obtendrán las evidencias necesarias, y procederán a remitirlas a la institución que corresponda para ese efecto, de acuerdo a la ley que crea el Sistema Nacional de Registros de ADN y su Reglamento.".

2.- Introdúcese el siguiente artículo 199 bis, nuevo:

"Artículo 199 bis. Exámenes y pruebas de ADN. Los exámenes y pruebas biológicas destinados a la determinación de huellas genéticas sólo podrán ser efectuados por profesionales y técnicos que se desempeñen en el Servicio Médico Legal, o en aquellas instituciones públicas o privadas que se encontraren acreditadas para tal efecto ante dicho Servicio.

Las instituciones acreditadas constarán en una nómina que, en conformidad a lo dispuesto en el Reglamento, publicará el Servicio Médico Legal en el Diario Oficial.".

Artículo 24.- Vigencia. La presente ley entrará a regir el día en que se publique en el Diario Oficial el reglamento a que se refiere el artículo 21.

Disposiciones Transitorias

Artículo 1º.- Para los efectos de lo dispuesto en el artículo 5º, el Servicio Médico Legal, o las instituciones públicas o privadas acreditadas ante él, determinarán la huella genética de las personas que se encontraren cumpliendo condena por alguno de los delitos señalados en el artículo 17, previa extracción de la muestra biológica respectiva en los establecimientos en que estuvieren internados.

Gendarmería de Chile informará a los condenados que no estuvieren recluidos el lugar y la oportunidad en que deberán proporcionar su muestra biológica, bajo apercibimiento de informar al tribunal respectivo sobre el incumplimiento de esta obligación.

Artículo 2º.- Normas especiales aplicables a los procesos substanciados conforme al Código de Procedimiento Penal. En los procesos substanciados conforme al Código de Procedimiento Penal se estará especialmente a lo dispuesto en las reglas siguientes:

a) Las referencias hechas en esta ley a los imputados se entenderán efectuadas a los procesados. En consecuencia, el Registro de Imputados contendrá, además de las huellas genéticas de imputados en conformidad con las normas del Código Procesal Penal, las de aquellas personas que fueren procesadas de acuerdo con las disposiciones del Código de Procedimiento Penal;

b) Las funciones o competencias que en esta ley se atribuyen al Ministerio Público, serán desempeñadas o asumidas por los jueces con competencia en lo criminal;

c) Los jueces con competencia en lo criminal ordenarán la incorporación al registro respectivo de las huellas genéticas determinadas a partir de muestras biológicas obtenidas durante el proceso para constatar circunstancias relevantes de la investigación, en virtud de lo dispuesto en los artículos 110, 111, 145 bis y 221 del Código de Procedimiento Penal;

d) En relación con los informes periciales destinados a determinar la huella genética, recibirá aplicación lo dispuesto en los artículos 221 y 245 del Código de Procedimiento Penal, y

e) La comunicación a que se refiere el inciso segundo del artículo 18 se efectuará por el tribunal que hubiere conocido del proceso en primera instancia, en la misma forma prevista en dicha disposición.

Artículo 3º.- El mayor gasto que irrogue esta ley durante el primer año de su aplicación, se financiará con cargo a los recursos asignados al Servicio de Registro Civil e Identificación y al Servicio Médico Legal en sus respectivos presupuestos, en lo que correspondiere a cada una de estas instituciones.".

Habiéndose cumplido con lo establecido en el Nº 1º del artículo 82 de la Constitución Política de la República y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

Santiago, 10 de septiembre de 2004.- RICARDO LAGOS ESCOBAR, Presidente de la República.- Luis Bates Hidalgo, Ministro de Justicia.- Nicolás Eyzaguirre Guzmán, Ministro de Hacienda.

Lo que transcribo a Ud. para su conocimiento.- Saluda atentamente a Ud., Jaime Arellano Quintana, Subsecretario de Justicia.

Tribunal Constitucional

Proyecto de ley sobre creación del Sistema Nacional de Registros de ADN

El Secretario del Tribunal Constitucional, quien suscribe, certifica que el Honorable Senado envió el proyecto de ley enunciado en el rubro, aprobado por el Congreso

Nacional, a fin de que este Tribunal ejerciera el control de constitucionalidad respecto de la letra b) del artículo 2º transitorio, del mismo, y por sentencia de 19 de agosto de 2004, dictada en los autos Rol Nº 419, declaró:

1. Que la letra b) del artículo 2º transitorio, del proyecto remitido, es constitucional.

2. Que los artículos 2º, 8º, 14, 16, y 2º transitorio, inciso único, letras a), c), d) y e), son igualmente constitucionales.

Santiago, agosto 24 de 2004.- Rafael Larraín Cruz, Secretario.

3) Ley 19233 relativa a Delitos Informáticos.

Identificación de la Norma: Ley-19.223
Fecha de publicación: 07.06.1993
Fecha de Promulgación: 28.05.1993

Articulo 1°.- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

Articulo 2°.- El que con el ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Articulo 3°.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Articulo 4°.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

4) Sentencia de la Corte Suprema ante Recurso de Protección

A continuación se transcribe en primer lugar el escrito presentado ante la Corte de Apelaciones de Santiago por la interposición de un recurso de protección que buscaba principalmente el resguardo, respeto y protección a la vida privada y honra de la persona y de su familia, seguida en contra de la Corporación Administrativa del Poder Judicial. En un primer término la Corte de Apelaciones rechazó el recurso y se presentó un recurso de apelación frente a la Corte Suprema, segundo escrito que también se encuentra agregado en forma íntegra. Lo subrayado y resaltado corresponde a un copia de lo que se subrayó y resaltó en el escrito originalmente presentado.

1º ESCRITO DE RECURSO DE APELACION

ROL 1211-2001.

MATERIA: RECURSO DE PROTECCIÓN (Respeto y protección a la vida privada y honra de la persona y de su familia; igualdad ante la ley, no discriminación arbitraria; integridad psíquica de la persona: derecho de propiedad, **art. 19 Nºs 1º, 20, 40 y 240. C. P. R. 1980)**

SECRETARÍA : ESPECIAL

RECURRENTE : XXXXX

RUT :XXXX

RECURRIDO : CORPORACIÓN ADMINISTRATIVA DEL PODER JUDICIAL

RUT :XXXX

REPRESENTANTE:XXX

En lo Principal: Interpone recurso de protección; **Primer Otrosí:** Acompaña documentos.

ILTMA. CORTE DE APELACIONES DE SANTIAGO

...a US., litma., respetuosamente digo:

HECHOS

El día primero de marzo de¡ 2001 me enteré por intermedio de una amiga, quien ingresó a través de Internet al recién inaugurado sitio Web del Poder Judicial de Chile, que en dicha página al introducir mi nombre en el sistema de búsquedas, (estado de causas de Santiago), aparecen los datos de una demanda que tengo interpuesta por la reclamación de paternidad de mi hija. A fin de indagar más antecedentes acerca de tal circunstancia al día siguiente ingresé a la referida página web -(www.poderjudicial.cl)- y en ella pude constatar que al pulsar en el vínculo "Cuaderno Principal" fuera de figurar los nombres de los abogados patrocinantes aparecían individualizadas las partes con nombre completo y número de cédula nacional de identidad, tanto los míos como los del demandado. Es decir, cualquier individuo, desde cualquier lugar del país o del mundo, con tan sólo ingresar mi nombre al sistema de búsquedas de la base de datos del referido sitio web podía enterarse que yo, (o cualquiera otra persona) tengo actualmente una hija no reconocida por su padre, o bien, mirándolo desde el punto de vista contrario, que determinada persona ha sido demandada por otra también determinada persona por ser el presunto padre o madre de un hijo no reconocido, INVADIENDO AL PODER ACCEDER A ESA INFORMACIÓN UNA DE LAS ESFERAS MÁS SENSIBLES DEL DERECHO A LA INTIMIDAD DE LA PERSONA Y DE SU FAMILIA; CUAL ES, LA NATURALEZA DE SU FILIACIÓN, hechos que me tienen muy afligida.

Asimismo, pude ver que en el cuadro "Materia" decía **"HIJO LEGITIMO, ACCIÓN",** lo cual me sorprendió sobremanera pues la demanda que tengo interpuesta, bajo la vigencia de la ley NO 19.585, es una acción de reclamación de paternidad en filiación no matrimonial. Digo me sorprendió, pues entiendo que las desigualdades jurídicas de los hijos han sido eliminadas, por lo que no puedo entender que la página web "hijo legítimo, acción", expresión de la cual se desprende que en este momento mi hija sería ¡legítima, CIRCUNSTANCIA ESTA QUE SIN DUDA LA ESTIGMATIZA Y DISCRIMINA.

También efectué la consulta ingresando el número de mi Cédula Nacional de Identidad y obtuve los mismos resultados señalados. Por otra parte, pude constatar del mismo

modo, que a diferencia de mi demanda de filiación, las causas sobre violencia intrafamiliar tienen el acceso restringido, figurando solamente con su respectivo número de proceso y tribunal sin siquiera señalar cómo está caratulada la causa. En cambio, respecto del juicio de filiación, en mi caso por lo menos - pues desconozco si se trata de una situación general que afecta a todas las personas que mantienen juicios de filiación pendientes o si solo me afecta a mí únicamente - además de informar los datos normales de cualquier causa judicial, como son el tribunal, el número de expediente, los últimos movimientos de la causa y el caratulado del proceso, también SE INFORMA A QUIEN QUIERA SABERLO, LA INDIVIDUALIZACIÓN DE LAS PERSONAS QUE TIENEN HIJOS NO RECONOCIDOS Y CUYA FILIACIÓN ESTÁN RECLAMANDO.

EL SITIO EN INTERNET ALUDIDO, - según consta de información proporcionada en la misma página web - ha sido elaborado y se encuentra en construcción por la CORPORACIÓN ADMINISTRATIVA DEL PODER JUDICIAL, PERSONA JURÍDICA, RUT 60.301.001-9, REPRESENTADA POR DON HERNÁN ÁLVAREZ GARCÍA, CON DOMICILIO EN HUÉRFANOS No 1409, PISO 17, SANTIAGO, ORGANISMO PÚBLICO ENCARGADO DEL REGISTRO DE LOS DATOS QUE CONTIENE, POR LO QUE EN RAZÓN DE LOS HECHOS EXPUESTOS Y DE LAS CONSIDERACIONES DE DERECHO QUE MÁS ADELANTE EXPONGO, VENGO EN RECURRIR DE PROTECCIÓN EN CONTRA DE LA CITADA CORPORACIÓN ADMINISTRATIVA DEL PODER JUDICIAL, POR PUBLICAR DATOS *SENSIBLES Y EXPRESIONES DISCRIMINATORIAS* EN EL BANCO 0 BASE DE DATOS QUE MANTIENE EN LA INTERNET, LO QUE CONSIDERO UNA ACTUACIÓN ILEGAL Y ARBITRARIA QUE CAUSA PRIVACIÓN, PERTURBACIÓN Y AMENAZA EN EL LEGÍTIMO EJERCICIO DE MI DERECHO A LA PRIVACIDAD Y HONRA DE Mi PERSONA Y DE Mi FAMILIA Y UN ACTO DE DISCRIMINACIÓN CONTRA MI HIJA, LO CUAL, A SU VEZ, DAÑA PROFUNDAMENTE MI DIGNIDAD HUMANA, AMENAZANDO Y PERTURBANDO MI INTEGRIDAD PSÍQUICA, MORAL Y EMOCIONAL.

