SERIE DE
DOCUMENTOS
MATERIALES
DOCENTES

ACADEMIA
JUDICIAL
CHILE

Derecho Informático

Autores

Lorena
Donoso
Abarca

Carlos
Reusser
Monsálvez

Academia Judicial de Chile | www.academiajudicial.cl

SERIE DE
DOCUMENTOS
MATERIALES
DOCENTES

ACADEMIA JUDICIAL CHILE

Autores

Lorena Donoso Abarca

Abogada de la Universidad de Chile, es Magíster en Informática y Derecho por la Universidad Complutense de Madrid. Árbitra de NIC Chile para la resolución de conflictos sobre nombres de dominio en internet, también es consejera del Instituto Chileno de Derecho y Tecnologías y profesora asociada del Departamento de Derecho Procesal de la Universidad de Chile. Fue directora del Centro de Estudios en Derecho Informático de esa misma universidad.

Carlos Reusser Monsálvez

Abogado de la Universidad de Chile y Magíster en Derecho Constitucional por la Pontificia Universidad Católica de Chile, es Máster en Informática y Derecho y Especialista en Derechos Humanos por la Universidad Complutense de Madrid. Experto en Gestión del Conocimiento por la Universidad Carlos III de Madrid, es profesor de Derecho de la Información en la Universidad Alberto Hurtado y consejero del Instituto Chileno de Derecho y Tecnologías.

Academia
Judicial
de Chile

Diseño y
Diagramación:
Estudio Real
somosreal.cl

Material
docente N° 31

Santiago,
Chile 2021

ISBN N°
2022-A-1849

Resumen

Bajo el título Derecho Informático, se agrupa en este material docente una serie de lecciones relacionadas con los distintos ámbitos de la ciencia jurídica que se han visto impactados por la irrupción de las tecnologías de la información y la comunicación (TIC).

Se introducen los temas generales, con una exposición de los principios y estándares normativos que se han ido construyendo durante los últimos años, destacando la relevancia los enfoques de neutralidad tecnológica y de mínima intervención del sistema normativo, que resultan esenciales a los efectos de mantener la coherencia del ordenamiento jurídico.

También se destaca la necesaria compatibilidad, a la hora de dictar normas y de interpretarlas, con los estándares internacionales, pues el derecho debe ser consciente de que internet ha difuminado las fronteras jurídicas entre los Estados, facilitando el paso de globalización económica, pero también el de mundialización de los derechos.

Palabras clave

Derecho informático – derecho de las tecnologías – derecho de internet – derecho de las TIC – derecho digital.

Índice de contenidos

Tabla de abreviaturas

CC	:	Código Civil
CE	:	Constitución española
CPC	:	Código de Procedimiento Civil
CPR	:	Constitución Política de la República de Chile
DT	:	Dirección del Trabajo
FEA	:	Firma Electrónica Avanzada
IA	:	Inteligencia Artificial
RGPD	:	Reglamento General de Protección de Datos, forma abreviada en que se conoce el "Reglamento relativo a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE", de la Unión Europea.
TIC	:	Tecnologías de la información y la comunicación
UNCITRAL	:	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

Introducción

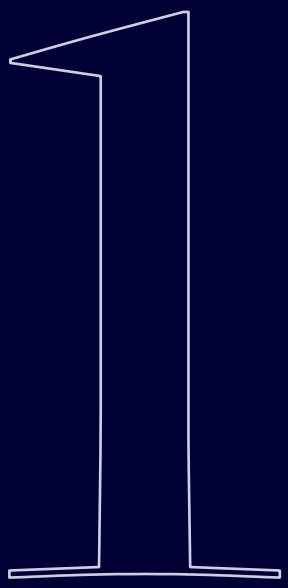
Bajo el título Derecho Informático, agrupamos una serie de lecciones relacionadas con distintos ámbitos del derecho que se han visto impactadas por la irrupción de las tecnologías de la información y la comunicación (TIC). Si bien el análisis no es exhaustivo, lo que sería más propio de un tratado, se pretende mostrar un abanico de materias que permita comprender la lógica con la cual se ha venido adaptando la legislación nacional, en muchos casos centenaria, para cubrir las hipótesis a que ha dado lugar el desarrollo de la tecnociencia.

En ese orden de ideas, en el primer capítulo se introducen los temas generales, con una exposición de los principios y estándares normativos que se han ido construyendo para estos efectos, en que cobra especial relevancia los enfoques de neutralidad tecnológica y de mínima intervención del sistema normativo, esenciales a efecto de mantener la coherencia del ordenamiento jurídico y evitar la dictación de normas que, por referirse a una tecnología concreta, devenga tempranamente en obsoleta.

Otro de los aspectos que debe resaltarse es que las nuevas normas han de ser compatibles y adecuadas, en la medida de lo posible, a los estándares internacionales, pues internet ha difuminado las fronteras jurídicas entre los Estados, facilitando el paso a los fenómenos de globalización económica y de mundialización de los derechos.

En los restantes capítulos aplicamos los principios y describimos el estado del arte en materia de protección de datos personales, firma electrónica, criminalidad informática, contratación electrónica y relaciones laborales y tecnologías.

Esperamos que los ejemplos que se entregan resulten ilustrativos respecto de las aplicaciones de la normativa que reseñamos y permitan comprender los razonamientos que están detrás.



Introducción al derecho informático

← Índice de contenidos

1.1 Del fulgor de la informática jurídica al advenimiento de la gestión del conocimiento jurídico

Tradicionalmente se habla de dos áreas de interacción entre el derecho y las tecnologías de la información y las comunicaciones (TIC); en una de ellas, la informática se aplica a las ciencias del derecho y, en la otra, la regulación jurídica se aplica al fenómeno informático, siendo estas interacciones las que explicaremos a continuación.

1.1.1 De la informática jurídica a la inteligencia artificial (IA) aplicada al derecho

La primera área de interacción fue denominada originalmente "informática jurídica" y se refiere al empleo de las TIC como herramientas al servicio de los juristas, en auxilio de sus labores. Ello en razón de que, desde sus inicios, las máquinas de cálculo automático demostraron una aptitud especial para el tratamiento de campos codificados de información de relevancia jurídica, especialmente documentos necesarios para la toma de decisiones.

Y ello era necesario, pues "el flujo incesante de normas y decisiones jurisprudenciales, cuyo exacto y puntual conocimiento son imprescindibles para un adecuado funcionamiento del sistema jurídico, hace casi imposible su discernimiento, interpretación y aplicación por los operadores jurídicos. La crisis de la información jurídica precipita en las tinieblas al ordenamiento jurídico".[1]

La informática jurídica, al decir de Losano (uno de los grandes pioneros en la materia) está integrada por aquellas técnicas informáticas generales que se han revelado como particularmente adecuadas para el tratamiento electrónico de datos jurídicos[2], a saber:

1 SIMITIS, Spiros, *Informationkrise des rechts un Datenverarbeitung*, C.F. Müller, Karlruhe, 1970; pp. 28 y ss.
2 LOSANO, Mario, *Manual de Informática Jurídica*, Tecnos, Madrid, 1990.

— Informática jurídica **documental,** que se refiere a la organización de las fuentes del derecho, tales como la legislación, la doctrina y la jurisprudencia, en pos de su recuperación para las labores de apoyo al razonamiento jurídico.

— Informática jurídica **de gestión** (u "ofimática", como se denominó años atrás), que subyace a la automatización de procesos rutinarios de los despachos de abogados y cuyo desarrollo ha conducido al conjunto de métodos, técnicas y medios que actualmente se denomina *legaltech* (abreviatura de la expresión anglosajona *legal technology*).

— Informática jurídica **decisional**, que se ha traducido en la creación de sistemas altamente complejos que pretenden emular el razonamiento jurídico y proponer soluciones a problemas concretos que enfrentan los juzgadores (sistemas expertos de apoyo a la decisión jurídica) o, derechamente, transformarse en el juzgador en casos de conflictos de relevancia jurídica, que es la forma en que son utilizados estos sistemas en el día a día de plataformas informáticas que intermedian servicios con múltiples usuarios, como es el caso, por ejemplo, de las aplicaciones de telefonía móvil que resuelven conflictos entre anfitriones y huéspedes de alojamientos particulares.

En el ámbito jurídico, en su evolución y a través del desarrollo de la inteligencia artificial se han creado sistemas que derechamente emulan la labor del juez. Tal es el caso de Prometea, sistema decisional que "resuelve la confección automática de los dictámenes jurídicos que el Fiscal General Adjunto envía al Tribunal Superior de Justicia para cada caso judicial"[3] a través del empleo de inteligencia artificial, esto es, de programas computacionales que analizan miles de resoluciones o dictámenes de los que *aprende,* de modo que cuando se le presentan nuevas hipótesis es capaz de analizar si hay casos similares en su memoria de aprendizaje y emula los razonamientos humanos para elaborar un documento de propuesta de resolución.

3 Véase ESTÉVEZ, Elsa y otros, "Prometea: Transformando la administración de justicia con herramientas de inteligencia artificial". BID, Washington DC, 2020. CC-IGO 3.0 BY-NC-ND.

Uno de los objetivos de quienes se dedican a esta disciplina ha sido analizar la aptitud del sistema normativo para absorber y regular adecuadamente la nueva realidad a partir del análisis de las reglas generales y principios que rigen en nuestro ordenamiento jurídico, verificando si las hipótesis que surgen del empleo de las TIC son susceptibles de ser subsumidas en sus normas.

1.1.2 El derecho informático o derecho digital

La segunda dimensión que nos interesa aquí dice relación con el **derecho informático**, la rama del derecho que estudia la regulación jurídica del fenómeno informático. Si bien derecho informático no es una denominación unívoca, sí es la más antigua.

Derecho informático o *Rechtsinformatik* fue un concepto acuñado por el profesor Wilhelm Steinmüller, quien en los años 70 se refirió así a estas materias en la Universidad de Ratisbona (Regensburg). Otros autores le han llamado derecho telemático, derecho de las nuevas tecnologías, iuscibernética, derecho tecnológico, derecho del ciberespacio, derecho de internet, derecho de las TIC y, más recientemente, **derecho digital**.

Más allá de la denominación, lo importante es que todos estos conceptos aluden a lo mismo, esto es, se trata de principios y de un "conjunto de normas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones".[4]

Uno de los objetivos de quienes se dedican a esta disciplina ha sido analizar la aptitud del sistema normativo para absorber y regular adecuadamente la nueva realidad a partir del análisis de las reglas generales y principios que rigen en nuestro ordenamiento jurídico, verificando si las hipótesis que surgen del empleo de las TIC son susceptibles de ser subsumidas en sus normas.

Por ejemplo, en su momento se hicieron ingentes esfuerzos para que los operadores del derecho se convencieran de que, cuando una disposición normativa establecía que determinado documento debía constar por escrito, se entendiera que dicho requisito también se cumplía si lo escrito constaba en un documento confeccionado a través de un computador. Y hoy puede parecer lo más natural del

4 CARRASCOSA, Valentín. "El Derecho Informático como asignatura para juristas e informáticos", en *Revista de Informática y Derecho*, Universidad Nacional de Educación a Distancia, Centro Regional de Extremadura, Mérida, 1995; p. 3

Se debe tener presente que el enfoque de esta disciplina es multidisciplinario (abarca cuestiones de muchas áreas del derecho) o más bien transdisciplinario, pues la resolución de los problemas que se presentan en el día a día requieren la aplicación de múltiples áreas del conocimiento.

mundo, pero requirió de decenas de artículos académicos, múltiples actividades de difusión y variopintas acciones de *evangelización* jurídica para asentar esto como una convicción.

Cuando la sola interpretación no ha rendido frutos, se ha debido revisar y adaptar la legislación, como ocurrió en Chile en materia de firmas y, por derivación, respecto de los documentos firmados, lo que dio lugar a la Ley Nº 19.799, que normó lo relativo a las firmas y documentos electrónicos.

De igual forma, en lo que respecta a la proliferación de sistemas automatizados de tratamiento de información de las personas, incluso se ha debido modificar la Constitución Política de la República (CPR) para actualizar las garantías fundamentales, agregando el derecho fundamental a la protección de datos personales, cuestión que se hizo a través de la Ley Nº 21.096, de 2018.

1.1.3 Características del derecho informático

La existencia de esta nueva rama del derecho no ha sido pacífica, discutiéndose incluso, como ya hemos visto, no solo la denominación sino también su existencia misma. Ello, porque para algunos en realidad solo de trataría de una fase de adecuación de nuestro sistema jurídico, en que las ramas tradicionales del derecho deben ir adaptándose a los nuevos fenómenos.

Pero a estas alturas es difícil rebatir su existencia, sobre todo si consideramos que ya no solo cuenta con instituciones y principios propios, normas específicas, una rica doctrina y variada jurisprudencia, sino también con una trayectoria que se acerca al medio siglo desde sus primeras formulaciones.

En segundo lugar, se debe tener presente que el enfoque de esta disciplina es multidisciplinario (abarca cuestiones de muchas áreas del derecho) o más bien transdisciplinario, pues la resolución de los problemas que se presentan en el día a día requieren la aplicación de múltiples áreas del conocimiento, como la ingeniería, la economía y la documentación, entre otras disciplinas, sin perjuicio de aquellos

conocimientos sobre tratamiento de la información (informática) y de su transmisión y comunicación (telemática, telecomunicaciones o, más modernamente, comunicaciones electrónicas).

1.1.4 La informática y las telecomunicaciones como objeto regulado

En este contexto, entendemos la **informática** como el conjunto de técnicas destinadas al tratamiento lógico y automático de la información necesaria para la resolución de un determinado problema. En palabras de Frosini, la informática es "la técnica de memorización artificial, de elaboración (o sea de descomposición y recomposición), de transmisión instantánea a distancia incluso muy considerable (en hipótesis teórica ilimitada) de una serie de informaciones en el lenguaje del calculador electrónico". [5]

En el mismo sentido, se afirma que estamos en una fase del desarrollo de la comunicación humana, en que las máquinas electrónicas de tratamiento de la información cobran un papel protagónico como medio transmisor de un *metalenguaje* que se caracteriza por ser totalmente artificial.

Complementaremos lo anterior afirmando que por **sistema de información** entenderemos al conjunto de elementos diseñados para el soporte, administración y gestión de información en sus diversas presentaciones: texto, imagen, sonido, etcétera. Cabe hacer presente a este respecto que un sistema de información puede ser tanto manual –como sería el conjunto de documentos ordenados en un kárdex– como electrónico o computacional, que es el de más uso en nuestros días.

Adicionalmente, **telecomunicaciones** en nuestro derecho se define como toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos e informaciones de cualquier naturaleza, por línea física, radioelectricidad, medios ópticos u otros sistemas electromagnéticos.[6] Resulta importante el concepto, por cuanto la

5 FROSSINI, Vitorio, *Cibernética, Derecho y Sociedad*, editorial Tecnos, Madrid, 1982.
6 Art. 1º Ley Nº 18.168.

informática y las telecomunicaciones, así como las aplicaciones a que estas dan lugar, en muchos casos han dotado de una nueva configuración a las relaciones jurídicas que tradicionalmente se realizaron en un entorno presencial.

Sin embargo, debemos tener presente que el concepto de telecomunicaciones como resultado de la digitalización de las comunicaciones también se está abandonando, a favor de uno más adecuado a los sistemas globales de comunicación al uso, como es la idea de **comunicaciones electrónicas**; de hecho, y a modo de ejemplo, ya existe la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la cual se establece el Código Europeo de las Comunicaciones Electrónicas, de modo que numerosos países ya están realizando ajustes a su normativa interna para efectos de dejar atrás las lógicas de las antiguas leyes de telecomunicaciones.

1.2 Principios que informan el derecho informático como disciplina jurídica

Aunque nos encontramos ante un área del derecho emergente y con pretensiones de independencia, también se inserta dentro del ordenamiento jurídico general y, por lo tanto, los principios generales del derecho tienen plena aplicación dentro de ella, como se verá a continuación.

1.2.1 El respeto a la dignidad humana como base del sistema normativo

En primer lugar encontramos el respeto a la **dignidad humana**, en virtud del reconocimiento de que todo sistema jurídico tiene por objeto central la regulación de la vida del hombre en sociedad, en aras del bien común. Veamos un ejemplo.

En materia de protección de datos personales, a nivel internacional se ha proscrito o restringido severamente la adopción de decisiones automatizadas respecto de una persona; el artículo 22 del Reglamento General de Protección de Datos Personales de Europa (RGPD)[7], como regla general prevé que toda persona "tendrá derecho a no ser objeto de una decisión únicamente basada en el tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos en él o le afecte significativamente de modo similar". Ello en razón de que, en términos amplios, se considera lesivo para la dignidad humana que una máquina decida el destino de una persona.

Ahora, si bien este reconocimiento no se ha realizado expresamente en nuestro ordenamiento jurídico, podemos deducirlo a partir de una interpretación en base a garantías fundamentales, especialmente en lo que se refiere a la garantía fundamental a la protección de datos, de

7 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

la igualdad ante la ley y del reconocimiento de la dignidad humana. En todo caso, en el proyecto de ley que busca actualizar la Ley Nº 19.628 se regula expresamente esta materia.[8]

1.2.2 La autonomía de la voluntad

En esta misma línea, el reconocimiento de la libertad humana y el respeto de la **autonomía de la voluntad**, que se refleja en la autodeterminación de las personas, tiene una importancia gravitante en el derecho informático.

A vía ejemplar, la Ley Nº 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma (en adelante, solo nos referiremos a ella como ley de firma electrónica), establece la libre prestación del servicio de certificación de firma electrónica; es decir, cualquiera que lo desee y cumpla los requisitos que ella exige, puede hacerlo.

También en el comercio electrónico rige el mismo principio, sin perjuicio de reconocerse la necesidad de salvaguardar los derechos de la persona, sobre todo cuando esta se encuentra en una posición más débil ya sea por la falta de conocimientos específicos en la materia, o de reconocimiento de las deficiencias del mercado.

Otra manifestación de este principio la encontramos en la Ley Nº 19.628 sobre protección de la vida privada (que en adelante llamaremos ley de datos personales), la cual reconoce el consentimiento del interesado como un factor legitimante del tratamiento de datos, aun de aquellos cuyo conocimiento por terceros sea fuente de discriminaciones arbitrarias.

1.2.3 El principio de buena fe y sus manifestaciones en las normas de derecho informático

El principio de **buena fe**, enunciado en el Código Civil como "la conciencia de haber adquirido el dominio por un medio lícito, exento de fraude y de cualquier otro vicio", pero que en general podemos

8 Nos referimos al Boletín Nº 11.144-07, refundido con el Nº 11.092-07, que "Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales".

entender como la conciencia de un sujeto sobre la bondad, rectitud o transparencia de su proceder, tiene plena vigencia en el área que aquí nos ocupa.

La reglamentación para el funcionamiento del registro de nombres del dominio .cl, emanado de NIC Chile, señala que siempre se presume que una solicitud de registro de nombre de dominio se ha efectuado de buena fe y en base a un interés legítimo, salvo se demuestre lo contrario.

Otra manifestación clara de este principio la encontramos en las leyes de tratamiento de datos personales de Chile y el mundo, en que prácticamente siempre se hace alusión expresa a que el tratamiento habrá de realizarse conforme a criterios de lealtad y licitud que debe imperar en las relaciones sociales.

Otro ejemplo lo vemos en materia penal, donde las figuras de criminalidad informática contenidas en la legislación exigen que, para que una conducta sea sancionada, concurra un elemento subjetivo del tipo que descarte la buena fe, ya sea que la conducta se haya realizado "maliciosamente", "indebidamente" o con "ánimo de", de forma talque no quepa la menor duda de que la intención del agente es la deprovocar daño a la persona o patrimonio del otro.

Esta es la tendencia internacional, sintetizada en el Convenio sobre la Ciberdelincuencia del Consejo de Europa (llamado usualmente Convenio de Budapest), que es el acuerdo internacional de uso más extendido y considerado a estos efectos como una ley modelo, como explicaremos más adelante.

1.2.4 La igualdad ante la ley como principio base

La **igualdad ante la ley** cobra asimismo especial relevancia en el entorno tecnológico, pues se considera que la paridad en el acceso a los medios y servicios de la sociedad red reviste un factor crítico en el avance hacia una sociedad más desarrollada y justa. Manifestaciones de este reconocimiento las encontramos en la Ley Nº 18.168, ley general de telecomunicaciones, que en su título 4° regula el Fondo

de Desarrollo de las Telecomunicaciones, destinado a subsidiar la instalación de servicios de telecomunicaciones en sectores de depresión económica o de baja densidad geográfica.

Otra manifestación del mismo principio es la normativa técnica relativa a la accesibilidad de los servicios de telefonía básica a personas que sufren de algún grado de discapacidad auditiva, visual o motora, entre otras.

Incluso, las demandas por un acceso a internet como derecho constitucional tienen de trasfondo la diferente posición de las personas en la sociedad, dependiendo de si cuentan o no con maneras de conectarse a la información que necesitan para cumplir con sus deberes ciudadanos.

1.2.5 La neutralidad tecnológica: equivalencia funcional y no discriminación

En derecho informático, un principio capital es el de **neutralidad tecnológica**, que implica que las normas generales o particulares enuncien los derechos y obligaciones de las personas sin nunca definir los medios tecnológicos necesarios para que se cumplan los objetivos de las normas.

Ello implica, por ejemplo en el ámbito de las comunicaciones electrónicas, "la aplicación de la misma regulación a los servicios de telecomunicaciones con independencia de la tecnología utilizada para la prestación de los mismos".[9]

De igual forma, en la normativa de firma electrónica, este principio se ha esbozado como "la no discriminación entre distintas tecnologías y, en consecuencia la necesidad de producir normas que regulen los diversos entornos tecnológicos. Este principio refiere a la flexibili-

9 Comisión Europea, "Revisión 1999 del sector de las comunicaciones", en *Comentarios de ANIEL en relación con la comunicación de la Comisión Europea, COM (1999)539*. Disponible en línea en <http://europa.eu.int/ISPO/infosoc/telecompolicy/review99/comments/aniel22b.htm>

dad que deben tener las normas, es decir, que las mismas no estén condicionadas a un formato, una tecnología, un lenguaje o un medio de transmisión específico".[10]

En el fondo, frente a la velocidad del desarrollo tecnológico, el principio de neutralidad tecnológica busca asegurar la permanencia en el tiempo de un marco normativo estable en la sociedad red. Lo contrario implica el riesgo de una rápida obsolescencia de las normas que se dicten, incluso antes de que las mismas hayan entrado en vigencia, especialmente atendidos los tiempos involucrados en un proceso legislativo.

Falta de neutralidad tecnológica en decisiones judiciales

Un ejemplo del fenómeno inverso, esto es, de falta de neutralidad tecnológica en una decisión judicial, podemos encontrarla en la resolución de 23 de febrero de 2021, de la Corte de Apelaciones de Santiago, que regula y uniforma el uso de herramientas informáticas en los oficios notariales.

En ella, el señalado tribunal establece que pueden autorizarse firmas en los instrumentos privados a distancia, y se considerarán como suscritas en presencia de ministro de fe.

Pero en vez de definir las condiciones para que ello ocurra y no se pongan reparos a la validez de la firma, derechamente define que ello debe hacerse a través de la tecnología de la videoconferencia o de la videollamada, aun cuando existan otras tanto o más confiables.

10 Asociación Argentina de Derecho de Alta Tecnología, *Conclusiones Generales de la Comisión de Firma Digital*, Asociación Disponible en línea (28-07-2003) en <http://www.aadat.org/conclusiones_generales42.htm>

Como consecuencia natural de este principio, las normas deberán ser interpretadas de manera progresiva, procurándose la adaptación de las normas al estado de la técnica en cada momento.

Y como manifestación de este principio, se reconoce la **equivalencia funcional** de los medios y aplicaciones que permiten celebrar actos y contratos en el entorno tecnológico, con aquellas que se realizan en el mundo presencial. Revisemos algunos ejemplos.

En el ámbito laboral, se reconoce la posibilidad de llevar el registro de asistencia y el libro de remuneraciones a través de medios tecnológicos.[11]

En materia procesal, otro ejemplo cotidiano es el creciente reconocimiento de los efectos jurídicos del correo electrónico como notificación, incluso en acciones de protección, o la publicación de "estados diarios" digitales; lo mismo sucede con la firma electrónica, que según ha reconocido la respectiva ley, produce los mismos efectos que la firma ológrafa y, por ende, se autoriza que las resoluciones judiciales se firmen de esta manera, sin que se requiera un ministro de fe, si se emplea firma electrónica avanzada (FEA).