CONSIDERACIONES DE DERECHO

La **Ley Nº 19.628,** publicada en el Diario Oficial de 28 de agosto de 1999, **Sobre Protección de la Vida Privada,** regula el tratamiento de datos personales en registros o

bancos de datos estableciendo el marco jurídico al que debe sujetarse toda persona natural o jurídica privada u organismo público a cargo de dichos registros, prescribiendo limitaciones, prohibiciones, responsabilidades y sanciones a fin de cautelar debidamente la efectiva protección de la vida privada y honra de la persona y de su familia. Se entiende por tratamiento de datos, de acuerdo a la definición que da **la letra o) del artículo 20** de esta ley "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma." Y se entiende por datos de carácter personal o datos personales "los relativos a cualquier información concerniente a personas naturales, identificadas o identificabas." (art. 20 letra f).

Asimismo, el artículo **20 letra g)** de la ley en comento define lo que debe entenderse por *datos sensibles:*

"DATOS SENSIBLES, SON AQUELLOS DATOS PERSONALES QUE **SE REFIEREN** A LAS CARACTERÍSTICAS FÍSICAS 0 MORALES DE LAS PERSONAS 0 A **HECHOS 0 CIRCUNSTANCIAS DE SU VIDA PRIVADA 0 INTIMIDAD,** TALES COMO LOS HÁBITOS PERSONALES, EL ORIGEN RACIAL, LAS IDEOLOGÍAS Y OPINIONES POLÍTICAS, LAS CREENCIAS 0 CONVICCIONES RELIGIOSAS, LOS ESTADOS DE SALUD FÍSICOS 0 PSÍQUICOS Y LA VIDA SEXUAL." (La expresión *"tales como"* que utiliza el precepto legal citado aclara el carácter meramente enunciativo de los hechos, circunstancias o características físicas o morales que quedan amparados bajo el concepto de *"datos sensibles'@.*

Es decir, queda comprendido dentro de lo que debemos entender por *datos sensibles* **la vida privada e intimidad de las personas. El Derecho a la** intimidad, **protege precisamente un ámbito de autonomía constituido por** los sentimientos-hábitos y costumbres, **las -relaciones filiales, familiares,** las creencias religiosas, la salud física y mental, en otros aspectos o facetas de la vida humana.

Luego, el **articulo 10º** de la citada **Ley 19.628** establece la siguiente prohibición: **"NO** PUEDEN SER OBJETO DE TRATAMIENTO LOS DATOS **SENSIBLES,** SALVO CUANDO UNA LEY LO AUTORICE, EXISTA **CONSENTIMIENTO DEL TITULAR 0 SEAN DATOS NECESARIOS PARA LA**

DETERMINACIÓN U OTORGAMIENTO DE BENEFICIOS DE SALUD QUE CORRESPONDAN A SUS TITULARES."

Ahora bien, la naturaleza de una filiación o relación filial como por ejemplo, estar o no reconocida una persona por su padre o madre, o ser madre o padre de un hijo no reconocido por su padre o madre, es indudablemente, unos de los aspectos que atañen directamente la intimidad de las personas, su vida privada, una de las esferas más íntimas y sensibles de la persona y de su familia. ¿Cómo podría estimarse que no constituye un atentado al derecho que tiene todo ser humano a recibir respeto y protección en su vida privada y honra personal y de su familia, especialmente por parte de¡ Estado y la sociedad, el hecho de que cualquier persona desde cualquier computador, pueda acceder a un banco de datos vía internet y sin necesidad de identificarse, sin pasar por ningún control o limitación de acceso, y con tan solo ingresar el nombre de la persona pueda enterarse de si ésta tiene algún hijo no reconocido por su padre o madre, o que tal persona (con nombres, apellidos y Rut), ha sido demandada por ser el presunto padre o madre de otra persona que reclama su filiación.? Como quiera que sea que definamos la intimidad, no podemos dejar de admitir que este derecho tiene que ver con la posibilidad de que algo de lo que hacemos, algo que nos acontece o que somos, no sea conocido por los demás (en el entendido de que ese algo no es ¡lícito), y, si fuera conocido por algunos, éstos no lo den a conocer a otros. ¿Será legal o razonable, publicar en la Internet, "tierra de nadie y de todos a la ve', algo tan delicado para una madre o un padre, como lo es la naturaleza filial de su hijo, especialmente si éste no ha sido reconocido por uno de sus padres? No debemos olvidar que la intimidad es un derecho que se incorpora en la Declaración Universal de los Derechos Humanos de 1948, como una de las garantías fundamentales del ser humano, derecho que es inherente al desenvolvimiento y realización del humano como tal. Mismo derecho que también el **artículo 11 inciso 211 del Pacto de San José de Costa Rica** consagra en términos tales **"Que nadie puede ser objeto de ingerencias, arbitrariedad o abusos a su vida privada o en la de su** familia." Instrumentos internacionales de Derechos Humanos suscritos y ratificados por Chile, que se encuentran actualmente vigentes y que de acuerdo al **inciso 20 del artículo 511 de la Carta de 1980,** se incorporan a nuestro ordenamiento jurídico con rango constitucional, o de menor jerarquía normativa según parte minoritaria de la doctrina y la jurisprudencia, pero en todo caso como ley de la República que viene a reiterar y complementar la garantía constitucional de respeto y protección a la vida privada y pública y a la honra de la persona y de su familia,

consagrada en el número 40 del artículo 19 de la Constitución, a la cual deben someter su acción los órganos del Estado, los titulares o integrantes de dichos órganos así como toda persona, institución o grupo.

El marco jurídico que establece la ya citada Ley 19.628, rige también con relación a los bancos o registros de datos de los organismos públicos, definidos éstos para los efectos de esta ley, en el artículo 21 letra k) del mismo cuerpo legal. "El tratamiento de datos personales por parte de un organismo 12úblico sólo puede efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes." (art.20) Es decir, garantizando la debida protección a los derechos y garantías constitucionales de sus titulares. Y si se trata de *datos sensibles,* como en el caso de autos, rige igualmente la prohibición que establece el artículo 100 trascrito precedentemente. Esto es, que tales datos no pueden ser objeto de tratamiento salvo si una ley lo autoriza expresamente, existe consentimiento del titular de los datos o su procesamiento sea necesario para determinar u otorgar beneficios de salud a sus titulares. En la especie, no existe ley que autorice a divulgar mediante un banco de datos en internet *datos sensibles* tales como la naturaleza de la filiación de las personas o el hecho de sí determinada persona es madre o padre de hijos no reconocidos.

A mayor abundamiento, LOS HECHOS POR LOS CUALES RECURRO DE PROTECCIÓN EN ESTOS AUTOS VAN CONTRA LOS PRINCIPIOS QUE INSPIRAN E INFORMAN LA **LEY NO** 19.585, publicada en el Diario Oficial de 26 de octubre de 1998, en vigencia desde el 27 de octubre de 1999, y que modificó el Código Civil y otros cuerpos legales en materia de filiación y derechos hereditarios, estableciendo rigurosos requisitos y mecanismos en resguardo de la intimidad y honra de los involucrados en un juicio de filiación, disponiendo, entre otras medidas, el **carácter secreto** del proceso. En efecto, el inciso primero de **Art. 197** del **Código Civil,** inserto dentro del **Libro I, Título VIII, "De las Acciones de Filiación",** dispone expresamente **"El proceso tendrá carácter** SECRETO **hasta que se dicte sentencia de término, y sólo tendrán acceso a él las partes y sus apoderados judiciales."**

PERO LOS HECHOS RECURRIDOS **NO** SOLO CONTRARÍAN EL ESPÍRITU DE ESTE NUEVO ESTATUTO DE FILIACIÓN, EN CUANTO NO SE RESGUARDA LA INTIMIDAD, HONRA E IDENTIDAD DE LAS PARTES ENVUELTAS EN LITIGIOS DE ESTA NATURALEZA, SINO ADEMÁS EN CUANTO CONTRADICE Y DESCONOCE UNO DE LOS PRINCIPIOS RECTORES DE LA REFORMA **EN** ESTA MATERIA CUAL ES EL MANDATO CONSTITUCIONAL

DE IGUALDAD ANTE LA LEY Y **NO** DISCRIMINACIÓN ARBITRARIA, EXPRESADO BÁSICAMENTE EN LA IGUALACIÓN JURÍDICA DE LOS HIJOS MEDIANTE LA ELIMINACIÓN DE LAS CATEGORÍAS, PROFUNDAMENTE DISCRIMINATORIAS, DE "HIJOS LEGÍT(MOS E ILEGÍTIMOS" Y EL ESTABLECIMIENTO DE UN ÚNICO ESTATUTO FILIATIVO QUE, CUMPLIDOS LOS REQUISITOS QUE -SEÑALA LA LEY, RECONOCE EL ESTADO CIVIL DE HIJO RESPECTO A DETERMINADA PERSONA ESTABLECIENDO LA IGUALDAD DE DERECHOS ENTRE TODOS LOS HIJOS. En este sentido, el principio de igualdad de los hijos envuelve no solo la igualdad ante la ley, pues además de¡ igualitario tratamiento legal de las personas en las diversas esferas de su vida social y familiar se requiere conjuntamente de un tratamiento igualitario primero por parte de quienes están llamados a ejercer las funciones públicas estatales, en especial, los agentes de la administración pública y los funcionarios de la actividad jurisdiccional, ya que frente al trato desigual y discriminatorio de las autoridades y empleados de la administración pública y judicial, por muy ocasional que sea, cualquiera disposición legal sin importar su mayor o menor jerarquía dentro de la pirámide normativa carecerá de toda eficacia y no pasará de ser una inútil declaración de buenas intenciones. Por ello, es preciso desterrar de nuestro vocabulario, y muy especialmente de nuestras prácticas, toda reminiscencia que de algún u otro modo haga supervivir la cultura discriminatoria en que por siglos nos hemos formado.

Finalmente, el derecho a respeto y protección de la vida privada y honra de la persona y de su familia, consagrado en el NI' 411 de¡ artículo 19 de la Constitución de 1980, protegido en forma especial en la Ley 19.628; así como la igualdad ante la ley que reconoce la Carta Fundamental, y que la ley 19.585, en particular, reconoce y declara respecto de todos los hijos, constituyen bienes incorporases que han ingresado a mi patrimonio jurídico y que quedan, en consecuencia, amparados por la garantía constitucional del derecho de propiedad del artículo 19 NO 24 de la Carta de 1980.

DERECHOS CONSTITUCIONALES CONCULCADOS

De los hechos expuestos y consideraciones de derecho precedentes se desprende con claridad meridiana que la información ya señalada, que respecto de mi persona y de mi hija publica la Corporación Administrativa del Poder Judicial en la base de datos del sitio en internet ya individualizado, Y de acuerdo al mérito de lo expuesto y lo previsto en el artículo 19 Nºs 1º, 2º y 4º y art. 20 de la Constitución Política de la República de

1980; el Auto acordado de la Excma. Corte Suprema de 24 de junio de 1992; y, demás normas legales citadas,

RUEGO A V.S.I.: tener por interpuesto recurso de protección en contra de la **CORPORACIÓN ADMINISTRATIVA DEL PODER JUDICIAL, ...** a fin que restableciéndose el imperio de¡ Derecho, se ordene a la recurrida eliminar los datos sensibles y expresiones discriminatorias referidos en el cuerpo de este escrito, que mantiene en el banco o base de datos de¡ sitio en internet individualizado en lo principal, por constituir una actuación ¡legal y arbitraria que causa privación, perturbación y amenaza en el legítimo ejercicio de mi derecho a la privacidad y honra de mi persona y de mi familia y un acto de discriminación arbitraria contra mi hija que le causa privación, perturbación o amenaza en el legítimo ejercicio de su derecho de igualdad ante la ley, todo cual, finalmente, amenaza y perturba mi integridad psíquica, moral y emocional, con costas.