Esta asimilación, en todo caso, no puede ser aplicada a ciegas, por cuanto en muchos casos la intervención de la tecnología lleva a cuestionarnos cuál es su real equivalencia con los actos realizados en forma presencial. Un ejemplo de esto son los sistemas de conversación simultánea, en los que si bien la forma de expresión es escrita, no podemos sostener a ciencia cierta que estamos frente a documentos, sino que, tratándose de cada aplicación informática deberemos analizar si se trata de una conversación telefónica o un correo, o simplemente no es posible asimilarlo a ninguna de las formas preexistentes de comunicación.

11 Véase al respecto ORD. Nº 1140/27 de la Dirección del Trabajo. Disponible en línea [consulta: 05.02.2021].

Complementariamente, otro principio que se desprende de la neutralidad tecnológica es el de **equivalencia normativa**, que busca la eficacia directa e indirecta de las leyes considerando que las relaciones jurídicas se desenvuelven en el contexto de la red internet y por lo tanto, por razones de certeza jurídica, es necesario que los países adopten marcos jurídicos equivalentes.

El tema es especialmente crítico, por ejemplo, en el caso de la firma electrónica en el marco del comercio global, que requiere tener reglas similares o equiparables para asegurar la validez de los documentos firmados electrónicamente en los países de cada una de las partes que intervengan en cada caso.

Esto es especialmente reconocido en la normativa europea de firma electrónica[12] y en la ley modelo de firma electrónica de UNCITRAL.[13] Así, en esta última norma se establece expresamente que uno de los objetivos de la ley es que la firma suscrita en un Estado tenga validez en los demás.

Otro ejemplo relevante lo encontramos en la normativa de delitos informáticos, materia en que dado el carácter transnacional de la red internet, sumado al virtual anonimato de los actores que se desenvuelven en ella, ha llevado a los Estados a plantearse con especial preocupación la necesaria equivalencia de las normas sustantivas y de persecución criminal, a efectos de evitar la impunidad de conductas realizadas a través de medios electrónicos o de telecomunicaciones.

Así se ha reconocido especialmente en el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest, al que Chile adhirió el 21 de abril de 2017) y en protocolos facultativos de la Convención sobre los Derechos del Niño, que buscan establecer mínimos comunes en la tipificación de delitos y en las reglas de persecución y cooperación internacional.

12 A vía ejemplar, el Reglamento Europeo (UE) Nº 910/2014 relativo a la identificación electrónica en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

13 Ley modelo de la CNUDMI sobre firmas electrónicas con la guía para su incorporación al derecho interno 2001.

En lenguaje de principios, opera como norma de clausura: una exigencia de "**mínima intervención**", que llama a ser prudentes al momento de regular los efectos de las tecnologías de la información y las comunicaciones, sobre todo en aquellas materias que la regulación pueda significar una alteración de las categorías jurídicas tradicionales.

Es así como las normas que se dictan debieran ser las estrictamente necesarias para la adecuación del sistema jurídico a las condiciones tecnológicas, pero sin adscribirse a una tecnología específica sino mediante la descripción general de los fenómenos y sus implicancias de relevancia jurídica.

1.3 Regulación jurídica de las redes de comunicaciones electrónicas

1.3.1 Antecedentes generales de la sociedad de la información y su sucesora, la sociedad red

Es muy frecuente el uso de la expresión "sociedad de la información", concepto muy en boga en los años 90 y que, desprovisto de significado, pervive aún hoy (de hecho, lo usaremos en este trabajo más de alguna vez).

Dicha expresión ofrecía una serie de esplendorosas promesas para la humanidad, unidas al auge de la informática y las tecnologías de la información, pero luego del atentado a las torres gemelas en Estados Unidos y la global sobrerreacción de los gobiernos, el futuro ya no es lo que era y las tecnologías para la libertad del ideario de la sociedad de la información, esas que expandirían las libertades públicas y ensancharían los derechos de las personas derribando los prejuicios y las limitaciones al conocimiento, han debido soportar un duro *via crucis* que las alteró en su esencia.

La sociedad de la información ya no existe pues no pudo cumplir sus objetivos, pero ante la disyuntiva de morir prefirió transformarse y hoy, en su lugar, emerge con renovados bríos la **sociedad red**, un modelo social que se levanta sobre una infraestructura de redes de comunicaciones electrónicas abiertas a las personas, las que a su vez ejercen su ciudadanía a través de plataformas sociales interdependientes e interrelacionadas, modificando la forma en que tradicionalmente nos relacionamos con nuestro entorno.

En ese contexto, la referencia a la regulación de las redes de comunicaciones electrónicas dice relación tanto con el marco normativo de las infraestructuras que las componen, como con los servicios que se prestan sobre dichas infraestructuras, pues ambas áreas son consustanciales a la denominada sociedad red, que se caracteriza por los aspectos que se revisan a continuación.

1.3.1.1 La información como eje central de la sociedad

La información y las industrias creadas para su tratamiento son el eje fundamental de la economía y de las relaciones sociales y políticas. Incluso hemos vivido ejemplos dramáticos, que evidencian el alcance que ha tenido este fenómeno. Las manipulaciones políticas y sociales en entornos tales como Estados Unidos y Gran Bretaña evidenciaron la fragilidad de los modelos sociales y políticos tradicionales frente a los gigantes de la información, en este caso Facebook.

1.3.1.2 Convergencia y digitalización

Los servicios antes se diferenciaban por los soportes y tecnologías en las cuales se prestaban, hoy en cambio todos los servicios son digitales y las redes de comunicaciones electrónicas son capaces de contenerlos a todos, por lo que son soportados por las carreteras de información integradas a través de los protocolos desarrollados a los efectos por las áreas técnicas.

1.3.1.3 Desmaterialización aparente

En el sentido de que lo que antes constaba en papel o soportes físicos hoy consta en las redes y servicios de comunicaciones electrónicas. Decimos "aparente" porque no se trata de que los documentos se desmaterialicen, sino que ahora constan en otros soportes distintos del papel o la piedra. Constan en los sistemas de almacenamiento, ocupan espacio y son susceptibles de ser transportados, entre otras características propias de las cosas que existen.

1.3.1.4 Eliminación de fronteras y límites difusos

Las relaciones económicas, jurídicas y sociales se desarrollan en espacios a-geográficos, a través de las redes. Un ejemplo de esto es la pretensión global del RGPD, que regirá en cualquier parte del planeta en que se traten datos personales de residentes europeos.

1.3.1.5 Globalización

Este término abarca una serie de fenómenos económicos, sociales y políticos que se traducen en la circulación transnacional de bienes, capitales, servicios. A vía ejemplar, llamamos a un *call center* de atención de usuarios y nos responden desde otro país, en el cual es horario laboral. O compramos una bicicleta en una tienda chilena, pero el

producto nos llega directamente del fabricante en China a través de los servicios de una naviera panameña, y la bicicleta cumple con los estándares de fabricación de la Unión Europea.

1.3.1.6 Nuevo orden social

En la sociedad red surgen nuevas formas de organización social, tales como las redes de colaboración, redes sociales, etcétera. Como un efecto secundario de este fenómeno, la sociedad se ha vuelto más horizontal, los flujos de información se desarrollan de manera libre y espontánea, no necesariamente sujetos al control editorial de un medio de comunicación.

Esta liberación de la información tiene efectos positivos, en el sentido que genera mayores posibilidades de ejercicio de la libertad de expresión, sin embargo ha traído aparejados riesgos para las democracias, a través de la manipulación del discurso, las noticias falsas, los linchamientos mediáticos y los denominados juicios paralelos.

Asimismo, las redes y servicios que nos ocupan han permitido el surgimiento de nuevos grupos de presión o de intereses, pero asimismo nuevos marginados: los analfabetos tecnológicos.

1.3.1.7 Modificación de los sistemas productivos

Atendido que la información y los servicios que se prestan a partir de ella están en el centro de la economía, se ha producido una valorización de los servicios por sobre la producción de bienes.

1.3.1.8 Modificación de los esquemas sociopolíticos relevantes

Las redes y servicios han devenido en una suerte de sociedad virtual paralela, capaz de generar premios, incentivos y también sanciones (a través de las denominadas "funas virtuales"), sistemas de reclamos, etcétera. Incluso se vislumbra una revelación contra el sistema normado, pues se han empleado en la organización de protestas sociales y también hechos delictivos, tales como atentados terroristas. Incluso el sistema financiero se ha visto afectado, debido al desarrollo del bitcoin y otras monedas virtuales o criptomonedas.

1.3.1.9 Modificaciones en la organización del trabajo

Los sistemas productivos se han visto afectados por las tecnologías de la información y comunicaciones, que conllevan una hiperconectividad de las personas. Los sistemas de producción se han flexibilizado, pues ya no es necesario mantener grandes stocks de productos para una demanda eventual, pues los algoritmos predicen la demanda en cada momento; los mercados productivos se han globalizado e industrias tradicionalmente separadas se han integrado en la producción y distribución de bienes y servicios.

En relación al trabajo, las TIC han obligado a las personas a reinventarse, aprender nuevamente a hacer las cosas, ahora "en digital"; el teletrabajo ha llegado para quedarse y, por qué no decirlo, la automatización ha hecho desaparecer muchos puestos de trabajo, pero también crea constantemente nuevos perfiles de empleo.

1.3.2 Servicio universal de telecomunicaciones y sociedad red

Si las redes y servicios de comunicaciones electrónicas se encuentran en el centro del desarrollo social, parece natural la pretensión de que sus beneficios lleguen a toda la población.

1.3.2.1 Conceptos de servicio y acceso universal a las telecomunicaciones

En los albores de la sociedad de la información (antecesora de la sociedad red), en el ámbito europeo se entendió por servicio universal de telecomunicaciones "... un conjunto mínimo de servicios definidos de una calidad determinada y la prestación de dichos servicios a todos los usuarios, independientemente de su situación geográfica y, a la vista de las condiciones nacionales concretas, a un precio asequible".[14]

Hoy, en cambio, se estima que el servicio universal exige al menos tener una conexión funcional a las redes de comunicaciones electrónicas. Bajo esta premisa, analizaremos aquí los elementos del concepto.

a. La prestación de un conjunto de servicios básicos:

14 COM (93)543 final (Bruselas, 15 de noviembre de 1993); p. 15.

Atendido el vertiginoso avance de las tecnologías, no es posible realizar *a priori* la determinación de los "servicios" que habrán de garantizarse, sino que más bien se prevén métodos a través de los cuales se decidirá sobre la adecuación del catálogo de servicios en cada instante y lugar, conforme al estado de la técnica y la situación económica.

En un comienzo, la aspiración era que en todo lugar estuviera disponible el servicio básico telefónico, sin embargo en el año 2020 quedó claro que lo básico es contar con una conexión a internet que permita estudiar y trabajar con independencia del lugar en que se encuentre la persona, y pese a sus circunstancias económicas.

De ello podemos desprender que los servicios básicos son aquellos que permiten a la persona comunicarse con su entorno, solicitar auxilio y desarrollar sus actividades cotidianas.

b. De una calidad determinada:
La calidad del servicio de que se trate dependerá del estándar técnico generalmente aceptado en el tiempo y lugar de que se trate. Siguiendo la lógica de lo que vimos antes, la determinación del estándar deberá estar impregnado de neutralidad tecnológica, responder a los imperativos de libre competencia y a los derechos de los consumidores.

c. Prestados en condiciones de calidad equivalente:
La calidad mínima debiera garantizarse con independencia de las condiciones geográficas de una localidad determinada.

d. A precios que sean asequibles para los usuarios finales:
Se trata de que los valores que en definitiva se cobren a los usuarios permitan que el mayor número de personas pueda realmente servirse de los servicios provistos a través de las redes de comunicaciones, para satisfacer sus necesidades en los tiempos que corren.

En la otra cara de la moneda de un servicio universal de telecomunicaciones, el análisis desde los usuarios se engloba dentro del concepto de "**acceso universal**" a los servicios de comunicaciones electrónicas "como parte del derecho a comunicarse y la necesidad de que la reglamentación asegure la disponibilidad geográfica universal, la igualdad de trato mediante un acceso no discriminatorio y a un costo accesible".[15]

Desde la óptica del acceso, más que centrarnos en las características del mercado habremos de considerar las necesidades de la persona, ya sea para comunicarse, estudiar, trabajar y entretenerse. El debate en este aspecto dice relación con la posibilidad de elevar este imperativo a la categoría de una garantía individual.

Dicho de otro modo, el *servicio* universal busca desarrollar el mercado de servicios, mientras que el *acceso* universal representa la mirada desde la demanda de servicios de comunicaciones, de manera de procurar que toda persona pueda utilizar algún sistema de telecomunicaciones en condiciones equivalentes, con independencia de sus circunstancias particulares, ya sean de salud, económicas, o geográficas.