PRIMER OTROSI: RUEGO A V.S.I. tener por acompañados los siguientes documentos-. Dos copias impresas (cuatro páginas cada una) de los resultados obtenidos en la dirección internet: www.poderjudicial.cl, efectuadas con las claves de búsqueda: *nombre y Rut* de la recurrente, debidamente autorizadas y certificadas ante notario público de esta ciudad.

Frente a este escrito la Corte de Apelaciones rechazó el recurso de protección presentado.

2º) **ESCRITO DE APELACION ANTE RECHAZO AL RECURSO DE APELACION.**

SECRETARÍA : ESPECIAL

TIPO DE RECURSO: : PROTECCIÓN

No DE INGRESO :1211-2001

EN LO PRINCIPAL : APELA; EN EL PRIMER OTROSI: ACOMPAÑA

DOCUMENTOS; EN EL SEGUNDO: SOLICITA ALEGATO.-

ILTMA. CORTE DE APELACIONES DE SANTIAGO

HUMBERTO CARRASCO BLANC, abogado, por la recurrente, doña NN, en los autos sobre Acción de Protección, **Rol Nº 1211-2001**, caratulados "NN c/ **CORPORACIÓN ADMINISTRATIVA DEL PODER JUDICIAL**", a S. S., Ilma., respetuosamente, digo:

Que, estando dentro del plazo que me confiere la ley y de conformidad a lo dispuesto en el Auto Acordado de la Excma. Corte Suprema de 27 de junio de 1992 y artículos 186 y siguientes del Código de Procedimiento Civil, vengo en apelar de la sentencia definitiva pronunciada por la Primera Sala de esta Ilustrísimo Corte, notificada a esta parte con fecha 01 de junio de 2001, solicitando desde ya se acoja a tramitación, se ordene elevar los autos para ante la Excelentísima Corte Suprema, a fin que dicho Excmo. Tribunal, conociendo del recurso, se sirva revocar en todas sus partes la sentencia apelada y en su lugar, declare que se acoge la acción de protección interpuesta, con costas, en atención a las consideraciones de hecho y de derecho que paso a exponer;

I

-

Breve relación de los hechos que motivan la acción de protección interpuesta, y hechos ocurridos durante su tramitación en primera instancia

- Ø El primero de marzo de 2001 la Corporación Administrativa del Poder Judicial ha inaugurado el Sitio Internet de dicho Poder del Estado, en tal Sitio Web mantiene una base o registro de datos de libre acceso público en la cual se informa el estado de causas judiciales de Santiago; con respecto a los juicios de filiación éstos se informan dando a conocer públicamente y sin restricción alguna las identidades de las personas involucradas; se publica concretamente el nombre completo y el número de cédula de identidad de quien actualmente es

padre o madre de hijos no reconocidos por el otro de los padres, y cuya filiación se está reclamando, así como la identidad completa de la persona actualmente demandada por ser el presunto padre o madre de otra persona.

- Ø Asimismo, los juicios de esta naturaleza hasta el 27 de marzo último, o sea, a más de un año de entrada en vigencia la Ley que puso término a la discriminación legal de los hijos -precisamente por ser inconstitucional-, según consta de los documentos acompañados por la propia Corporación recurrida, se informaron en la Página Web identificando la materia con la glosa "hijo legítimo acción". fecha en que la Corporación reconociendo tácitamente su error, al ser éste manifiesto y evidente, procedió a rectificar la información en este sentido.

Sin embargo, el hecho que la recurrida haya subsanado, en alguna medida, la conducta que motiva la protección -reemplazando la expresión "hijo legítimo acción" por "'acción Ley 19.585"- si bien pone término a la conducta que conculcó la garantía constitucional de igualdad ante la ley y no discriminación arbitraria, no obsta, por una parte, a que deba dictarse fallo sobre el punto, pues el hecho ocurrió y es menester un pronunciamiento a fin de evitar futuros "errores" y determinar eventuales responsabilidades; tampoco evita, por la otra, que se mantenga la situación de arbitrariedad e ilegalidad con respecto a la publicación de la identidad (nombre completo y NI' de RUT) de las partes en los juicios de filiación, con infracción a la prohibición de dar tratamiento en registros de libre acceso público a los denominados datos sensibles, y con violación, además, del carácter secreto que tienen los juicios de filiación, al menos hasta que se dicte sentencia de término en el proceso respectivo, vulnerando en ello, entre otras, la garantía constitucional de respeto y protección a la vida privada y honra de ¡a persona y de su familia.

En breves palabras, estos son los hechos que afectaron y siguen afectando los intereses de mí representada y que conculcan sus derechos constitucionales, según se expondrá más adelante.

- Ø Por otra parte, la Primera Sala de la Ilma. Corte de Santiago, declaró admisible el recurso de protección, y acogiéndolo a tramitación, se recibieron los alegatos de esta parte, para Posteriormente decretar como medida para mejor

resolver la Inspección personal del Tribunal del sitio web www.poderjudicial.cl, a fin de constatar la Ilma. Corte la información que sobre los juicios de filiación, interpuestos bajo la vigencia de la Ley 19.585, se da a conocer en la base de datos de dicho sitio web.

- Ø Mediante la medida decretada, sin embargo, según consta del acta de Inspección, el tribunal de primera instancia no pudo constatar que efectivamente en el sitio web referido se da a conocer las identidades (nombre y RUT) de las partes en los juicios de filiación. En efecto, no comprobó cómo en el juicio de filiación que mantiene actualmente la recurrente doña NN -causa rol 1844 -2000 del 19º Juzgado Civil de Santiago- así como en todos los juicios de filiación pendientes bajo la vigencia de la Ley **Nº** 19.585, se dan a conocer públicamente en el Sitio Web aludido las identidades de las partes, a pesar que dicha circunstancia puede ser constatada utilizando alguno de estos tres parámetros de búsqueda: el Rut de la persona; su nombre; o bien, el rol de la causa y el número del tribunal.

- Ø Al ingresar alguno de estos parámetros en el sistema de búsquedas que aparece en la página principal del sitio web, esto es, búsqueda por nombre, búsqueda por RUN, o búsqueda por rol en "Causas Civiles", por ejemplo, aparecerá una página con los últimos movimientos de la misma, al hacer clic al costado izquierdo del cuaderno principal se muestra una nueva página que contiene la identidad completa de las partes del juicio, tal y como se grafica a continuación en una secuencia de búsqueda efectuada con el nombre de la persona:

La **página 1 es** la página de inicio, la que se muestra al ingresar al sitio web www.poderjudicial.cl al hacer **clic** donde aparece la palabra **acceso** aparece una segunda página.

La **página 2,** en ella al costado izquierdo están las opciones de "búsqueda por nombre" "búsqueda por RUN" y "Causas Civiles" donde se efectúa la búsqueda por el Rol de la causa, en el ejemplo, al hacer **clic** en **"búsqueda por nombre"** aparece la tercera página.

La **página 3,** que aparece al hacer clic en la opción búsqueda por nombre, siguiendo el ejemplo, permite ingresar el nombre **de** la persona, **ingresado el nombre** se hace **clic** en la casilla **buscar** y aparece una cuarta página.
La **página 4,** muestra los resultados de la búsqueda, identificando la causa, al hacer **clic en el caratulado de la causa** aparece una quinta página.
La **página 5,** muestra los movimientos de la causa, y además, muestra los cuadernos de la misma, en el ejemplo, al hacer **clic** en la **fecha** que está al **costado izquierdo de donde dice "cuaderno principal"** se pasa a una sexta página.
La **página 6** da a conocer la identidad completa de las partes.

En un otrosí de esta apelación, se acompañan los ejemplares impresos de las búsquedas efectuadas en el sitio web referido utilizando el nombre de la recurrente, su RUT, y el rol de la causa judicial sobre filiación que actualmente mantiene. Utilizando estos tres parámetros de búsqueda el resultado es el mismo; la individualización completa de las partes del juicio, es decir del presunto padre y de ¡a madre que reclama judicialmente la filiación de su hija.

EN **SÍNTESIS:** A través de este sistema de búsqueda se puede averiguar por terceros no interesados que mi representada es demandante en un juicio de filiación. Este conjunto de datos, constituyen datos sensibles que deben ser protegidos por la Corporación Administrativa del Poder Judicial. El hecho que la recurrida haya cambiado la glosa "hijo legítimo acción" por "acción ley 19.585" no cambia el carácter de sensible de estos datos. Al ser datos sensibles, no pueden ser objeto de tratamiento a menos que la ley lo autorice, exista consentimiento de mi representada o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

Queremos en apoyo de nuestra tesis citar un párrafo expuesto por el autor GOMEZ LOECHES en artículo titulado **"La Confidencialidad de los Datos Contenidos en los Ficheros Jurisdiccionales"'** tratando la incidencia de la normativa sobre protección de datos en la utilización por los Juzgados y Tribunales españoles de medios electrónicos, informáticos y telemáticos. Expone este autor que "Los datos personales obrantes en estos ficheros (judiciales) tienen, en la mayoría de los casos, la consideración de datos sensibles. Es una realidad indiscutible que los meros datos nominativos o de mera

identificación, que en **sí** mismos no poseen entidad suficiente para ser considerados incluidos en aquellas categorías de datos que merecen especial protección, por el mero hecho de constar en un proceso judicial, permiten asociar o dar noticia de la implicación de una persona determinada con un concreto proceso. Tal información adquiere, en el caso de que esa información resulte accesible a terceros o trascienda fuera del ámbito propio del proceso, inmediatamente una connotación prima facie potencialmente negativa para su titular (o mejor, para su imagen, fama, o estima o consideración social)". (GÓMEZ LOECHES, LUIS, "La Confidencialidad de los Datos contenidos en ficheros jurisdiccionales", en Revista Informática y Derecho 30,31 y 32, Editorial UNED, año 2000, Pág. 333).

II

Consideraciones previas de derecho

La **Ley NO 19.628,** publicada en el Diario Oficial de 28 de agosto de 1999, **Sobre Protección de la Vida Privada,** regula **el** tratamiento de datos personales en registros o bancos de datos estableciendo el marco jurídico al que debe sujetarse toda persona natural o jurídica privada u organismo público a cargo de dichos registros, prescribiendo limitaciones, prohibiciones, responsabilidades y sanciones a fin de cautelar debidamente la efectiva protección de la vida privada y honra de la persona y de su familia. Se entiende por tratamiento de datos, de acuerdo a ¡a definición que da la letra o) del artículo **20** de esta ley "cualquier operación o complejo de operaciones o procedimientos técnicos. de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar. interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma." Y se entiende por datos de carácter personal o datos personales "los relativos a cualquier información concerniente a personas naturales identificadas o identificables." (art. 20 letra f).

Asimismo, el artículo **211** letra **g)** de la ley en comento define lo que debe entenderse por *datos sensibles:*

"DATOS SENSIBLES, SON AQUELLOS DATOS PERSONALES QUE **SE REFIEREN** A LAS CARACTERÍSTICAS FÍSICAS 0 MORALES DE LAS

PERSONAS 0 A **HECHOS 0 CIRCUNSTANCIAS DE SU VIDA PRIVADA 0 INTIMIDAD,** TALES COMO LOS HÁBITOS PERSONALES, EL ORIGEN RACIAL, LAS IDEOLOGÍAS Y OPINIONES POLÍT]CAS, LAS CREENCIAS 0 CONVICCIONES RELIGIOSAS, LOS ESTADOS DE SALUD FÍS]COS 0 PSÍQUICOS Y LA VIDA SEXUAL."

Por otra parte, la **Ley NO 19.585,** publicada en el Diario Oficial de 26 de octubre de 1998. en vigencia desde el 27 de octubre de 1999. y que modificó el Código Civil y otros cuerpos legales en materia de filiación y derechos hereditarios, estableciendo rigurosos requisitos y mecanismos en resguardo de la intimidad y honra de los involucrados en un juic7lo de filiación, dispone, entre otras medidas, el carácter secreto del proceso. En efecto, el inciso primero de Art. 197 del Código **Civil,** inserto dentro del Libro 1, Título VIII, "De **las** Acciones de Filiación", señala expresamente

"El proceso tendrá carácter SECRETO hasta que se dicte sentencia de término, y sólo tendrán acceso a él las partes y sus apoderados judiciales."

III

Acto arbitrario e ilegal y derechos constitucionales conculcados

Los hechos que motivan la acción de protección conculcan los siguientes derechos fundamentales que la Constitución Política reconoce. Artículo 19. La Constitución asegura a todas las personas:

Artículo 19 Nº 4º: "...El respeto y protección a la vida privada y pública y a la honra de a persona y de su familia ...' Resulta conculcado este derecho, al publicarse en la base de datos que mantiene en Internet la recurrida Corporación, las identidades (nombres, apellidos y Rut) de las partes involucradas en el juicio de filiación que sostiene la recurrente por la paternidad de su hija; y, asimismo, por el hecho de que cualquier persona pueda enterarse vía internet acerca de la naturaleza de la filiación actual de su hija, así como que tal persona está demanda por ser el presunto padre.

El hecho de publicar en dicho sitio web la información que respecto de la recurrente maneja la Corporación, y que como se verá, son datos sensibles, no sólo es un acto ¡legal en cuanto infringe la prohibición expresa del artículo 10 de la Ley 19.628 y el

artículo 197 del Código Civil, sino ante todo porque atenta contra la "Ley Fundamental de la República", esto es, la Carta Constitucional de 1980. Tal acto, es también arbitrario, puesto que el acceso a los datos sensibles en Internet no puede permitirse por criterios como el nombre o el Rut. sino por el Rol, ya que dicho dato será conocido únicamente por las partes y sus apoderados judiciales. Este sería el procedimiento ajustado a derecho conforme al cual debieran informarse en internet los juicios de filiación y otros de naturaleza semejante como son, por ejemplo, los juicios sobre violencia intrafamiliar. Tal procedimiento es absolutamente posible desde el punto de vista técnico, prueba de ello es que la recurrida da este tratamiento a los juicios sobre violencia intrafamiliar, pero no a todos -, pues no existe un criterio único ni siquiera para tratar la información relativa a causas de la misma naturaleza. La causa sobre violencia intrafamiliar Rol F-230-2001, del Sexto Juzgado Civil de Santiago, por ejemplo, según consta de las copias acompañadas en autos, se informa en el Sitio Web en cuestión sin dar a conocer las identidades de ¡as partes, ni siquiera en el caratulado del proceso, únicamente se identifica la causa por su número de Rol y Tribunal. Es decir, la Corporación recurrida tiene los medios técnicos para dar la debida protección y reserva que los juicios de esta índole exigen.

Artículo 19 Nº 2º: "La igualdad ante la ley... Ni la ley ni autoridad alguna podrán establecer diferencias arbitrarias." Conculca este derecho fundamental, básicamente. el hecho de que se haya utilizado, a pesar de haber sido suprimidas por la ley 19.585. expresiones profundamente discriminatorias y estigmatizantes como lo son las de "hijo legítimo e legítimo", como en e caso de autos respecto de la hija de mi representada, y con la agravante de que dichos términos son utilizados en un banco de datos al que cualquiera persona tiene libre acceso desde la Internet.

Artículo 19 Nº 1º: "...El derecho a la vida y a la integridad física y psíquica de la persona..." En efecto, los hechos recurridos constituyen privación, perturbación o amenaza, a la integridad psíquica de la recurrente, desde que al lesionar la honra y privacidad de su persona y de su familia provocan gran menoscabo en su integridad emocional y moral dañando profundamente su dignidad humana, imagen, fama, estima o consideración social.

Artículo 19 Nº 24º: ... "El **derecho de propiedad en sus diversas** especies sobre toda clase de bienes corporales o incorporales." Finalmente, los derechos señalados precedentemente constituyen bienes incorporases que como tales han ingresado al

patrimonio jurídico de mi representada y que quedan, en consecuencia. amparados por la garantía constitucional del derecho de propiedad.

IV

-

Carácter permanente del acto arbitrario e ilegal

El carácter permanente del acto arbitrario e ¡legal que se reclama se desprende del hecho de que actualmente los datos sensibles que afectan a mi representada continúan en la base de datos del sitio web de la recurrida Corporación.

V

Datos sensibles: hechos y circunstancias de la vida privada o intimidad:
Ley Nº 19.628 sobre Protección de la Vida Privada

La Ley sobre Protección de la Vida Privada es categórica al prohibir en su artículo 10º todo tratamiento de datos sensibles, señalando que ello no podrá efectuarse *salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.'* 'El tratamiento de datos personales por parte de un organismo público sólo puede efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes." (art.20) Es decir, garantizando la debida protección a los derechos y garantías constitucionales de sus titulares. Y si se trata de *datos sensibles,* como en el caso de autos, rige igualmente la prohibición que establece el artículo 10º trascrito precedentemente. Esto es, que tales datos no pueden ser objeto de tratamiento salvo si una ley lo autoriza expresamente. existe consentimiento del titular de los datos o su procesamiento sea necesario para determinar u otorgar beneficios de salud a sus titulares. En la especie, no existe ley que autorice a divulgar mediante un banco de datos en internet *datos sensibles* tales como la naturaleza de la filiación de las personas o el hecho de sí determinada persona es madre o padre de hijos no reconocidos, o bien, que está actualmente demandada por ser el presunto padre o madre de otra persona.

Los hechos que han motivado esta protección se enmarcan dentro de lo que el artículo 2º letra g) de la misma ley define como datos sensibles. respecto, es del caso señalar que los datos personales son de tres clases: datos personales propiamente tales (cualquier información concerniente a personas naturales, identificadas o identificabas), datos de mera identificación (nombres, dirección, cédula de identidad, por ejemplo, que suelen figurar en las fuentes accesibles al público), y los datos sensibles (sobre aspectos de la personalidad cuya vulneración daña con mayor profundidad la dignidad humana y, normalmente, atentando también contra derechos fundamentales distintos a la intimidad, como la vida (integridad psíquica), o la igualdad.

En el caso de autos, se atenta contra estos derechos constitucionales no porque se haya publicado datos de mera identificación, como son el nombre y la cédula de identidad, sino porque dichos datos se publican con relación a *hechos o circunstancias de la vida privada o intimidad* (tener una persona determinada un hijo no reconocido por su padre o madre, o estar actualmente demandada por ser el presunto padre o madre de otra determinada persona). Es decir, aquí los datos de mera identificación se tornan sensibles al estar publicados o informados en relación a hechos o circunstancias de la vida privada o intimidad. Nótese que el concepto de dato sensible es tremendamente abierto, la expresión "*hechos o circunstancias de su vida privada o intimidad, tales como...",* junto con ser imprecisa, es ejemplar. Por eso, los datos sobre filiación, sobre todo cuando estén en proceso de reconocimiento judicial. son sensibles y requieren cumplir mayores exigencias para su tratamiento (esa es la justificación del 10º de la Ley 19.628).

Queda comprendido entonces, dentro de lo que debemos entender por *datos sensibles*, la vida privada e intimidad de las personas. El Derecho a la intimidad, protege precisamente un ámbito de autonomía constituido por los sentimientos, hábitos y costumbres, las relaciones filiales es, familiares, las creencias religiosas, la salud física y mental, en otros aspectos o facetas de la vida humana. En suma, estar o no reconocida una persona por su padre o madre, o ser madre o padre de un hijo no reconocido por su padre o madre, o bien, estar actualmente demandado por el ser presunto padre o madre de otra persona, es indudablemente, uno de los aspectos que atañen directamente la intimidad de las personas, su vida privada, una de las esferas más íntimas y sensibles de la persona y de su familia, que como bien dice don Hernán Álvarez García, entre otros Excmos. Ministros "... *El respeta a la vida privada, a la Dignidad y a la honra de la persona humana y de la familia constituyen valores de tal jerarquía y trascendencia*

que la sociedad política se organiza precisamente para preservarlos y defenderlos, de modo que no puede admitirse concepción alguna de/ bien común que permita el sacrificio de ellos, ni convertir tal sacrificio en medio para que prevalezca otra garantía constitucional" (en Revista Fallos Del Mes, Nº 415, Junio, 1993, página 347, Rol 21.053-93, Excma. Corte Suprema).

Concordando con lo dicho por el Presidente de la Excma. Corte, entonces ¿Será legal o razonable, publicar en la Internet, "tierra de nadie y de todos a la vez", algo tan delicado para una madre o un padre, como lo es la naturaleza filial de su hijo, especialmente si éste no ha sido reconocido por uno de sus padres? ¿O sin que se haya dictado sentencia de termino, estigmatizar a un hombre como alguien que no responde de sus conductas, pues asta que no se establezca lo contrario, el demandado es sólo presunto padre?

No debemos olvidar que la intimidad es un derecho que se incorpora en la Declaración Universal de los Derechos Humanos de 1948. como una de las garantías fundamentales del ser humano, derecho que es inherente al desenvolvimiento y realización del humano como tal. Mismo derecho que también el artículo 11 inciso 2º del Pacto de San José de Costa Rica consagra en términos tales "Que nadie puede ser objeto de ingerencias, arbitrariedad o abusos a su vida privada o en la de su familia." Instrumentos internacionales de Derechos Humanos suscritos y ratificados por Chile, que se encuentran actualmente vigentes y que de acuerdo al inciso 2º del artículo 5º de la Carta de 1980, se incorporan a nuestro ordenamiento jurídico con rango constitucional, o de menor jerarquía normativa según parte de la doctrina y la jurisprudencia, pero en todo caso como ley de la República que viene a reiterar y complementar la garantía constitucional de respeto y protección a la vida privada y pública y a la honra de la persona y de su familia, consagrada en el número 41 del artículo 19 de la Constitución, a la cual deben someter su acción los órganos del Estado, los titulares o integrantes de dichos órganos así como toda persona. institución o grupo.

VI

Publicidad de los actos de los tribunales y carácter secreto de los juicios de filiación en el nuevo estatuto de la Ley NO 19.585

Por otra parte, es preciso también detenemos en el único precepto legal que la recurrida cita para fundamentar su actuación, el artículo 9,1 del Código Orgánico de Tribunales,

ello dice relación directamente con el carácter secreto de los juicios de filiación. En efecto, de acuerdo al inciso 1º del artículo 197 del Código Civil, modificado por la Ley Nº 19.585- "El *proceso tendrá carácter de secreto hasta que se dicte sentencia de término, y sólo tendrán acceso a él las partes y sus apoderados judiciales."*

El carácter secreto que la norma del artículo 197 del Código Civil da a los juicios de filiación, no estaba contemplado en el proyecto de ley del Ejecutivo, sino que fue fruto del trabajo legislativo en el Congreso Nacional., especialmente en el Senado. El alcance de este carácter es amplio, abarcando el secreto incluso el hecho mismo de la demanda. Al respecto, permítasenos citar lo siguiente, con relación a una indicación propuesta por un grupo de Senadores:

"La indicación Nº 72, en el inciso que propone, señala que, si se reclama la paternidad o maternidad no matrimonial respecto de una persona casada, el proceso tendrá carácter de reservado y sólo tendrán acceso a éste las partes y sus apoderados judiciales. Castiga *con pena privativa de libertad y multa la* divulgación del hecho de la demanda y de sus *antecedentes.*
La Comisión estimó declarar que, en general, los procesos sobre filiación tendrán carácter secreto, y Limitar su conocimiento a las partes y sus apoderados judiciales. Prefirió hablar de "secreto" y no de "reserva" para hacer aplicables inequívocamente las disposiciones penales que sancionan la vulneración de secretos, contempladas en los artículos 246 y 247 del Código Penal. Por el mismo motivo, suprimió las penas que proponía la *indicación."* (Informe 1060-07. Comisión Constitución. Legislación Justicia y Reglamento el Senado, sesión 12ª, página 1821)

Como puede observarse la historia fidedigna del establecimiento de la norma que consagra el carácter secreto de os juicios de filiación es clara y categórica.