1.3.2.2 Normativa internacional

Un hito importante en esta materia es la aprobación por parte del Comité Administrativo de las Naciones Unidas, en 1995, de la Declaración sobre Acceso Universal a las Comunicaciones Básicas y Servicios de Información, elaborada a iniciativa del Secretario General de la Unión Internacional de Telecomunicaciones (UIT).

Más recientemente, los objetivos de desarrollo sostenible de las Naciones Unidas consideran, en su número 9,"construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación".[16] Al respecto, señala que"en términos de infraestructura

15 Véase al respecto el Manual de reglamentación de las telecomunicaciones (itu.int). Disponible en línea [consulta: 22.12.2020].

16 Economic and Social Council. U.N. Progress towards the Sustainable Development Goals. Report of the Secretary General. Disponible en línea [consulta: 22.12.2020].

de comunicaciones, más de la mitad de la población mundial está ahora conectada y casi toda la población global vive en un área con cobertura de red móvil". Al momento de la dictación del documento, se estimaba que a 2019 el 96,5 % de la población tenía cobertura de red, como mínimo 2G.[17]

Sobre las personas a quienes les afecta algún grado de discapacidad, debemos destacar las Normas Uniformes sobre la igualdad de oportunidades para las personas con discapacidad, que en su artículo 5º disponen que "los Estados deben elaborar estrategias para que los servicios de información y documentación sean accesibles a los diferentes grupos con incapacidad", y además "velar porque los nuevos servicios de sistemas y de datos informatizados que se ofrezcan al público en general sean desde un comienzo accesibles a las personas con discapacidad, o se adapten para hacerlos accesibles a ellas".[18]

1.3.2.3 Normativa nacional

En Chile, el servicio universal de telecomunicaciones se ha desarrollado en el Título IV de la Ley Nº 18.168, ley general de telecomunicaciones, a través del Fondo de Desarrollo de las Telecomunicaciones, que busca promover el aumento de la cobertura de los servicios de telecomunicaciones, preferentemente en áreas rurales y urbanas de bajos ingresos. Se trata, por tanto, de generar incentivos y subsidios que permitan mejorar la oferta de servicios en las distintas zonas del país.

El fondo es administrado por un consejo "integrado por el Ministro de Transportes y Telecomunicaciones, quien lo presidirá, y por los Ministros de Economía, Fomento y Reconstrucción; de Hacienda; de Planificación y Cooperación; o sus representantes y por tres profesionales con experiencia en el área de las telecomunicaciones y vinculados a las diversas regiones del país, que serán designados por el Presidente/a de la República" (art. 28 B Ley Nº 18.168).

17 Naciones Unidas, Objetivos de desarrollo sostenible. Disponible en línea [consulta: 22.12.2020].

18 Normas Uniformes sobre la igualdad de oportunidades para las personas con discapacidad. Aprobadas por la Asamblea General de las Naciones Unidas mediante Resolución 48/96, de 20 de diciembre de 1993, en el marco del 48º Periodo de Sesiones.

Conforme al artículo 28 D de la misma ley recién citada, entre los proyectos que se permite financiar se incluyen los siguientes servicios:

a. Teléfonos públicos o centros de llamadas.

b. Telecentros comunitarios de información.

c. Servicios de telecomunicaciones de libre recepción o de radiodifusión locales, cuyas transmisiones están destinadas a la recepción libre y directa por el público en general, sean emisiones sonoras, de televisión abierta o limitada, o de otro género, especialmente los servicios de radiodifusión de mínima cobertura definidos en el inciso segundo de la letra a del artículo 3º de esta ley.

d. Inversiones en sistemas de transmisión e infraestructura para promover el aumento de cobertura de radiodifusión televisiva digital de libre recepción y servicios de acceso a internet, de preferencia en forma simultánea en lugares rurales, insulares o aislados.

e. Cualquier otro servicio de telecomunicaciones que beneficie directamente a la comunidad en la cual habrá de operar.

1.3.2.4 Tipos de servicios de telecomunicaciones

Si bien se estima que la Ley Nº 18.168 en varios aspectos ha caído en obsolescencia, de este cuerpo normativo tomaremos los conceptos que se han establecido para los servicios de telecomunicaciones:

a. Servicios públicos de telecomunicaciones (art. 3º letra b)
Los servicios públicos de telecomunicaciones son aquellos "destinados a satisfacer las necesidades de telecomunicaciones de la comunidad en general", dentro de los cuales destacan los servicios de telefonía fija y móvil, servicio de transmisión de datos, servicios "buscapersonas", servicio de telegrafía pública y servicio móvil a través de repetidora comunitaria. Estos servicios "deberán estar diseñados para interconectarse con otros servicios públicos de telecomunicaciones".

b. Servicios de radiodifusión sonora y televisiva (art. 3º letra a)
En este caso, se trata de servicios "cuyas transmisiones están destinadas a la recepción libre y directa por el público en general". Integran este tipo de servicio las radioemisoras AM o FM y la

"televisión abierta", que podrá ser de carácter nacional, regional, local o comunitaria o de mínima cobertura.

En materia de radiodifusión televisiva regirá principalmente la Ley Nº 18.838, ley general de televisión. Su tutela queda encargada al Consejo Nacional de Televisión e intervendrá la Subsecretaría de Telecomunicaciones en la dictación y aplicación de algunas normas relativas a aspectos técnicos de infraestructura y servicios de base.

c. Servicios limitados de telecomunicaciones (art. 3º letra c)
Se trata de servicios "cuyo objeto es satisfacer necesidades específicas de telecomunicaciones de determinadas empresas, entidades o personas previamente convenidas con estas. Estos servicios pueden comprender servicios de radiodifusión sonora o televisiva y su prestación no podrá dar acceso a tráfico desde o hacia los usuarios de las redes públicas de comunicaciones".

Este es el caso de la televisión por cable que llega a nuestras casas, o del denominado "hilo musical" de establecimientos comerciales o industriales.

d. Servicios de aficionados a las radiocomunicaciones (art. 3º letra d)
Son aquellos destinados a la "intercomunicación radial y la experimentación técnica y científica, llevadas a cabo a título personal y sin fines de lucro".

e. Servicios intermedios de telecomunicaciones (art. 3º letra e)
En este caso se trata de servicios prestados por terceros a través de instalaciones y redes, destinados a satisfacer las necesidades de los concesionarios o permisionarios de telecomunicaciones en general, o a la prestación de servicio telefónica de larga distancia internacional a la comunidad en general.

Dentro de estos servicios cobran relevancia aquellos proveedores que únicamente provean infraestructura física para telecomuni-

caciones. Ellos están en la base de la estructura de provisión de servicios, como podemos apreciar en el siguiente esquema:

Fuente: elaboración propia

El control y aplicación de la normativa de telecomunicaciones corresponde a la Subsecretaría de Telecomunicaciones, dependiente del Ministerio de Transportes y Telecomunicaciones. Sin embargo, durante la vigencia de los estados de excepción constitucional, el todo o parte de las telecomunicaciones podrán estar a cargo del Ministerio de Defensa Nacional.

Asimismo, como señalamos en materia de televisión, las competencias se han radicado en el Consejo Nacional de Televisión (CNTV).

1.4 Garantías fundamentales y tecnologías de la información y la comunicación (TIC)

Desde fines del siglo XIX, las tecnologías han avanzado a pasos agigantados al punto que hoy vivimos en una sociedad informatizada de punta a cabo. Esto ha tenido impacto en el desarrollo de los derechos que los instrumentos internacionales y las constituciones nacionales reconocen a las personas.

Sin pretender hacer un análisis pormenorizado de la historia de los derechos fundamentales, creemos necesario al menos distinguir entre derechos humanos, derechos fundamentales y garantías constitucionales, pues son conceptos básicos a la hora de abordar el tema que nos ocupa.

La historia de los **derechos humanos** es relativamente reciente y se enmarca en la idea de Estado Moderno, en su concepción más amplia, acuñada y teorizada por Maquiavelo y Bodin. Entre sus características destacan la legalidad de la función pública, la pluralidad de los órganos constitucionales, la división de poderes, la justicia constitucional y administrativa, y la consagración de una esfera de libertades.

Producto de este nuevo orden de principios, la persona se reposiciona frente al gobernante, ahora no "sometido" sino "reconocido" como un sujeto con el cual se generan relaciones recíprocas "derecho-deber", entre las cuales se destacan los derechos subjetivos públicos que la persona puede hacer valer en contra del gobernante. Es así como la forma clásica de las declaraciones de derechos de fines del siglo XVIII y principios del XIX consisten en la afirmación de la existencia de los derechos del hombre contra todo absolutismo político, constituyendo por sí mismas un diseño básico de la estructura del Estado.

Los **derechos fundamentales**, en cambio, son derechos subjetivos previamente identificados, en cuanto encuentran reconocimiento en las Constituciones y en la medida en que de este reconocimiento se derive alguna consecuencia jurídica. En todo caso, se entiende por

tales a todos y cada uno de los derechos reconocidos en la norma fundamental (Constitución) y no necesariamente aquellos que se encuentran en el capítulo de garantías fundamentales.

Las **garantías fundamentales** otorgan fuerza constitucional a los derechos individuales así garantizados, a fin de protegerlos incluso contra el legislador y otros poderes del Estado. Visto desde una óptica humanista, los derechos fundamentales son aquellos derechos del hombre (humanos) que el constituyente reconoce, porque existe unconsenso social amplio en cuanto a la necesidad de resguardarlos deuna determinada manera.

Se establece por tanto una relación jurídica entre el ciudadano y el Estado, en el sentido de que al ser reconocidos derechos en la Constitución, estos gozan de permanencia e imprescriptibilidad, además de su tutela judicial y el respeto de su contenido esencial por parte del legislador.

Los instrumentos de control para resguardar el orden en que se sustentan son: el **control de constitucionalidad**, que busca hacer efectivo el principio de primacía constitucional, columna vertebral del Estado democrático de derecho; el **control de legalidad**, dirigido a los órganos aplicadores del derecho, y el **control social**, dirigido a la conducta de los particulares, que entra en funciones cuando se lesiona o se pone en peligro normas básicas de la organización tales como los "derechos humanos", control que corresponde al derecho penal como instrumento garantizador de la convivencia pacífica en una organización establecida.

Esta explicación resulta importante, porque las tecnologías de la información y las comunicaciones han impactado tanto en la concepción de los derechos humanos como de los derechos y garantías fundamentales, en tanto su desarrollo nos ha impuesto analizar la forma como se venían configurando e incluso, en algunos casos, cuestionar su contenido esencial, como veremos más adelante.

Las normas sobre derechos fundamentales sirven como un límite a la aplicación de las tecnologías respecto de las personas, pero también pueden ser la clave de bóveda para propiciar su desarrollo.

1.4.1 Derechos fundamentales. Límite e impulso del desarrollo tecnológico.

En general, en las bases de nuestro ordenamiento jurídico encontramos un conjunto de normas y principios que lo inspiran. Dentro de ellos, los derechos fundamentales expresamente reconocidos, o que se integran por aplicación del bloque de constitucionalidad, son plenamente aplicables a las tecnologías de la información y las comunicaciones. Estimamos que estas normas y principios habrán de interpretarse y aplicarse con sujeción a los valores que moldean la institucionalidad política, social y económica proclamada en la Constitución.

Así, debe entenderse que el propósito perseguido por el constituyente al consagrar una garantía fundamental es reafirmar el derecho protegido para evitar que se impida o perturbe arbitrariamente su ejercicio, en la medida que su titular respete las normas legales que la regulan. En este sentido, entonces, las normas sobre derechos fundamentales sirven como un límite a la aplicación de las tecnologías respecto de las personas, pero también pueden ser la clave de bóveda para propiciar su desarrollo.

Son dos caras de la misma moneda, que trataremos de esbozar en las siguientes páginas.

1.4.2 Los derechos fundamentales reconocidos y su adaptación a la realidad actual

El fenómeno tecnológico, con su aptitud para recolectar, tratar y comunicar grandes volúmenes de información incluso más allá de las fronteras de un país determinado, ha permitido modelar aspectos antes insospechados, tales como la vida, gracias al desarrollo de la investigación genómica que permite diseñar, planificar o incluso extinguir las capacidades humanas de decidir su destino.