Pues bien, atendida la naturaleza especialísima de los asuntos que se ventilan en los juicios de filiación, el legislador estableció precisamente en la norma citada una excepción a la regla general de publicidad. El a 91 del Código Orgánico de Tribunales dispone que- *"Los actos de los tribunales son públicos, salvo las excepciones expresamente establecidas en la ley".* Esta es una de ellas.

Pero, ¿qué debemos entender por “secreto”?. Sin perjuicio de lo ya dicho al respecto, diremos que existen tres interpretaciones- a) Desde luego, el carácter secreto del proceso está referido, , primeramente., al acceso material del expediente, por lo que las causas de esta índole se tramitan permaneciendo físicamente el expediente en custodia del tribunal, y a ellas sólo tienen acceso las partes, es decir, la persona del demandante y del demandado, y sus respectivos abogados patrocinantes y apoderados; b) en segundo lugar, el carácter secreto de los juicios de filiación alcanza también al contenido mismo del proceso. 0 sea, además de impedirse el acceso materia¡ al expediente a quien no sea parte ni patrocinante o apoderado en la causa, no se debe proporcionar información acerca del contenido del expediente a terceros ajenos a la causa, ese es precisamente el objeto de que al proceso sólo tengan acceso las partes, permaneciendo al efecto en la custodia del tribunal; y, c) en tercer lugar, el carácter secreto de los juicios de filiación, además de referirse al acceso material del expediente y a su contenido, comprende también el deber de mantener en reserva las identidades del presunto padre o madre que ha sido demandado, así como la del padre o madre que reclama la filiación de su hijo. Secreto Que respecto de la persona del presunto Padre o madre cautela la honra del demandado, ya que en definitiva puede resultar no ser el padre o madre del hijo que se pretende. También debe mantenerse en secreto la identidad del demandante, porque el hecho de que determinada persona sea madre o padre de un hijo no reconocido por su otro padre. es una circunstancia que debe quedar comprendida en la esfera de intimidad de la persona, y como tal constituye dato sensible.

Obviamente la causa tendrá que individualizarse con su respectivo número de proceso y tribunal, pero fuera de ello no puede un tercero ajeno a la causa enterarse de quién es la persona del demandado o quién es la persona del demandante, conociendo sus identidades y Rut. Ello haría ilusorio el carácter secreto del proceso y constituiría una privación, perturbación o amenaza al legítimo ejercicio del derecho de respeto y protección a la vida privada y pública y a la honra de ¡a persona y de su familia.

Con relación a estas tres interpretaciones en tomo a lo que debe entenderse por carácter "secreto" de los juicios de filiación, la que debe prevalecer es aquella interpretación que se encuentre más acorde a la Constitución Política y a la historia fidedigna del establecimiento de la ley. Esta es sin duda aquella que garantiza en mayor medida o de mejor manera los derechos fundamentales, en el caso de a tos, la privacidad y la honra de la persona y de su familia.

VII

La sentencia que se apela

El sentenciador en el considerando 5º expresa "Que de este modo cabe concluir que la información que suministra el sitio WEB del poder judicial respecto de procesos iniciados de conformidad con las normas de la ley 19.585 está limitada única y exclusivamente a la que es posible obtener por cualquier persona, de los libros de ingreso de causas de los Juzgados correspondientes, cuyos datos son de público conocimiento".

En primer término, existe una imprecisión en esta afirmación, ya que no es posible obtener de los libros de ingreso el RUN de las partes, a lo más el nombre completo, pero nunca su RUT..

Además no es lo mismo acudir a un tribunal a solicitar los libros de ingreso para tener conocimiento sobre el nombre de las partes y del rol. que poder averiguarlos a través de medios automatizados, en este caso, a través de Internet.

Es probable que un libro de ingreso pueda ser consultado por 30 0 50 personas al día, respecto de distintas causas. En cambio, cuando se trata de datos que se encuentran automatizados se facilita su consulta haciendo posible que miles de usuarios accedan a esta información desde cualquier punto y simultáneamente.

En este sentido expresa el autor DAVARA RODRÍGUEZ que "En primer lugar se trata de proteger a las personas ante el manejo o manipulación, no autorizada, de sus datos personales, pero siempre que estas datos sean susceptibles de tratamiento automatizado o se encuentren en un soporte susceptible de tratamiento automatizado. Es una protección jurídica ante la potencial agresividad de la informática..... Es en el carácter y la calidad de informatización - o posible informatización- y en las características y consecuencias del tratamiento informática de datos, donde nace esta necesidad de protección.

Luego, para el estudio del tema hay que tener en cuenta, como primordial, el efecto que sobre los datos -y las consecuencias para la persona titular de los datos- puede tener el tratamiento informática".

(DAVARA RODRÍGUEZ, MIGUEL ANGEL, "Manual de Derecho Informático", Editorial Aranzadi, España, 1997, pág. 47.).

Con lo anterior se demuestra que no es efectivo lo afirmado en el considerando y a su vez, que no es lo mismo obtener los datos de un libro de ingreso que a través de un sistema automatizado de datos de libre y masivo acceso público.

Por otra parte, tampoco es efectivo lo afirmado en el considerando 40 de la sentencia apelada, puesto que el Tribunal de primera instancia jamás constató mediante la inspección personal al sitio web en cuestión, el que efectivamente la recurrida al infomar en él las causas de filiación da a conocer las identidades de las partes (nombre completo y RUT).

Finalmente. atendido todo lo expuesto precedentemente, tampoco es efectivo lo afirmado en el motivo 60 del falto apelado, en cuanto a que:

"... no resulta comprobado que la autoridad recurrida, haya trasgredido, o está trasgrediendo el carácter secreto que reviste un proceso de filiación..." ni que se "...advierte que mediante dicho sitio de Internet, se hayan proporcionado, o se estén proporcionando datos sensibles relativos a la vida privada de la recurrente..."

El acto arbitrario e ilegal que conculca las garantías constitucionales de la recurrente -ya referidas-, es claro y evidente.

VIII

Posibles consecuencias en caso de ser rechazado el recurso

Las consecuencias del rechazo de este recurso son de trascendental importancia. En efecto, de no acogerse la acción de protección podríamos encontramos en la situación de creación de un nuevo negocio para aquellas empresas que se dedican a la recolección y venta de informes o datos de las personas. En efecto, si se estima que los datos que dan a conocer que una persona es madre o padre de un hijo no reconocido y cuya filiación está reclamando judicialmente o que se encuentra demandada por ser el presunto padre o madre de otra persona son nominativos y no sensibles,, estaríamos en presencia de una fuente de datos accesibles al público (artículo 2º letra I) de la ley 19.628), cuyo tratamiento para fines distintos para los cuales fue recolectada no requiere de autorización alguna (artículo 9º de la ley citada en relación al artículo 4"). Con ello, las entidades como DICOM u otras similares podrían vender la situación judicial de las personas (utilizando como fuente el sitio web del poder judicial) y en esta información podría aparecer que tienen en tramitación un juicio de filiación.

A su vez, muchos empleadores pueden consultar directamente el sitio Web del Poder Judicial y ver si el postulante al trabajo o el trabajador tienen actualmente algún juicio de Maternidad o maternidad y en virtud de esta información tomar decisiones que pueden perjudicar a estas personas o discriminarías, pues se estaría creando y dando a conocer un perfil de éstas. En conclusión: Con este fallo se estaría legalizando el tratamiento de datos personales que den a conocer si una persona tiene un juicio de filiación o de violencia intrafamiliar cuya sensibilidad aparece claramente, y en los cuales el derecho a ¡a intimidad. honra y dignidad de la persona humana y de su familia reclaman mayor protección.

En un fallo de la Excma. Corte Suprema, ya citado. , puede leerse: *"La procedencia de la protección ante la sola amenaza, se afirma al considerar que los valores en cuestión son por su naturaleza de tal índole,. que el solo inicio de su vulneración genera daños imposibles de reparar en términos equivalentes al bien que significa su respeto para quién los posee y requiere conservarlos íntegros e inviolables.'(en* Revista Fallos De¡ Mes, NI, 415, Junio, 1993, página 347, Rol 21.053-93, Excma. Corte Suprema).

SOLUCIÓN:

Nada más y nada menos que acoger el recurso ordenando se bloquee la búsqueda por el nombre o por el RUN en ¡a causa de mi representada (y sería recomendable en todas aquellas causas que digan relación con la "acción ley 19.585" o juicios de violencia intrafamiliar) y sólo se permita aquella por el ROL (ya que se presume que sólo las partes y los abogados o apoderados de ellas tienen cono miento de la misma).

POR TANTO,

SIRVASE S.S., ILTMA., de conformidad a lo previsto en el Auto Acordado de la Excma. Corte Suprema de 27 de junio de 1992, sobre Tramitación del Recurso de Protección de Garantías Constitucionales, y lo dispuesto en los artículos 186 y siguientes del Código de Procedimiento Civil, tener por interpuesto recurso de apelación en contra de la sentencia de primera instancia que rola a fs. treinta y tres y siguientes de autos, concederla para ante la Excma. Corte Suprema, a fin de que ese Excmo. Tribunal, en definitiva, revoque la resolución que declaró sin lugar la acción de protección interpuesta por esta parte y, en su lugar., acoja el presente recurso para la protección de los derechos constitucionales antes expuestos, en contra de la Corporación

Administrativa del Poder Judicial, y restableciéndose el imperio del Derecho se ordene a la recurrida:

Eliminar los datos sensibles referidos en el cuerpo de este escrito, que mantiene en su banco o base de datos del sitio web en internet.

Que se declare que no obstante que la recurrida, y a raíz del presente recurso, reemplazó las expresiones "hijo legítimo acción" por "acción ley 19.585", el derecho de igualdad ante la ley y no discriminación arbitraria de mí representada, resultó efectivamente conculcado por la actuación arbitraria e ilegal de la recurrida Corporación Administrativa, y

Pagar las costas del recurso.-

PRIMER OTROSI: Sírvase S.S., Excma., tener por acompaños, con c7itación. los siguientes documentos-.

1.- Fotocopias simple de cuatro páginas del Informe 1060-07 de la Comisión, Constitución, Legislación, Justicia y Reglamento del Senado, (páginas 1890, 1821, 1527 y 1528), de las que se desprende la historia fidedigna del

establecimiento de la norma del artículo 197 del Código Civil relativa al carácter de secreto de los juicios de filiación. 2.- Copia impresa de la página web (una hoja), autorizada ante notario público de esta ciudad, en la cual constan los datos sensibles referidos en lo principal..

3.- Tres ejemplares impresos (20 hojas) de las búsquedas efectuadas en el sitio web que mantiene la recurrida, con el nombre de la recurrente, su RUT, y el Rol y Tribunal de la causa e filiación que tramita actualmente. 4.- Extracto del fallo de la Excma. Corte Suprema recaído en los autos de Protección Rol 21.053 de 1993, (en Revista Fallos Del mes, NI, 415, 1993, página 347).