Dentro de los beneficios de estas capacidades, cabe destacar que el desarrollo de las tecnologías y al trabajo mancomunado (en red) de muchos científicos hizo posible descifrar el código genético de las personas y con ello descifrar las relaciones filiales y aspectos relativos

con las predisposiciones a ciertos males o enfermedades. Más tarde, en este mismo campo, fue posible descifrar las huellas de ADN que permiten identificar a una persona, haciéndola única e irrepetible.

Estos avances han sido profusamente aplicados para diversas finalidades que impactan los derechos de las personas, siendo reconocidos en nuestro sistema jurídico. Es el caso del reconocimiento de paternidad y la identificación de personas con finalidades de interés criminal.

Otro aspecto relevante es que las actuales sociedades se desarrollan "en red", en el sentido que las distintas plataformas ya se encuentran interconectadas y en condiciones de interoperar (funcionar interconectadas de manera transparente para los usuarios). Ello promueve nuevos desafíos, adicionales a los ya advertidos en la época de la eclosión de la convergencia tecnológica propiciada por la digitalización de las redes y servicios.

Entre dichos desafíos, están aquellos que dicen relación con la protección de la información de las personas que circula, se almacena y/o procesa en esas redes. A este respecto, ha sido necesario configurar y reconocer un nuevo derecho fundamental, el de la protección de los datos personales, como un derecho independiente de otros derechos fundamentales. Así lo ha reconocido la Carta de Derechos Fundamentales de Europa, de 2010, y más recientemente la Constitución chilena, en 2018.

Frente a esto se ha generado todo un movimiento legislativo y doctrinal, tendiente a evidenciar la necesaria relación existente entre el avance de las tecnologías de la información y las comunicaciones en las sociedades modernas y la efectiva protección de las garantías fundamentales.

En los próximos acápites, realizamos una sucinta descripción de la configuración de los derechos fundamentales generalmente reconocidos como susceptibles de verse afectados por el fenómeno informático, a fin de determinar su sentido y alcance y mecanismos de protección ideados por el legislador para garantizar su vigencia efectiva.

Como método de trabajo, y para el solo efecto de ordenar el discurso, seguiremos el orden que ha establecido la Constitución chilena para las garantías fundamentales, antes de hacer referencia a la transparencia, consagrada en las bases de nuestra institucionalidad.

En nuestro análisis nos referiremos a algunos derechos que ya pueden ser considerados como tradicionales, sin que ello signifique que no se reconozca la importancia de los demás, y veremos cómo podrían verse afectados por las TIC y de qué manera su contenido esencial limita y/o modela el desarrollo tecnológico.

1.4.2.1 El derecho a la vida y las TIC

Las tecnologías de la información y la comunicación han impactado la esencia misma de la vida. Al descifrarse el código genético, se ha generado una serie de desarrollos que rayan en una afectación esencial del derecho a la vida, en tanto permiten generar vida humana y seleccionar los "mejores" ejemplares para privilegiarlos con el derecho a desarrollarse en un extremo, pasando por las posibilidades de generar órganos de reemplazo para el caso de requerirlos una persona, o incluso, en el otro extremo, contribuir al término de la existencia humana.

Al respecto, es importante destacar que si bien el desarrollo tecnológico puede alcanzar límites insospechados, las comunidades científicas han propiciado que se adopten acuerdos internacionales para ponerle coto cuando ello entrañe atentar contra la esencia del derecho a la vida.

Es en este sentido que el Convenio de Oviedo (1996) protege la vida embrionaria, prohibiendo el uso de embriones humanos para experimentación, y la Declaración Universal sobre Genoma Humano y Derechos Humanos (1997) fija los principios que deben regir en la investigación genómica, a saber:

a. **Dignidad**, en tanto en este campo se debe procurar siempre la preeminencia del ser humano y la no discriminación.

b. **Libertad**, de la cual deriva el consentimiento libre e información, la protección al vulnerable y el derecho a saber (y a no saber).

c. **Adecuación/razonabilidad**, que impone el establecimiento de protocolos de investigación aprobados por comités ético-científicos, así como mecanismos de reparación de los daños directos producidos por la investigación en la persona y en el principio de confidencialidad.

d. Finalmente el principio de **justicia**, conforme al cual los Estados deben instar a la cooperación científico-cultural y al reconocimiento de las "identidades culturales".

Un tercer instrumento relevante en esta materia es la Declaración sobre Datos Genéticos Humanos, de la Unesco (2003), que precisa los principios de la Declaración de 1997 en relación al uso de los datos genéticos, otorgándoles el carácter de datos sensibles y consagrando los derechos que a su respecto les corresponde a sus titulares:

a. Derecho de **acceso del titular**.

b. **Confidencialidad/reserva/secreto** en cuanto a la identidad del titular de la muestra, la muestra propiamente tal y el consentimiento expreso e informado del afectado por el tratamiento de datos de esta naturaleza, sin perjuicio de establecer excepciones fundadas en un interés público importante, previsto en una ley interna compatible con la legislación internacional de los derechos humanos.

c. **Temporalidad** del almacenamiento.

d. **Exactitud**, **fiabilidad**, **calidad** y **seguridad** de esos datos y del tratamiento de las muestras biológicas.

e. Y finalmente, su tratamiento de acuerdo a la **finalidad**.

Estas normas vienen a complementar la protección que ya habían dado a la vida y a la dignidad humana en la primera generación de derechos, básicamente a través del Código de Núremberg (1947) y la Declaración Universal de Derechos Humanos (1948), y en la segunda generación, con el Pacto Internacional de Derechos Civiles y Políticos (1966), que ya reconocían como derechos humanos que ninguna persona fuera sometida a torturas ni a penas o tratos crueles, inhumanos o degradantes, así como el derecho a que no ser sometido sin su libre consentimiento a experimentos médicos o científicos.

Demás está señalar que la Constitución chilena no se ha adaptado a las nuevas exigencias de protección del derecho a la vida que surgen de la evidente capacidad exponencial de los sistemas tecnológicos. No se ha incorporado a nivel constitucional la protección de la vida embrionaria a cuyo respecto "no se espera que exista", por cuanto no se ha implantado sino que se encuentra en un laboratorio, monitorizado por complejos sistemas de información. Tampoco se ha adoptado una decisión a nivel constitucional respecto de si avanzaremos hacia la creación de vida humana "de diseño", opción claramente posible a través del empleo de estas tecnologías.

1.4.2.2 La igualdad ante la ley

La igualdad fue reconocida en el Pacto Internacional de Derechos Civiles y Políticos (1966) en su artículo 3º, en los términos siguientes: "Los Estados Partes en el presente Pacto se comprometen a garantizar a hombres y mujeres la igualdad en el goce de todos los derechos civiles y políticos enunciados en el presente Pacto". En tanto, la Convención Americana de Derechos Humanos (1969) la reconoce en su artículo 1º como una de las principales obligaciones de los Estados.

En la sociedad red, se advierten ciertas ventajas comparativas de las que gozan aquellos que se han conectado respecto de quienes no. En tal sentido, estimamos por una parte que la actualización de esta garantía fundamental impone que se reconozca el derecho de las personas a acceder a los servicios de este nuevo modelo social, y que se dé un igual trato jurídico a los servicios en línea respecto de aquellos que se prestan en los entornos desconectados, y por otra, que se dé igual trato económico a las actividades en línea respecto de aquellas que se desarrollan por métodos tradicionales.

En la primera de las esferas, en la segunda generación de derechos fundamentales se construyó el servicio universal y acceso universal a las telecomunicaciones, que de acuerdo a lo que postula la Unión Internacional de Telecomunicaciones (UIT), se erigen como manifestaciones expresas del derecho que toda persona tiene a comunicarse, ameritando por tanto la elevación de estos imperativos a la categoría de una garantía individual.

En cuanto a los alcances de la protección, se han mencionado los siguientes:

- Conjunto definido de servicios asequibles a todos los ciudadanos y condicionados por dos aspectos esenciales: a) el estado de la técnica y b) el avance social y económico de una sociedad determinada.
- Otras obligaciones de servicio público complementarias de la institución anterior (guías, números de emergencia, etcétera).
- Implantación de servicios adicionales o complementarios de telecomunicaciones.
- Derecho al uso compartido de infraestructuras de telecomunicaciones, por cuanto, básicamente: a) minimizan el impacto urbanístico y medioambiental de dichas infraestructuras y b) facilitan la introducción de la competencia en el mercado de las telecomunicaciones.

Entre los instrumentos internacionales de derechos humanos que han ayudado a la construcción del servicio y acceso universal, como manifestación de la igualdad ante la ley, aparece la Declaración sobre Acceso Universal a las Comunicaciones Básicas y Servicios de Información, del Comité Administrativo de las Naciones Unidas (1995), que dispone que "los Estados deben velar por que los nuevos servicios de sistemas y de datos informatizados que se ofrezcan al público en general sean desde un comienzo accesibles a las personas con discapacidad, o se adapten para hacerlos accesibles a ellas".

Por una parte, estas garantías imponen a los Estados el no generar beneficios para quienes actúan a través de medios tecnológicos y que rompan el equilibrio de la igualdad ante la ley, pero a la vez el promover aquellos desarrollos e implementaciones tecnológicas que contribuyan a bajar las barreras de la desigualdad. Este último es el caso de aquellas normas que tienden a equiparar las condiciones de las personas con necesidades especiales, las que requieren que los sistemas propios de la sociedad en red contemplen funcionalidades que les ayuden a servirse de sus beneficios, tales como controles de voz para las personas con hipoacusia, o lectores a viva voz de texto en pantalla para las personas ciegas, entre otros.

Lo anterior ha sido reconocido en el artículo 5º de las Normas Uniformes sobre la igualdad de oportunidades para las personas con discapacidad, aprobadas por la Asamblea General de las Naciones Unidas mediante Resolución 48/96, de 20 de diciembre de 1993, durante su 48º Periodo de Sesiones. En ella se acordó que "los Estados deben elaborar estrategias para que los servicios de información y documentación sean accesibles a los diferentes grupos con incapacidad".

En derecho comparado, hoy ya algunos países consagran como garantía fundamental el acceso a internet. Es el caso de Finlandia, Costa Rica y Perú, por mencionar algunos, en los cuales, ya sea por vía de consagración legal o por decisión jurisprudencial, se considera que el acceso a internet merece alcanzar este reconocimiento. En Chile existe actualmente un proyecto de ley que busca este mismo objetivo.

1.4.2.3 Igualdad ante la justicia

La garantía fundamental del artículo 19 Nº 3 de la Constitución se funda en la necesidad de asegurar a todas las personas que tengan iguales posibilidades de defender sus derechos a través de los medios que establece la ley para la resolución de conflictos de intereses de relevancia jurídica.

Cuando abordamos esta garantía desde las tecnologías de la información y las comunicaciones, debemos necesariamente hacer referencia a los siguientes aspectos que integran lo que se ha dado en llamar "e-justicia":

- TIC en apoyo de los procesos asociados al ejercicio de derechos de las partes y a la consulta de sus avances (procesos de información y gestión del conocimiento).
- TIC para la presentación de escritos o notificación de actuaciones (procesos transaccionales).
- TIC para construcción de la verdad procesal (informática forense).
- TIC en apoyo de la ejecución de lo resuelto (herramientas TIC de cumplimiento).

Cada una de las fases tendrá sus complejidades, desde la óptica de los derechos fundamentales, por cuanto las tecnologías empleadas podrían afectar otros derechos, tales como la privacidad o la honra de las personas (por ejemplo, en el caso de la vigilancia telemática de personas durante el proceso o la fase de ejecución de la sentencia, la que debe ser escrupulosamente diseñada e implementada a los efectos de no afectar indebidamente la privacidad, la honra o incluso la salud de las personas).

En lo que nos interesa, en relación a la igualdad en el acceso a la justicia y al debido proceso legal, los principales principios que emanan de esta garantía se señalan a continuación.

a. **Prohibición de toma de decisiones informatizadas**: en general se ha entendido que la facultad de juzgar debe ser ejercida por una persona y no una máquina. En este sentido, se ha cuestionado el desarrollo de sistemas expertos de decisión judicial, no obstante existir consenso en la legitimidad de su empleo en los procesos administrativos relativos a infracciones en las cuales, frente a la constatación de la infracción, procede hacer una aplicación cuasi matemática de la norma correspondiente para determinar la sanción a aplicar.

b. **Bilateralidad de la audiencia**: en este ámbito se traduce en que las partes tengan las mismas posibilidades de intervenir en el proceso, con independencia de si actúan de manera presencial o a través de sistemas tecnológicos. Asimismo, que las partes tengan las posibilidades ciertas de opinar respecto de los antecedentes allegados por la contraria y/o por orden del tribunal.