SEGUNDO OTROSI: Atendido lo dispuesto en el Auto Acordado de la Excma. Corte Suprema, de fecha 27 de junio de 1992, y el carácter complejo, especialísimo y novísimo de la materia, ruego a S.S., Excma., ordenar traer los autos en relación a fin que esta parte pueda rendir sus alegatos.

- Frente a esta solicitud, la Corte resolvió:

Santiago, 3 de julio de 2001
No a lugar a alegatos.
VISTOS:
SE CONFIRMA sentencia apelada de primero de junio recién pasado que se lee a fojas 33 .
Regístrese y devuélvase
Nº 2299-2001

5) Dictámen Ord. Nº 260/19 de la Dirección del Trabajo.

De acuerdo a las facultades con que cuenta el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, pero en ningún caso podrá tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores.

ORD. Nº 260/19

MATE: Empresa. Facultades de administración. Acceso correspondencia electrónica. Procedencia.

RDIC: De acuerdo a las facultades con que cuenta el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, pero en ningún caso podrá tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores.

ANT.: Presentación del señor Gianpaolo Peirano, de 21.02.2001.

FUENTES:
Constitución Política, artículo 19 Nºs. 5, 24 y 26.
Código del Trabajo, artículos 5º y 153 y 154.

SANTIAGO, 24.01.2002
DE : DIRECTORA DEL TRABAJO
A : SEÑOR GIANPAOLO PEIRANO

VITACURA Nº 2939, PISO 8º
L A S C O N D E S/

Se consulta a esta Dirección, si es lícito que la empleadora tenga acceso a la correspondencia electrónica de sus trabajadores, en el caso que el dependiente use bienes de propiedad de ésta.

Como se advierte, en la situación descrita aparecen en conflicto dos valores, los que a su vez el ordenamiento jurídico ampara mediante dos garantías constitucionales distintas, debiendo resolverse, en consecuencia, la forma en que deben compatibilizarse ambas y en que condiciones prima una sobre la otra. Por una parte, la garantía constitucional de inviolabilidad de toda forma de comunicación privada, y por la otra, la facultad del empleador de organizar, dirigir y administrar su empresa, que emana de la garantía constitucional del derecho de propiedad, contempladas respectivamente, en el artículo 19 Nos 5 y 24 de la Constitución Política del Estado.

Asimismo, especial consideración deberá prestarse al actual inciso 1º del artículo 5º del Código del Trabajo, incorporado por el párrafo Nº 4 del artículo único de la ley Nº 19.759, que precisa:

"El ejercicio de las facultades que la ley le reconoce al empleador, tiene como límite el respeto a las garantías constitucionales de los trabajadores, en especial, cuando pudieran afectar la intimidad, la vida privada o la honra de éstos".

Ahora bien, la experiencia práctica que emana de los hechos y la costumbre, indican que en el ámbito de las relaciones de trabajo, lo habitual y frecuente es que el empleador no pretenda enterarse del contenido de las llamadas telefónicas de sus dependientes, aún cuando la línea y el aparato pertenezcan al empleador. Igual cosa sucede con cierto mobiliario y lugares de la empresa que usa el dependiente, tales como casilleros, escritorios y cajones, entre otros, en que lo corriente será que estos reductos sean una proyección natural de la persona y actividad del dependiente, y por tanto, habitualmente tampoco serán controlados ni invadidos por el empleador, aún cuando -se reitera- en estricto rigor sean de propiedad de éste. Con similar predicamento deben abordarse las situaciones a que dé lugar el uso del correo electrónico.

Lo anterior no es impedimento para que resulte aconsejable la regulación formal del uso de estos bienes de que es titular la empleadora, lo que naturalmente no puede ni debe significar limitar la garantía constitucional de inviolabilidad de la comunicación privada.

En efecto, como se sabe, es obligatorio para las empresas que ocupen diez o más trabajadores, "confeccionar un reglamento interno de orden, higiene y seguridad que contenga las obligaciones y prohibiciones a que deben sujetarse los trabajadores, en relación con sus labores, permanencia y vida en las dependencias de la respectiva empresa o establecimiento", conforme lo precisa el inciso 1º del actual artículo 153 del Código del Trabajo. Previa la entrada en vigencia de esta normativa, de oficio o a petición de parte, esta Dirección puede "exigir modificaciones al referido reglamento interno en razón de ilegalidad", según -ahora- el inciso final de la citada disposición legal.

Conforme a estas disposiciones legales, será entonces el empleador quién podrá tomar la iniciativa para formalizar esta normativa interna de la empresa y, en el ámbito de sus facultades de administración, podrá también incorporar preceptos a este reglamento con el fin específico de regular, limitar o restringir el empleo de los correos electrónicos por los dependientes, todo lo cual no obsta - como se ha dicho - que "El delegado del personal, cualquier trabajador, o las organizaciones sindicales de la empresa respectiva" (artículo 153 inciso 3º del Código del Trabajo), pueda impugnar de ilegalidad estas normas ante este Servicio. Se reitera, esta regulación podrá recaer en el uso del correo electrónico, no en la garantía constitucional de inviolabilidad de la comunicación privada.

Con todo, deberá tenerse presente que el artículo 154 del Código del Trabajo precisa una serie de disposiciones que, "a lo menos", debe contener este reglamento interno, y, entre ellas, la Nº 5, que precisa: "las obligaciones y prohibiciones a que estén sujetos los trabajadores". Pues bien, de regularse el uso del correo electrónico por el reglamento interno de la empresa, conforme al inciso final del referido artículo 154, "Las obligaciones y prohibiciones a que hace referencia el Nº 5 de este artículo, y, en general, toda medida de control, sólo podrán efectuarse por medios idóneos y concordantes con la naturaleza de la relación laboral y, en todo caso, su aplicación deberá ser general, garantizándose la impersonalidad de la medida, para respetar la dignidad del trabajador".

En empresas de menos de diez trabajadores, nada impide que esta regulación opere por la vía del contrato individual de trabajo o el instrumento colectivo, cuidando siempre de preservar la plena vigencia de la garantía constitucional involucrada, la que no podrá en ningún caso ni en ninguna medida ser materia de acuerdo entre las partes ni tampoco de regulación por el reglamento interno de la empresa.

Por ejemplo, podrá regularse radicalmente el uso del correo electrónico por alguna de las formas descritas precedentemente, en términos tales que todo envío del personal se efectúe con copia a alguna Gerencia o Unidad de la empresa, envío que de esta forma perderá - en el instante - su condición de comunicación privada, regulación que sin embargo no es practicable en el caso de la recepción de correspondencia electrónica, y por tanto, en este aspecto, esta modalidad de comunicación conserva siempre su carácter privada, como asimismo, permanecerá plenamente amparada por la referida y correspondiente garantía constitucional.

Asimismo, la doctrina comparada ha imaginado los costos de uso extraproductivos del correo electrónico, los que también podrían regularse por el reglamento interno de la empresa: "Siendo el titular de la empresa el pagador de los gastos inherentes al uso del correo electrónico, no se le puede, de entrada, exigir que vaya a su costa la utilización del mismo para fines personales del asalariado o no relacionado directamente con la propia producción o la prestación del servicio de que se trate: se trataría de un enriquecimiento injusto, cuando no, en determinados casos, de un abuso de derecho o una deslealtad contractual" (Miguel Angel Falguera i Baró, "Uso por el trabajador del correo electrónico de la empresa para fines extraproductivos y competencias de control del empleador", Revista Relaciones Laborales Nº 22, España, noviembre de 2000, página 24).

En síntesis, como se ha dicho, el empleador podrá regular las condiciones de uso de los correos electrónicos, cubriendo los casos y situaciones descritos precedentemente y otros, pero en ningún caso - ni por reglamento interno ni por acuerdo de las partes - podrá regularse el ejercicio mismo de la respectiva garantía constitucional.

Por lo demás, no podría ser de otra forma, si se tiene presente que aún las regulaciones legales de una garantía constitucional autorizadas por la propia Constitución, "no podrán afectar los derechos en su esencia, ni imponer condiciones, tributos o requisitos que impidan su libre ejercicio" (artículo 19 Nº 26 de la Constitución Política del Estado).

En consecuencia, sobre la base de las disposiciones constitucionales y legales precedentes, cúmpleme manifestar a Ud. que de acuerdo a las facultades con que cuenta el empleador para administrar su

empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, pero en ningún caso podrá tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores.

Saluda a Ud.,
MARIA ESTER FERES NAZARALA
ABOGADA
DIRECTORA DEL TRABAJO
RGR/emoa

6) Dictámen Ord. Nº 1147/34 de la Dirección del Trabajo.

ORD.: Nº 1147/34

MATE.: Empresa. Facultades de Administración. Acceso Correspondencia Electrónica. Procedencia.

RDIC.: Se niega reconsideración de dictamen Nº 260/019, del 24.01.2002, que estableció las facultades de que disponen los empleadores en materia de control de los correos electrónicos de sus trabajadores.

ANT.: 1.- Presentación del Sr. Ignacio Torrontegui, del 05.11.04.

2.- Pase Nº 54 del Jefe del Dpto. Jurídico, del 23.02.05.

SANTIAGO, 21.03.2005

DE : DIRECTOR DEL TRABAJO .

A : SR. IGNACIO TORRONTEGUI M. CATEDRAL 1009, OFICINA 2101, SANTIAGO.

Se ha solicitado a este Servicio, por presentación del Sr. Ignacio Torrontegui M., una rectificación del dictamen N 260/ 019, de fecha 24.01.2002, sobre la facultad del empleador respecto de las correspondencia enviada por los trabajadores a través de correos electrónicos provistos por la empresa.

Según señala la presentación, sería licito pactar entre las partes del contrato de trabajo que el correo electrónico solo puede ser utilizado para mantener comunicaciones concernientes a la actividad de la empresa, como también que la empresa revise dichos correos electrónicos, tanto los enviados como recibidos.

Al respecto cumplo con informar a Ud. lo siguiente:

El dictamen cuya reconsideración se solicita señala que "de acuerdo a las facultades con que cuenta el empleador para administrar su empresa, puede regular las condiciones, frecuencia y oportunidad de uso de los correos electrónicos de la empresa, pero en ningún caso podrá tener acceso a la correspondencia electrónica privada enviada y recibida por los trabajadores".

La razón de lo anterior corresponde a la naturaleza de comunicación privada protegida constitucionalmente que este Servicio le reconoce al correo electrónico de los trabajadores, según se expone en el cuerpo del dictamen recurrido.

Lo anterior, sin perjuicio, de que nada impide que el empleador en el reglamento interno o las partes en los respectivos contratos individuales de trabajo establezcan normas, restricciones y formalidades para el uso de los correos electrónicos.

Ahora, del análisis de su solicitud, no se aprecia ningún elemento de juicio que haga, precisamente, apartar a este Servicio de la consideración de que los mensajes electrónicos enviados o recibidos corresponden a correspondencia privada, y por lo tanto, protegidos por la inviolabilidad constitucional de la correspondencia (artículo 19 numero 5 de la Constitución Política del Estado), con limitaciones arriba señaladas.

En consecuencia, de la inviolabilidad citada se seguiría la imposibilidad de que la empresa revise el contenido de los correos electrónicos de sus trabajadores, tanto los enviado como los recibidos, sin perjuicio de la facultad empresarial de regular el acceso y el envío de dichos correos electrónicos, como establecer restricciones sobre el uso de los sistemas de soporte de dichos correo en la empresa.