   A modo de ejemplo, cuando se dictó la ley de firma electrónica en Chile no se advirtió que su texto afectaba este derecho, al no considerar una oportunidad cierta para la percepción de los documentos electrónicos que pudieren ser presentados por las partes. Es por ello que la Ley Nº 20.217 debió modificar el Código de Procedimiento Civil y establecer la audiencia de percepción documental, momento desde el cual empiezan a correr los plazos para impugnar los documentos. Por esta misma razón también, el nuevo texto del artículo 348 de este cuerpo normativo establece que es de carga de la parte que presenta el documento proveer

los medios necesarios para la percepción del documento, y por tanto si no lo hace se tendrá este por no presentado.

c. **Equivalencia funcional:** este principio se manifiesta aquí en el sentido de que en el proceso se considerará el mérito probatorio de los antecedentes allegados a los autos, con independencia del soporte en el cual consten o en el que se hayan generado, en la medida que se resguarde la seguridad, fiabilidad y disponibilidad de esas pruebas, aspectos que se tratan más en profundidad más adelante, en el área de informática forense.

d. **No discriminación:** en lo que nos interesa, destaca la imposibilidad de que los sistemas jurídicos impongan condiciones inequitativas para el acceso al medio tecnológico cuando este represente una mejora en las condiciones de acceso de la persona al circuito judicial. Como ejemplo, a nuestro juicio sería discriminatoria la norma que prescribiese un cobro de dinero como condición para acceder a un sistema de vigilancia telemático en reemplazo de la prisión.

1.4.2.4 El derecho a la educación y libertad de enseñanza

En la línea argumental que venimos sosteniendo, resulta esencial referirnos al derecho a la educación y la libertad de enseñanza, derechos de segunda generación cuyo origen es el Pacto de Derechos Civiles y Políticos (1966).

Este derecho implica que cada niño y joven, con independencia de sus condiciones personales, sociales, económicas o geográficas, debe poder acceder y permanecer en el sistema educativo en los niveles que alcanza su cobertura (educación básica y media). Además, el niño y luego joven tiene derecho a un aprendizaje de calidad y a un trato no discriminatorio acorde con su dignidad humana (respeto) (Unicef-2000).

La educación cumple una función socioeconómica relevante en pos de la superación de la pobreza y el acortamiento de la brecha de desigualdad socioeconómica. Por su parte, la libertad de enseñanza supone la posibilidad de que cualquier persona o grupo de personas

pueda abrir y mantener establecimientos educacionales. En este modelo, el Estado tiene un rol fundamental como promotor y regulador de la actividad educativa.

Ahora bien, una sociedad conectada en red requiere políticas de alfabetización digital que consideren tanto las destrezas necesarias para el manejo de los sistemas de información, como la formación de una "cultura digital" que permee en todas las capas sociales y permita a las personas conocer e internalizar no solo el funcionamiento técnico, sino las implicancias de su desenvolvimiento en la nueva sociedad.

A vía de ejemplo, las personas no solo deben saber cómo utilizar los sistemas y servicios asociados a las redes sociales, sino que además deben ser capaces de comprender las consecuencias de sus actos en dichas redes. Debieran así ser capaces de diferenciar entre las actividades *offline* y *online*. Tal como a nuestros niños les enseñamos a interpretar las señales de advertencia en la vía pública, habrá de transmitírseles las medidas de autocuidado que deben emplear en las redes digitales. Esto es lo que se ha dado en llamar "alfabetización digital".

En segundo lugar, el derecho a la educación se ha visto potenciado en su vertiente "informal" por las redes y servicios de comunicaciones electrónicas, que recogen, administran y ponen a disposición de los usuarios de internet, una gran cantidad de contenidos relevantes, tanto para apoyar los procesos educativos formales como para crear esta cultura digital.

En este aspecto, debemos enfatizar nuevamente la importancia del acceso a las redes (conectividad) como factor esencial para que niños, niñas y adolescentes tengan las posibilidades de acceder a los beneficios de la sociedad en red en materia educativa.

Ahora, en lo que respecta a la libertad de enseñanza, así como toda persona puede fundar colegios, cualquier persona puede acceder a los nuevos servicios para crear y distribuir contenidos educativos, sobre todo sirviéndose de los beneficios de la convergencia tecnológica.

1.4.2.5 Libertad de expresión, derecho a la información y derecho de petición

La libertad de expresión se erigió en su momento como uno de los bastiones de las democracias modernas, en tanto empodera a los ciudadanos frente al Estado. Este derecho, reconocido en el artículo 13 de la Declaración Americana de Derechos del Hombre, en el artículo 19 de la Declaración Universal de Derechos Humanos y en el artículo 8 de la Declaración Universal de la Unesco sobre la Diversidad Cultural, entre otros instrumentos internacionales, hoy se encuentra en el ojo del huracán pues mientras la ciudadanía se abre espacios en internet, los grandes conglomerados de las industrias de información hacen asimismo ingentes esfuerzos para copar este nuevo espacio, haciendo avanzar su poder hacia las redes digitales.

En todo caso, la evidencia demuestra que se han abierto nuevos canales de expresión, con una cobertura y alcance mucho mayor, dada la naturaleza del medio. Este poder social se ha visto reflejado en el interés creciente de los Estados y de las grandes corporaciones para que se regule la red.

Ahora bien, en cuanto a las facilidades para acceder a un medio de expresión en internet, especialmente en su presentación actual (*world wide web*), que se muestra a los usuarios como una planicie donde no es fácil diferenciar y categorizar a cada uno de los oferentes de información, pues aparecen como similares o al menos muy parecidos entre sí, en lo que nos concierne conlleva varias situaciones conflictivas.

Por una parte, basta navegar un poco en la red para advertir su fuerte orientación al consumo de bienes o servicios. Pues bien, las dificultades para diferenciar a los distintos oferentes de productos o servicios impiden al consumidor categorizar adecuadamente sobre las confianzas que cada uno de los oferentes pueda proporcionarles.

Hay personas que no han alcanzado un grado de "madurez digital" y muchas veces terminan aceptando ofertas de bienes o servicios que se le presentan, sin tomar conciencia real de las consecuencias

jurídicas de su actuación. En efecto, la "digitalización" de la relación hace que pierdan el cariz de reales y por tanto no siempre podremos hablar de un consentimiento perfecto de parte del aceptante.

En un segundo punto, en la red encontramos un conjunto descentralizado e inorgánico de información, la que normalmente no está estructurada y menos aún "comentada". Esto hace que el usuario no siempre esté en condiciones de discriminar en cuanto a la calidad de los contenidos que arroja una búsqueda temática.

De esta forma, si bien una cara de la moneda nos lleva a alabar la red como un modelo de democracia participativa, en la que todo quien lo desee puede publicar información, la otra cara nos hace levantar la voz de alarma por cuanto en ella encontramos mucha información "basura" y otra definitivamente errónea, inexacta, ilegítima o incluso ilícita. Nuevamente llamamos la atención aquí en la necesidad de contribuir a generar una cultura digital en los usuarios, que les permita diferenciar la información de buena calidad de la información basura.

Agrava esta situación el entorno gráfico hipertextual de la red, donde una información puede ser presentada ante el usuario como un hipertexto, dotado de enlaces a distintas partes de la red, que añadirán a la sensación veracidad de la información la de ser información muy bien documentada, y a su vez difuminará la responsabilidad por dichas informaciones.

Un tercer aspecto conflictivo relevante dice relación con las facilidades para expresarse de manera anónima en la red. Esta posibilidad también tiene dos caras, pues por un lado las tecnologías facilitan que se difundan las ideas en sociedades donde el temor a la represalia, al terrorismo de Estado o simplemente al más fuerte ha sido una de las principales mordazas, contexto en el que las nuevas tecnologías aparecen como liberadoras. Sin embargo la otra cara nos muestra un laboratorio ideal para la difamación, las teorías conspirativas y otros vicios de los procesos comunicacionales. Más aun, el hipertexto permite descontextualizar la información mediante el enlace de distintos sectores de la red, con la consecuente tergiversación de la realidad.

En este sentido, se habla de contenidos nocivos e ilícitos que son difundidos a través de estos medios, entre los cuales se menciona: a) aquellos que incitan al odio ("*hate speech*"), al desprecio de alguna raza, cultura o grupo determinado por el solo hecho de su pertenencia a dicho grupo; b) contenidos destinados a la apología de ideologías extremas o radicales, tanto en el plano político como religioso, y c) contenidos que desprecian la dignidad humana, tales como la pornografía, información difamante, imágenes distorsionadas o deformes, etcétera.

Estos contenidos en general representan un abuso de la libertad de expresión y quedan en consecuencia prohibidos.

En cuanto al derecho de petición, las tecnologías de la información y las comunicaciones han abierto nuevos canales y nuevos espacios para que los ciudadanos formulen sus requerimientos a los distintos poderes de un Estado y/o una sociedad. Este derecho se relaciona en la sociedad en red con el derecho de reunión, en el sentido de que a veces cientos, o incluso miles de personas, se hacen parte de las redes sociales para organizarse frente a la autoridad cuando esta no cede frente a demandas sociales.

Ahora bien, surge la duda sobre el alcance de estas libertades, en el sentido de que a veces los manifestantes ya no se reúnen en una plaza pública, sino que se citan en una determinada dirección electrónica, a la cual atacarán de manera sistemática como una forma de rechazo a su actuación o simplemente a una persona.

1.4.2.6 Protección a la vida privada y honra de las personas: la inviolabilidad del hogar y de toda forma de comunicación privada y la libertad de conciencia

En la sociedad red, el análisis de estos derechos es especialmente crítico, por cuanto las ingentes capacidades de los sistemas de información y las potencialidades de las redes de telecomunicaciones los amenazan de manera constante y uniforme.

Sin entrar en los conceptos de "vida privada", "honra" o "comunicación privada", que los constitucionalistas han tratado de manera extensa, y en el entendido de que estas no son garantías absolutas, sino que

admiten limitaciones derivadas del interés general o de los derechos de terceros de acceder a información específica respecto de una persona, pondremos el acento en algunos tipos de tecnologías que pueden resultar atentatorias contra estos derechos fundamentales:

- Sistemas de **escucha tecnológica**, que tienden a recoger información desde las redes y otros sistemas de comunicaciones electrónicas, proveniente por ejemplo de las navegaciones web, de la participación de una persona en redes sociales, del empleo de sistemas de telecomunicaciones, entre otros.
- Sistemas de **videovigilancia**, consistente en la captura de imágenes o sonido o ambos, sumado normalmente al procesamiento y almacenamiento de estos registros.
- Sistemas de **control telemático**, que a través de dispositivos y sistemas remotos tienen la capacidad de realizar vigilancia a distancia de personas y/o cosas. Se distinguen aquí dispositivos RFID (por su sigla en inglés), que son dispositivos de identificación por radiofrecuencia; mecanismos de control biométrico tales como lectores de iris, de huella digital o identificador por reconocimiento de voz, y dispositivos GPS, capaces de posicionar a la persona o cosa en tiempo real, para seguir su ubicación y desplazamientos. Este último es el caso de los brazaletes telemáticos de videovigilancia.
- Sistemas de **identificación tecnológica**, tales como sistemas de recogida y análisis de evidencia, por ejemplo de muestras biológicas para su análisis y comparación de huellas de ADN con bases de datos de ADN, con fines de interés criminal como la identificación de víctimas o victimarios de delitos.

Atendida la variedad de sistemas que pueden afectar estos derechos, en nuestro caso fijaremos los límites que se reconocen respecto del desarrollo e implementación de tecnologías en estos ámbitos, a saber:

a. **Razonabilidad.** Reconociendo que puede existir un derecho o interés legítimo en la recogida de información respecto de una persona, el respeto a las garantías fundamentales en comento exige que exista fundamento razonable para la implementación de estas medidas, que las autoridades que las imponen hagan un

tratamiento de las mismas dentro del marco de la finalidad para la que se establecieron, y que se mantengan almacenadas solo el tiempo que sea necesario para cumplir esa finalidad.

b. **Licitud.** El empleo de tecnologías intrusivas debe fundarse en normas jurídicas que regulen la oportunidad, forma y condiciones de las medidas. Por su parte, las autoridades que las impongan y/o apliquen en cada caso concreto, deben estar investidas de las competencias necesarias para realizar estas actividades.

c. **Calidad.** En el sentido de que los procesos y sistemas de tratamiento de esta información deben cumplir exactamente con los imperativos anteriores y, además, garantizar la seguridad de que esta información no será afectada por ataques o por errores o fallas que pueda destruirla, inutilizarla o alterarla. Asimismo, afecta la calidad el que los sistemas no prevean mecanismos de seguridad asociados a los procesos de comunicación de esta información, tales como "sesionización", control de accesos, registro de la información requerida y de aquella que efectivamente se entregó, etcétera.

Como es posible apreciar, los derechos fundamentales que hemos seleccionado, que vienen desde la primera generación de derechos y se remoldearon en la segunda o tercera generación, se han visto impactados por las TIC. Pero esto no es todo, pues como señalamos hay entornos en los cuales se han venido configurando nuevos derechos fundamentales. Tal es el caso de la **protección de datos personales**, como se verá en el acápite siguiente.

1.4.2.7 La privacidad en la sociedad red

El desarrollo progresivo de los derechos humanos se ha sistematizado por la doctrina en las "generaciones", que no son sino diversos estadios de avance del bloque de derechos.

En nuestro análisis anterior, nos hemos referido a algunos derechos y a las amenazas u oportunidades que les afectan y que se originan en las tecnologías de la información y las comunicaciones. Pues bien, hay casos concretos en los cuales existe la convicción de que un hecho

tecnológico afecta la dignidad, la igualdad, o la libertad humana, pero no queda claro que alguna de las categorías tradicionales de derechos humanos se ajuste completamente a su descripción.

Es el caso del tratamiento de datos personales, ámbito en el que existe un consenso bastante amplio sobre derechos (fundamentales y no fundamentales) que se ven afectados por el tratamiento de datos, pero no queda claro cuál es el derecho fundamental al que debe adscribirse.

Si bien en un principio se pensó que la intimidad era el derecho adecuado para radicar la protección de datos personales, hoy queda claro que esto no es efectivo.

Desde 1983, cuando el Tribunal Constitucional alemán se pronuncia respecto de la ley de censo configurando la "autodeterminación informativa" como un derecho autónomo, y más tarde, cuando en 1990 el Tribunal Constitucional español hiciera lo propio bajo la denominación "libertad informática", se han ido configurando las bases de este nuevo derecho, que en definitiva se asienta sobre tres bases concretas:

- El reconocimiento de que las personas a que se refieren o conciernen los datos personales son sus únicos "dueños" y, por ende, la imposibilidad de que los terceros que los recogen, almacenan, y en general, que realizan operaciones de tratamiento, adquieran el dominio de estos datos, sino que a lo más serán sus custodios. Del mayor o menor desarrollo de este eje dependerá el régimen de responsabilidad que se defina en un Estado determinado.
- La convicción de que todo dato personal es relevante y por tanto ha de protegerse respecto de su tratamiento por terceros, distintos de su titular. Esto, sin perjuicio de reconocerse que existen datos más sensibles que otros, como veremos más adelante. El desarrollo de este aspecto conlleva la configuración legal del derecho a tratar datos de terceros y el encasillamiento de cada tipo de dato personal en cada una de las categorías que se definan (datos de libre acceso al público, datos sensibles, etcétera).

Este nuevo derecho ha sido reconocido por las nuevas constituciones en los aspectos antes señalados, haciendo especial énfasis en la necesidad de proteger a la persona titular de los datos contra la actuación abusiva de los terceros que por distintas razones, acceden a sus datos personales.

- La consecuencia necesaria de las dos anteriores: el titular de los datos debe en todo momento poder controlar el uso que terceros hacen de los datos personales que le conciernen. Esta es la base sobre la cual se desarrollan los distintos derechos que se reconocen al titular de datos personales, usualmente conocidos como derechos ARCO, esto es, de Acceso, Rectificación, Cancelación y Oposición al tratamiento de datos personales.

Como se señaló antes, este nuevo derecho ha sido reconocido por las nuevas constituciones en los aspectos antes señalados, haciendo especial énfasis en la necesidad de proteger a la persona titular de los datos contra la actuación abusiva de los terceros que por distintas razones, acceden a sus datos personales.

Protección de datos personales en Chile

← Índice de contenidos

2.1 En torno a la historia y alcances de un derecho

A partir del desarrollo de las técnicas de tratamiento automatizado de la información, ha ido emergiendo un problema: se han evidenciado singulares formas de vulneración de diversos derechos fundamentales de las personas, como la injustificada denegación de créditos, la negativa a contratar seguros de salud, denegación de acceso a determinados colegios, la imposibilidad de arrendar viviendas, y un largo etcétera de sinsabores, con ninguna o pocas posibilidades de identificar las fuentes utilizadas para extraer los datos ni cómo o ante quién defenderse.

La comunidad internacional llamó la atención sobre el fenómeno y en 1981, en el seno de la Comunidad Económica Europea, se suscribió el Convenio Nº 108; más adelante, en 1983, el Tribunal Constitucional alemán[19] se pronunció en relación a la ley del Censo de 1982[20], declarando inconstitucionales algunas de sus normas y estableciendo que las personas tenían el derecho fundamental a la **autodeterminación informativa**, esto es, a controlar qué se hace con los datos personales que le conciernen.

La creación alemana se entiende porque en ese entorno no se considera la privacidad como derecho, como tampoco existe la intimidad en la Ley Fundamental (*Grundgesetz*) de Bonn, pero sí se ampara la dignidad de la persona (1.1) y el libre desarrollo de la personalidad (2.1).[21] Dicha sentencia reconoció que:

19 Todos los fragmentos de la sentencia que en adelante reproduciremos corresponden a la traducción que hizo de la misma Manuel Daranas, publicada en el *Boletín de Jurisprudencia Constitucional* N° 33 de las Cortes Generales, Madrid, 1984, pp. 126 a 170; lo que aparezca encerrado entre corchetes es de los autores.

20 Esta ley, aprobada por unanimidad y sin mayor debate por el *Bundestag*, compelía a responder a las más de 100 preguntas del censo poblacional correspondiente. Dada la entidad y cantidad de las interrogantes, algunos ciudadanos se negaron a responderlas, por lo que el Estado accionó contra ellos, con las consecuencias que se traducen en la referida sentencia.

21 "Todos tienen derecho al libre desarrollo de su personalidad en tanto en cuanto no lesione los derechos ajenos y no contravenga el orden constitucional o las buenas costumbres".

> "En las condiciones de la elaboración moderna de datos, la protección del individuo contra la recogida, almacenamiento, utilización y difusión ilimitada de sus datos personales queda englobada en el derecho general de protección de la persona del artículo 2º, párrafo 1 [*derecho general a la propia personalidad*], en relación con el artículo 1º del párrafo 1 [*protección de la dignidad humana*] de la ley fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y utilización de los datos referentes a su persona".

Con ello se independiza la protección de datos personales respecto de la intimidad, el honor y la propia imagen como garantías protegidas, y se recalca la función instrumental a la protección de la dignidad, la libertad y la igualdad que asiste a la persona humana en general, de la que derivan la generalidad de las garantías consagradas en los distintos catálogos de derechos.

A partir del convenio Nº 108 y de la sentencia antes citada, se marca el inicio de 40 años de desarrollo y consolidación de este derecho a la protección de la persona respecto del tratamiento de sus datos, el que va reflejando los giros legislativos y las experiencias de los países.

En Chile, nuestro Tribunal Constitucional (TCCh) también tuvo ocasión de referirse a la autodeterminación informativa, y lo hizo primero en 2011, señalando que "la protección de la vida privada de las personas guarda una estrecha relación con la protección de los datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa"[22], y que la Ley Nº 19.628 sobre protección de la vida privada era consecuente con este objetivo.

Al mes siguiente, el TCCh sostuvo derechamente que entendía que dicha ley "resguarda lo que se denomina derecho de la autodeterminación informativa. Es decir, se encarga de proteger a las personas de la circulación de la información que sobre ellas mismas existe en

22 Sentencia del Tribunal Constitucional de Chile, de 21 de junio de 2011, recaída en la causa rol Nº 1800-2010.

distintos centros de acopio. Dicho derecho es la dimensión activa del derecho a la vida privada. Mientras la vida privada era concebida clásicamente como la no interferencia ilegítima en la vida personal, se entendía de una manera pasiva. Era el derecho a no ser molestado. El derecho a la autodeterminación, en cambio, "implica controlar los datos que circulan sobre cada uno de nosotros".[23]

Esto se entiende porque en Chile, entre 1999 y 2018, el derecho a la autodeterminación informativa fue recogido por nuestra legislación como parte del derecho constitucional a la vida privada, en la Ley Nº 19.628 de 1999, que se llama a sí misma "de protección de la vida privada".

En la moción que dio lugar a la discusión del proyecto de ley, se dijo: "Sometemos a consideración del Senado un proyecto de ley que viene a llenar un vacío manifiesto en nuestro ordenamiento jurídico y cuyo propósito es dar una adecuada protección al derecho a la privacidad de las personas, en el ámbito del derecho civil, ante a eventuales intromisiones ilegítimas". Asimismo, se señala que "partiendo del precepto contenido en el artículo 19 Nº 4 de nuestra Carta Fundamental, nuestra moción comienza anunciando la inviolabilidad de la vida privada y advirtiendo que toda intromisión en la misma es, en principio, ilegítima".[24]

Sin embargo, y a pesar del discurso, lo cierto es que nuestro ordenamiento jurídico de esa época no tenía respuestas sobre cómo proteger a las personas frente al tratamiento automatizado de sus datos personales.

Como resultado se dictó la Ley Nº 19.628, titulada "sobre protección de la vida privada" aunque en realidad regula el tratamiento de los datos personales, especialmente en relación a la actividad que a esa época desarrollaba Dicom.[25]

23 Sentencia del Tribunal Constitucional de Chile, de 12 de julio de 2011, recaída en la causa rol Nº 1894-2011.
24 Moción del senador Eugenio Cantuarias Larrondo, de 5 de enero de 1993.
25 Dicom, después Dicom-Equifax o solo Equifax, es una empresa con amplia presencia en el mercado de la evaluación de riesgo comercial. En un momento, prácticamente ninguna decisión relativa a personas naturales se tomaba sin consultar a Dicom y solo sucesivas reformas legislativas morigeraron esta situación.

Más recientemente, el 16 de junio de 2018 entró en vigor la Ley Nº 21.096, que modifica la Constitución Política de la República y consagra expresamente el derecho a la protección de datos personales bajo la fórmula siguiente:

> "Artículo 19. La Constitución asegura a todas las personas: (…) 4º. El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley".

Como consecuencia, si bien aún no es ley, en la sesión del Senado que estudia las reformas a la actual Ley Nº 19.628, los legisladores acordaron cambiarle el nombre y pasar a denominarla derechamente "sobre protección de datos personales".[26]

Entonces, si la protección de datos es ahora un derecho fundamental[27], ¿cuál es su contenido? ¿Quiénes son los titulares? ¿Quiénes son los obligados?

Respecto del contenido, y en palabras de Gómez Sánchez, "consiste en un poder de disposición y de control sobre los datos personales quefaculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esosdatos personales para que, pudiendo oponerse a esa posesión o uso".[28]

De acuerdo al artículo 1º de la ley," el tratamiento de datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares se sujetará a las disposiciones de esta ley".

26 Tal decisión está contenida en el Segundo Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento recaído en el proyecto de ley, en primer trámite constitucional, que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, que se tramita a partir de los boletines Nº 11.092-07 y Nº 11.144-07, refundidos.

27 Coincidentemente, también el Reglamento General de Protección de Datos, que había entrado en vigencia el mes anterior, declara que el derecho a la protección de datos personales es un derecho fundamental, aunque sus fundamentos son la Carta de Derechos Fundamentales de la Unión Europea y el Tratado de Funcionamiento de la Unión Europea.

28 Yolanda Gómez Sánchez, *Derechos Fundamentales*, Aranzadi, Cizur Menor, 2018; p. 286.

Los titulares del derecho a la protección de datos son las personas naturales, sean nacionales o extranjeras, mientras que los obligados o sujetos pasivos de la ley son los responsables del tratamiento de datos personales, sean estos, personas naturales o jurídicas, públicas o privadas.

Los titulares del derecho a la protección de datos son las personas naturales, sean nacionales o extranjeras, mientras que los obligados o sujetos pasivos de la ley son los responsables del tratamiento de datos personales, sean estos personas naturales o jurídicas, públicas o privadas.