De este modo, se niega solicitud de reconsideración de la doctrina contenida en el dictamen Nº 260/019, de fecha 24.01.2002.

Saluda atentamente a Ud.

MARCELO ALBORNOZ SERRANO
ABOGADO
DIRECTOR DEL TRABAJO.

Capitulo X Conclusión

Creo que tal vez haya mercado para cinco ordenadores.
Thomas Watson, presidente de IBM, 1943

En general, y no está mal comprenderlo así, se entiende por brecha digital a la brecha o la separación entre los ciudadanos, países o regiones que poseen mayor número de conectados a Internet o bien que hacen uso de los diferentes servicios que pueden circular en torno a las tecnologías de información y comunicación y a Internet.

El criterio que se utiliza para evaluar esta distancia se da casi exclusivamente a través de indicadores que dan cuenta del acceso a estos servicios, pero nada dicen en relación a cuales son las razones por las cuales estas estadísticas muestran estos resultados, la mayoría de las veces negativos. Como es sabido, esta instancia requiere de un análisis particular.

Cuando los teóricos abordan los nuevos enfoques sobre las regulaciones en la sociedad de la información, una de las problemáticas más importantes que abordan es la de la brecha digital. En este punto debe tenerse en cuenta un elemento esencial: es interesante hacer notar que las condiciones de acceso de los ciudadanos, las comunidades y las regiones son también condiciones sociales, y básicamente culturales, puesto que muchas limitantes en relación a la brecha digital tiene que ver directamente con la educación y la apropiación que puedan hacer las comunidades de estos procesos y mediaciones técnicas. Por ello, no solo debemos llamar digital a esta separación o distanciamiento entre los que tienen o no acceso a las infraestructuras, sino que debemos emplear un criterio abarcativo que incluya visiones y análisis sociológicos y culturales de cada una de las regiones analizadas. Este es un puntoesencial. El derecho a la información, a las comunicaciones libres y seguras, el acceso a un servicio universal y a la universalización del acceso (según el caso) son piezas esenciales para el desarrollo de las regiones. Desafortunadamente para muchos de los países latinoamericanos estos derechos se han visto mal protegidos, o dicho técnicamente -como se ha mostrado en los materiales del curso-, se han visto mal regulados tanto

directa como indirectamente. Si bien todos los programas (y sus correspondientes y fragmentadas legislaciones) a nivel nacional –muchos de ellos de una calidad excelente- han receptado el principio de universalidad de las comunicaciones y en todos ellos rige el concepto básico de que todos los habitantes tienen el derecho a que les sea prestado el servicio de comunicaciones en condiciones económicas razonables, los resultados no siempre han sido buenos. Muchos han quedado en una mera retórica.

Legislaciones complejas e ineficientes, regulaciones que perjudican y ensombrecen las ya de por sí complejas condiciones de mercado y perjuicios sobre la calidad de los servicios, son moneda corriente en el mundo de las regulaciones. ¿A que de debe que esta ineficiencia en las técnicas regulativas discursivas? ¿A que se debe este cansancio sobre la retórica de grandes declaraciones que no conducen más que desperdiciar tiempo y recursos valiosos? No podríamos asegurar aún ninguna de las respuestas posibles. Pero podemos observar que el emergente de las regulaciones a través de la tecnología y la creciente importancia de la mediación técnica para el desarrollo de nuestras sociedades puede explicar algunas partes de este sofisticado y sinuoso laberinto. Existen por un lado legislaciones, mas o menos eficientes, las regiones también poseen instituciones más o menos preparadas para trabajar sobre las nuevas incumbencias de convergencia tecnológica y liberalización del mercado de comunicaciones en un sentido amplio. Podemos marcar que también se observan empresas, que siendo locales (las menos) o extranjeras, están dispuestas a contribuir en la regulación y a desarrollar sus servicios. Pero, ¿no nos está faltando algo del esquema presentado anteriormente en relación a las regulaciones?

Bueno, aquí nos topamos de lleno con el problema de las regulaciones en la sociedad de la información. Paulatinamente el derecho entra en un olvido de su potencialidad de técnica regulativa, producto del exponencial desarrollo tecnológico y de la invasión del mercado hacia las esferas públicas que dominaron la tradición moderna de acceso a los bienes culturales. El desarrollo tecnológico prescinde del derecho y esta técnica solo queda para brindar una suerte de garantía sobre lo que ya está solidificado bajo otras arquitecturas. Si observamos que una de las formas regulativas esenciales -para toda regulación que se precie de tal- se da a través del diseño y desarrollo de tecnología, podemos afirmar que las regiones que no diseñan tecnología están imposibilitadas de alcanzar una de las importantes instancias de las regulaciones actuales. Específicamente la tecnológica, quedando acríticamente sujetas a la importación de tecnología y, como tal, a regulaciones que no le pertenecen.

El error tantas veces repetido y no siempre visto es subestimar el impacto de las mediaciones técnicas sobre las sociedades. No se comprenden los procesos tecnológicos de las tecnologías, dado que no se los analizan desde una perspectiva cultural. El punto a poner de resalto en los análisis es justamente observar que el nuevo paradigma tecnológico es el fiel reflejo cultural de las sociedades que desarrollan la tecnología. Allí es donde este nuevo tipo de regulaciones, apegado al diseño y proyección de la tecnología, cobra la real entidad en el contexto actual.

Encontraremos entonces, por un lado, regiones y estados que desarrollan tecnología y por el otro, estados y regiones que se verán incapacitados de cierta planificación, intentando participar en el gobierno de las redes mediante sus necesarias pero obsoletas herramientas jurídicas.

Conocer el estatus tecnológico disponible en un momento histórico determinado importa para las sociedades informacionales, la posesión de las llaves que conducen al desarrollo de las regiones. Conocer el estatus tecnológico de una época equivale al manejo del conocimiento sobre los horizontes que podría alcanzar y buscar una sociedad. La nueva forma regulativa requiere de planes, legislaciones e instituciones que puedan captar cual es el desarrollo tecnológico que su región puede tener. Este es el punto importante a desarrollar. Una tecnología desarrollada localmente, con sus correspondientes servicios, es una tecnología que podrá ser fácilmente aceptada y tendrá asegurada su potencialidad para contribuir al desarrollo de las regiones. Esta tecnología no requerirá ser apropiada, puesto que estos desarrollos ya les pertenecen.

Es por la misma razón antes expuesta que hemos aceptado el desafío de:

- investigar las distintas posturas de los autores, incluso creando posturas propias respecto al tema,
- analizar a cabalidad la legislación nacional y derecho comparado en lo relativo a los distintos ámbitos de protección de la privacidad.
- Comentar ya sea jurisprudencia nacional y extranjera, dictámenes, proyectos de ley y todo lo relativo al tema desde una perspectiva crítica e informada.
- Corroborar los distintos avances que existen a nivel micro y macro de las legislaciones, doctrina y jurisprudencia.
- comparar los distintos regímenes legislativos existentes, buscando sus similitudes y diferencias en cuanto a la aplicación y protección de la privacidad por el Uso de las Tecnologías de la Información.

- Y atrevernos en forma activa a criticar la realidad nacional, regional y mundial relativo específicamente al cuando nos preguntamos ¿Qué sucede con el Derecho a la Privacidad por el uso de las Tecnologías de la Información?

Esperamos que con la sola lectura de esta memoria, la cuestión tenga una respuesta concreta.

Para concluir y proyectarnos más allá de este presente trabajo, es que nos atrevemos a visualizar lo que vendrá en un futuro, no con osadía, sino con la mirada de un investigador.

- Por un lado proyectamos en Chile un cambio en la legislación nacional respecto a la protección civil de la privacidad, amparando ya no solo a personas naturales, sino que se sumarán además a esta protección, las personas jurídicas, las que tendrán plena capacidad para interponer recursos como el habeas data.
- Por otro lado, en lo relativo a protección penal, existirá una modificación sustantiva respecto al mal uso que se le puede dar a las tecnologías de las Información y las Comunicaciones, aumentando no tan solo los delitos derivados, sino el ámbito de aplicación material y territorial.
- Existirá una mayor regulación en lo concerniente a la privacidad por el uso de tecnologías como Internet y redes.
- Se formarán Organismos Nacionales en Chile cuya misión sea la Protección de los Datos y Consumidores con herramientas efectivas y prácticas.
- Surgirán Organismos Internacionales de las Convenciones Internacionales que asumirán un papel integrador, conciliador y omnicomprensivo en la protección de bienes jurídicos como la privacidad que se pudieran ver vulnerador por el Uso de las Tecnologías de la Información. Y si estas figuras jurídicas no nacen por esta vía, surgirán por vía de Tratados Internacionales, sobre todo cuando hagan referencia a Tratados de Libre Comercio entre distintos países.
- Por último podemos aventurarnos que la Utopía del anonimato en Internet nunca será posible comprobarse ni tecnológica ni legalmente, pues siempre existirán valores por sobre privacidad, valores como el bien común, la integridad del Estado y la nunca falto de polémica “guerra” contra el Terrorismo, pues la intervención de los Estados en el uso de las Tecnologías de la Información será completa. Por tanto, la privacidad, entendida como el derecho a estar solo, nunca será posible de asegurar completamente.

Bibliografía:

Autores:

- CASTAÑEDA GONZÁLEZ, Alberto, BONADEO FIOONI, Rodrigo y SÁNCHEZ ECHEVARRÍA, Jesús, "Guía práctica de Protección de Datos de Carácter Personal", Ed. Experiencia, Barcelona, 2002.

- CONSEJO DE ESTADO FRANCÉS, "Internet y las redes digitales. Los estudios del Consejo de Estado", 1997 en http://www.ladocfrancaise.gouv.fr (Consulta: 28-02-2000)

- DE MIGUEL ASENSIO, Pedro, "Derecho privado de Internet", Civitas, 3ª ed., Madrid, 2002.

- ESTEVE GONZÁLEZ, Lydia (Coord.) y otros, "Derecho e Internet. Textos Jurídicos Básicos", Ed. Compás, Alicante, 2001.

- LLÁCER MATACÁS, Mª Rosa, "La Protección de los Datos Personales en Internet", en La regul@ción del comercio electrónico, Dykinson, Madrid, 2003, pp. 158 – 190.

- MAYOL GIL, Juan Antonio, MEDRÁN VIOQUE, Rafael y ORTEGA GIMÉNEZ, Alfonso, "Data Protection in Internet", en REDI: Revista Electrónica de Derecho Informático, núm. 50, 2002.

- MAYOL GIL, Juan Antonio, MEDRÁN VIOQUE, Rafael, MIESKES, Manfred y ORTEGA GIMÉNEZ, Alfonso, "Comparative analysis between spanish and german law concerning data protection in internet", en uaipit.com –Portal de la Universidad de Alicante sobre Propiedad Industrial e Intelectual y Sociedad de la Información– (http://www.uaipit.com/en/ITL/Data_Protection_Internet.pdf), 2003.

- ORTEGA GIMÉNEZ, Alfonso, "Censo promocional y consentimiento del afectado", en IURIS. Actualidad y Práctica del Derecho, núm. 68, La Ley, Madrid, Enero 2003.

- ORTEGA GIMÉNEZ, Alfonso, "La protección de datos de carácter personal en Internet (con especial referencia a la transferencia internacional de datos)", en uaipit.com – Portal de la Universidad de Alicante sobre Propiedad Industrial e Intelectual y Sociedad de la Información–, 2003.

- RUIZ CARRILLO, Antonio, "La protección de los datos de carácter personal", Ed. Bosch, Barcelona, 2001.

- Corripio Gil-Delgado, María de los Reyes. Regulación jurídica de los tratamientos de datos personales realizados por el sector privado en Internet. Premio de la Agencia de Protección de Datos, Madrid, 2000

- Garfinkel, Simson y Spafford, Gene. Seguridad y comercio en el Web. Ed. McGraw-Hill, México, 1999

- Herrera Bravo, Rodolfo, "La protección de datos personales como una garantía básica de los derechos fundamentales". Revista de Derecho Público, de la Agrupación de Abogados de la Contraloría General de la República, Año 2 Nº 5, mayo/agosto 2001

- Johnson, Deborah G., Ética On-line. La ética en las redes informáticas. Moralia Nº20, 1997 Real Academia Española, Diccionario de la Lengua Española. 22ª edición, 2001

- Ull Pont, Eugenio. Derecho público de la informática (Protección de datos de carácter personal). UNED Ediciones, Madrid, 2000

- USER'S DECLARATION. European Ministerial Conference. Bonn, 1997. Forum Information Society Report 1997

- 'Curso de Regulación de Nuevos Servicios y Aplicaciones IP', módulos 1 al 9 ofrecidos por la CITEL, la UIT, e INICTEL, año 2002.

- 'La galaxia Internet', Castells, Manuel, Areté, 317, 2001, España.

- 'La era de la información', Castells, Manuel, Siglo XXI, 591, 1999, México.

- 'The future of the ideas: the fate of the commons in a connected world', Lessig, Lawrence, Random House, 352, 2001, USA.

- 'Code and other laws of cyberspace', Lessig, Lawrence, Basic Books, 297, 1999 USA

- 'Open Code and Open Society', Lessig, Lawrence, Tutzing, Germany, 1 June, 2000; http://cyberlaw.stanford.edu/lessig/content StanfordLawSchool. (A)

- 'Las leyes del ciberespacio', Lessig, Lawrence, en "Cuadernos Ciberespacio y Sociedad" Nº3 Marzo 1999. Traductor: Javier Villate, URL del documento original: http://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf (3 abril 1998).

- 'La ética del hacker y el espíritu de la era de la información', Pekka Himanen, Destino, 255, 2001, España

- Eugenio Alberto Gaete Gonzalez, Derecho a la Intimidad: Protección de Datos Personales, Revista de Derecho Informático Alfa Redi, 2003

- - Herrera Bravo, Rodolfo y Núñez Romero, Alejandra. Derecho Informático. Editorial La Ley Ltda. Santiago, 1999.

- - Suñé Llinás, Emilio.Tratado de Derecho Informático. Universidad Complutense. Volumen I. Madrid, 2000.

- Consumer International, Office for Developed and Transition Economies, Privacy@net an international comparative study of consumer privacy on the internet, London, United Kingdom, 2001.

- MAGLIONA MARKOVICTH, Claudio Paul; "Breve Análisis De La Ley Número 19.628 Sobre Protección de la Vida Privada", Revista Electrónica De Derecho Informático, http://vlex.com/redi/No._29_-_Diciembre_del_2000/4; http://www.alfa-redi.org/revista/data/30-7.asp.

- MAGLIONA MARKOVICTH, Claudio Paul; "Decreto Supremo N°779 Que Aprobó el "Reglamento del Registro de Banco de Datos Personales a Cargo de Organismos Públicos", Boletín Hispanoamericano de Informática y Derecho, Año III - No. 10 Tercer Cuatrimestre - 2000 http://www.ulpiano.com/Chile_Comentario_reglamento.htm.

- Rafael Roncagliolo. "¿Se Construye Ciudadanía en la Sociedad de la Información?" en Ciudadanos en la Sociedad de la Información. Pontificia Universidad Católica del Perú y The British Council Perú. Lima, 1999.

- Yoneji Masuda. La Sociedad Informatizada como Sociedad Post-Industrial. Editorial Tecnos, 1994.

- El Libro Verde fue elaborado por la Comisión de la Sociedad de la Información del Ministerio de Ciencias de Portugal y aprobado por el Consejo de Ministros de Portugal en abril de 1997. Disponible en http://www.missao-si.mct.pt/ . [Consulta: 12 dic. 2001]

- Francisco Aguadero Fernández. La Sociedad de la Información. Acento Editorial, 1997.

- Gilles Lipovetsky, El Crepúsculo del Deber. La Ética Indolora de los Tiempos Democráticos. Editorial Anagrama, 1998, citado por Jesús Mercader Uguina en Derecho del Trabajo, Nuevas Tecnologías y Sociedad de la Información, Editorial LexNova, 2002.

- Manuel Castells. La Era de la Información: La Sociedad Red, Vol. I. Alianza Editorial, 1997.

- David Held. Modelos de Democracia. Alianza Editorial, 2001.

- Santiago Muñoz Machado. La Regulación de la Red. Poder y Derecho en Internet. Taurus, 2000.

- Comisión Europea. Libro Verde sobre la Convergencia de los Sectores de Telecomunicaciones, Medios de Comunicación y Tecnologías de la Información y sobre sus Consecuencias para la Reglamentación. 3 de diciembre de 1997. http://europa.eu.int/ISPO/convergencegp/97623es.pdf

- NIC Chile en http://www.nic.cl

- Internet Corporation for Assigned Names and Numbers, en http://www.icann.org.

- Internet Assigned Numbers Authority, en http://www.iana.org/ .

- Jon Katz. Revista Wired, “Birth of a Digital Nation”. http://www.wired.com/wired/5.04/netizen.html

- Asdrad Torres. ¿Qué es la Sociedad de la Información?, en Ciudadanos en la Sociedad de la Información, publicada por el Fondo Editorial de la Pontificia Universidad Católica del Perú y The British Council Perú, 1999.

- Giménez, Irene M. ¿Es posible una regulación en Internet? Ponencia disponible en ECOMDER 2000. Área Temática: Business to Goverment

- Loreti, Damián Miguel. Las Relaciones Laborales en la Era de la Información: El Papel del Gobierno y los Interlocutores Sociales. Ponencia disponible en ECOMDER 2000. Área Temática: Business to Government

- Del Pozo Moreira, José Vicente. Una Visión General del Comercio Electrónico en el Ecuador. Ponencia disponible en ECOMDER 2000. Área Temática: Business to Government.

- LUCAS MURILLO DE LA CUEVA, Pablo. "El derecho a la autodeterminación informativa", Temas claves de la Constitución Española, Editorial Tecnos, Madrid, 1990.

- LUCAS MURILLO DE LA CUEVA, Pablo. "Informática y protección de datos personales", Cuadernos y Debates nº 43, Centro de Estudios Constitucionales, Madrid, 1993.

- MANZANARES, José Luis; CREMADES, Javier. "Comentarios al Código Penal", La Ley-Actualidad, Las Rozas (Madrid), 1996.

- MARTÍN BERNAL, José Manuel; MARTÍN GARCÍA, Pilar. "Intimidad y libertades", Informática y Derecho nº 4, UNED, Editorial Aranzadi, Centro Regional de Extremadura, Mérida, 1994, págs. 119 a 128.

- MORALES PRATS, Fermín. "El Código penal de 1995 y la protección de los datos personales", Jornadas sobre el derecho español de la protección de datos personales, Madrid 28-30 octubre 1996.

- ORZABAL, Josefina C. "Bases de datos, privacidad y responsabilidad civil", Informática y Derecho nº 4, UNED, Editorial Aranzadi, Centro Regional de Extremadura, Mérida, 1994, págs. 137 a 144.

- PESO NAVARRO, Emilio del ; RAMOS GONZÁLEZ, Miguel Ángel. "Confidencialidad y seguridad de la información: La LORTAD y sus implicaciones socioeconómicas", Editorial Díaz de Santos, Madrid, 1994.

- REY GUANTER, Salvador del. "Tratamiento automatizado de datos de carácter personal y contrato de trabajo", Relaciones Laborales nº 15, 1993, págs. 7 a 30.

- RUIZ MIGUEL, Carlos. "El derecho a la intimidad informática en el ordenamiento español", Revista General de Derecho, Año LI, núm. 607, abril 1995, págs. 3207 a 3234.

- SÁNCHEZ PEGO, Francisco Javier. "La intimidad del trabajador y las medidas de prevención de riesgos laborales", Actualidad Laboral nº 2, 6-12 enero 1997, págs. 19 a 31.

- SÁNCHEZ TORRES, Esther. "El derecho a la intimidad del trabajador en la Ley de Prevención de Riesgos Laborales", Relaciones Laborales nº 20, Octubre 1997, págs. 95 a 124.

- SARDINA VENTOSA, Francisco. "El derecho a la intimidad informática y el tratamiento de datos personales para la prevención del fraude", Actualidad Informática Aranzadi nº 25, Octubre 1997.

- SERRADILLA SANTOS, Mº Paz; TRINIDAD NUÑEZ, Aurelia; VELÁZQUEZ RODRÍGUEZ, Teresa. "Implicaciones de la informática en el ámbito laboral", Informática y Derecho nº 4, UNED, Editorial Aranzadi, Centro Regional de Extremadura, Mérida, 1994, págs. 657 a 673.

- TONIATTI, Roberto. "Libertad informática y derecho a la protección de los datos personales: principios de legislación comparada", Revista Vasca de Administración Pública, nº 29, enero-abril 1991, págs. 139 a 162.

- Memoria de la Agencia de Protección de Datos de 1996, Madrid, 1997.

- BLÁZQUEZ ANDRÉS, Mª Consuelo; CARRASCOSA LÓPEZ, Valentín; . "Intimidad personal y limitaciones", Informática y Derecho nº 4, UNED, Editorial Aranzadi, Centro Regional de Extremadura, Mérida, 1994, págs. 85 a 90.

- CANTERO RIVAS, Roberto. "Los derechos inespecíficos de la relación laboral: libertad de expresión, libertad ideológica y derecho a la intimidad", La Ley nº 4402, viernes, 24 octubre 1997, págs. 1 a 6.

- CARRASCOSA LÓPEZ, Valentín. "Derecho a la Intimidad e Informática", Informática y Derecho nº 1, UNED, Centro Regional de Extremadura, Mérida, 1992, págs. 7 a 26.

- COSTA CARBALLO, Carlos da. "Introducción a la informática documental. Fundamentos teóricos, prácticos y jurídicos", Editorial Síntesis, Madrid, 1993.

- DAVARA RODRÍGUEZ, Miguel Ángel. "La Ley española de protección de datos (LORTAD):¿una limitación del uso de la informática?", Actualidad Informática Aranzadi n 77, 19 noviembre 1992.

- DAVARA RODRÍGUEZ, Miguel Ángel. "Manual de Derecho Informático, Aranzadi Editorial, Pamplona, 1997.

Legislación Nacional

- Compilación de Textos Oficiales del Debate Parlamentario de la Biblioteca del Congreso Nacional, Ley N°19.628 (D.Oficial, 28 de agosto de 1999) Santiago, Chile 1999.
- Diario Oficial de La República de Chile N°36.810, de fecha 11 de noviembre de 20000, en el cual se publicó el Decreto Supremo N°779 que aprobó el Reglamento del Registro de Banco de Datos Personales a Cargo de Organismos Públicos.
- Ley 19.628 Sobre Protección de la Vida Privada
- Ley. 19.970 sobre Sistema Nacional de Registros de ADN
- Ley 19.233 relativa a Delitos Informáticos
- Sentencia de la Corte Suprema ante Recurso de Protección .
- Dictamen nº 260/19 de la Dirección del Trabajo.
- Dictámen Ord. Nº 1147/34 de la Dirección del Trabajo.
- Variada

JURISPRUDENCIA

- Variada

Legislación Extranjera

- Variada

Indice