2.2 Conceptos esenciales: datos personales, tratamiento de datos y registro o banco de datos

A continuación nos referiremos a los conceptos principales de la normativa de protección de datos, los que no solo se entienden desde nuestra realidad sino que su significado es internacionalmente uniforme. Se trata de los conceptos de datos personales, de tratamiento de datos, de registro o banco de datos y de responsables y encargados del tratamiento de datos.

2.2.1 Los datos personales

2.2.1.1 Concepto

En su artículo 2º, el texto de la ley nos indica qué se entiende por datos personales, siendo estos "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables". Se debe destacar, entre los elementos que forman el concepto, que comprende "**cualquier información**", por tanto el concepto es amplio en varios sentidos.

En primer lugar, comprende todo tipo de datos que se refieran a una persona y lo serán con independencia de su naturaleza y forma de representación, ya sea imagen, sonido, o conjunto de caracteres grafológicos, muestras biológicas, etcétera, en la medida que aporten información respecto de una persona y/o que permitan describirla.

En segundo lugar, estos datos refieren a una **persona física o natural**. Por tanto, no se incluye aquellos que aportan información en relación a una persona jurídica. Esta es la tendencia generalmente adoptada por los Estados que entienden que la protección se radica en los atributos de la personalidad, derivado directamente de la dignidad humana.

Finalmente, el concepto restringe la protección a los datos que sean atribuibles a personas "**identificadas o identificables**". Al respecto, las dudas suelen producirse respecto de la expresión "identificable", en el sentido de determinar cuándo considerar que los esfuerzos para llegar a una identificación son tan desmedidos que no resulta

razonable estimar que el dato pueda asociarse a una persona. Sin embargo, no cabe duda que estamos ante datos personales tratándose del número de identificación, o de la combinación de varios datos específicos que entreguen características de la identidad física, fisiológica, psíquica, económica, cultural o social que permita llegar a una persona determinada.

Las reflexiones sobre este punto han transitado desde una visión restrictiva, contenida en el Convenio 108 de la Unión Europea, que disponía que la persona es identificable si "puede ser **fácilmente** identificada; no se incluye al respecto la identificación de personas por métodos complejos", con lo cual se excluía de suyo todo método de carácter científico o técnico de identificación, tal como el análisis de huellas digitales o el procesamiento de imágenes o sonidos.

Pero luego, la Directiva 95/46/CE admitió que la identificación pudiera llevarse a cabo a través de procedimientos más complejos. Es así como en su artículo 2.a, dispuso que se considerará 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".

Hoy, el criterio internacionalmente aplicado es el del Reglamento General de Protección de Datos de Europa (vigente desde 2018), en cuyo artículo 4º número 1 define dato personal como "toda información sobre una persona física identificada o identificable ('el interesado'); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

Los datos sensibles o "especialmente protegidos" incluyen tipos de datos que se caracterizan por referir a aquellas esferas de la personalidad en que, si fueran mal utilizados por terceros, podrían prestarse para discriminaciones ilegales o arbitrarias, o conllevar graves riesgos para el interesado.

2.2.1.2 Categorías de datos personales y sus implicancias desde la óptica de su protección

Existe consenso doctrinario acerca de la inexistencia de datos personales irrelevantes, pues al combinarse los datos podrían entregar información crítica respecto de la persona. Especial interés cobra la elaboración de perfiles de una persona, porque ello podría permitir adoptar decisiones arbitrarias en su contra o incluso manipular la voluntad de esa persona. Hay quienes sostienen que las redes sociales pueden llegar a conocer a la persona mejor de lo que se conoce ella misma, pudiendo modelar los estímulos a los que ella responde para obtener una determinada reacción, ya sea en el ámbito personal, comercial, o incluso político.

Si bien no existen los datos irrelevantes, ello no significa que todos los datos sean iguales o de idéntica categoría. Coincidentemente, nuestra Ley Nº 19.628 reconoce que existen al menos dos categorías de datos personales diferentes: por una parte, los datos personales que podríamos denominar "a secas" y por otra, los datos "sensibles" o especialmente protegidos.

Las definiciones las encontramos en el artículo 2º de la ley, en los términos siguientes:

> "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".

Como podemos apreciar, los datos sensibles o "especialmente protegidos" incluyen tipos de datos que se caracterizan por referir a aquellas esferas de la personalidad en que, si fueran mal utilizados por terceros, podrían prestarse para discriminaciones ilegales o arbitrarias, o conllevar graves riesgos para el interesado.

Respecto de los datos sensibles, el artículo 10 de la Ley Nº 19.628 es enfático: "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".

En el texto vigente de la Ley Nº 19.628, la enumeración de los datos sensibles no es taxativa sino una lista abierta ("tales como…"), por lo que el encuadre de los datos personales en alguna de estas categorías dependerá de la apreciación que realicen los tribunales en cada caso concreto. Perfectamente, podría considerarse por los tribunales que en ciertas circunstancias los datos relativos a personas beneficiarias de programas sociales son datos sensibles, y que por tanto es ilegal la publicación que hacen las municipalidades de listas con nombres y apellidos, exponiendo a las personas a la vergüenza y el escarnio.

Respecto de los datos sensibles, el artículo 10 de la Ley Nº 19.628 es enfático: "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".

Además, a nivel doctrinario se reconoce que quienes se dedican a tratar datos sensibles, ya sea por autorización legislativa o bajo consentimiento del propio titular de los datos, están obligados a tomar todos los resguardos jurídicos, organizativos y técnicos para que ellos solo puedan ser conocidos y utilizados en ámbitos en que su uso sea necesario y aceptable, pero manteniendo siempre medidas de seguridad incluso superiores a otros tipos de datos personales.

Ahora bien, también existe otro tipo de datos que constituyen una categoría especial y no se mencionan como tales, pero contradictoriamente, constituyen el núcleo de la Ley Nº 19.628 y la razón de por qué se dictó la misma. Nos referimos a los "datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial", regulados en el Título III, que establece el régimen aplicable tanto a datos relevantes en procesos de mercadeo como para aquellos necesarios para la determinación de la solvencia patrimonial de las personas.

Finalmente cabe señalar que dentro del universo de datos personales existen algunos que, conforme a los principios y normas de protección de datos, tienen un régimen especial de protección, como son los datos sensibles, y "el carácter 'sensible' de estos datos se funda en que su uso indiscriminado puede traer aparejado que se tomen

decisiones arbitrarias respecto de sus titulares, con el consecuente desmedro de la dignidad humana y las garantías personales que de ella derivan"[29]; es decir, normalmente son aquellos que afectan la esfera más íntima del titular de los mismos o cuya utilización puede dar origen a una discriminación ilegal o arbitraria, o conllevar un riesgo grave para el interesado o titular.

En particular, como ejemplifica la Resolución de Madrid, serán considerados sensibles aquellos datos de carácter personal que puedan revelar aspectos como el origen racial o étnico, las opiniones políticas o las convicciones religiosas o filosóficas, así como los datos relativos a la salud o a la sexualidad. No se trata entonces de un *numerus clausus*, sino que está abierto a cualquier otro tipo de datos que tengan esa capacidad o aptitud para el daño a sus titulares.

Y precisamente, esa es la idea que recoge el artículo 2° de la Ley N° 19.628 al señalar que "para los efectos de esta ley se entenderá por (…) 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".

Para el legislador, esta especial categoría de datos implica que puede y debe establecer garantías adicionales para preservar los derechos de los interesados; de hecho, en Chile y en principio existe una prohibición de tratamiento, aunque la redacción de la misma no es feliz. Señala la ley, en su artículo 10, 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".

29 Lorena Donoso Abarca, "Derechos humanos y derechos fundamentales en la sociedad en red", en *Ciudadanas 2020 II*, al cuidado de Patricia Reyes Olmedo, Instituto Chileno de Derecho y Tecnologías, Santiago de Chile, 2013; p. 94.

Nuestra legislación reconoce los datos sensibles como una categoría especial de datos para luego, inexplicablemente, darle el mismo tratamiento jurídico que a los datos personales no sensibles.

Como se puede apreciar, es solo una prohibición aparente: si se cuenta con el consentimiento de las personas, los datos sensibles igualmente pueden ser tratados. Y la obligación de especial cuidado, o de tomar especiales medidas técnicas y organizativas para cautelar la seguridad de su tratamiento, está presente en la legislación y doctrina internacionales, pero no en nuestra ley.

Es decir, nuestra legislación reconoce los datos sensibles como una categoría especial de datos para luego, inexplicablemente, darle el mismo tratamiento jurídico que a los datos personales no sensibles.

2.2.2 Tratamiento de datos personales

En segundo lugar, el concepto de **tratamiento de datos** u operaciones de tratamiento de datos personales está referido a cualquier operación o conjunto de operaciones, sean o no automatizadas, que se aplique a datos de carácter personal, en especial su recogida, conservación, utilización, revelación o supresión.

De hecho, el artículo 2º de la Ley Nº 19.628 es un poco más descriptivo todavía, al entender que tratamiento de datos es "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizados 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 forma".

Como se ve, la ley no se limita a los tratamientos automatizados de datos personales, sino que además regula los tratamientos manuales de información, como podría ser un sistema de registros llevado por escrito. Adicionalmente, es importante tener en cuenta que la enumeración de operaciones que contienen la ley es meramente enunciativa, por lo que las operaciones que pueden entenderse como tratamiento de datos está abierta a otras actividades, como por ejemplo la publicación de datos personales en páginas o sitios web.

En realidad, la forma de la descripción de actividades que hace nuestra ley no es muy distinta al reglamento europeo ya mencionado, que casi 20 años después define "tratamiento" en su artículo 4º número 2 como "cualquier operación o conjunto de operaciones realizadas

sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

Para nuestros efectos, cobra relevancia la operación de recolección o recogida de datos personales, que comprende las operaciones a través de las cuales el responsable del tratamiento de datos obtiene la información de la persona, ya sea a través de medios directos o indirectos.

Asimismo, cobra relevancia la comunicación de datos que incluyen las operaciones a través de las cuales se da a conocer los datos personales a terceros distintos del titular de los datos, ya sea los originalmente recolectados o los que se hayan producido a través de las operaciones de tratamiento. Por ejemplo, en la consulta al "Dicom" de la persona, se elabora un informe y los datos son informados (comunicados) a la entidad que los requiere dentro de su proceso de evaluación de crédito.

La cesión de datos, en cambio, es la entrega de los datos a terceros, en términos tales que el tercero podrá inyectarlos en sus propios sistemas de tratamiento de datos. Tal es el caso, por ejemplo, de la venta de una base de datos, o la transferencia de una cartera de clientes.

En el apartado relativo a los derechos de las personas, nos referiremos a otras operaciones de tratamiento de datos que resultan relevantes a la hora de enfrentarse a un conflicto de relevancia jurídica asociado al tratamiento de datos.

2.2.3 Registro o banco de datos (art. 2º letra m, Ley Nº 19.628)

Un registro o banco de datos se define como "el conjunto organizado de datos de carácter personal, sea automatizado o no, 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". El RGPD, en su artículo 4º número 6, adoptó la definición que contenía la Directiva Europea 95/46/CE, que consideraba que era

tal "todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido en forma funcional o geográfica".

Como podemos apreciar, cualquiera sea el lado del Atlántico en que nos encontremos, el "registro", "banco de datos" o "fichero" hace referencia a un **conjunto estructurado u organizado de datos, dotado de un sistema lógico de recuperación.**

Ahora bien, el requisito de estructuración cobra relevancia tratándose de bancos de datos manuales, según hace notar el reglamento europeo en su motivación número 15, donde se señala que "a fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento".

En el fondo, si determinada información personal consta en soportes físicos, como hojas de papel, sin que estén sistematizadas o estructuradas de forma alguna y, por ende no permitan hacer recuperación de los datos en ellos contenidos, pues es prácticamente imposible encontrarlos, no sería aplicable la legislación de protección de datos.

2.2.4 Responsable del banco de datos y encargados del tratamiento (art. 2º letra n, Ley Nº 19.628)

En nuestra legislación, se entiende por 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".

Las decisiones a que se refiere el artículo son aquellas relativas a qué información o proceso se desea realizar con los datos personales, y es el gestor del registro o banco de datos quien define la finalidad del mismo.

Cuestión muy diferente es la del "encargado del tratamiento", que es la persona o entidad que define y ejecuta los procedimientos técnicos de gestión de los datos. Si bien en nuestra legislación no se considera de manera expresa, debemos entender que la forma como se reconoce esta figura es a través del reconocimiento de que el tratamiento de datos personales puede realizarse a través de mandatarios, respecto de lo cual la ley dispone lo siguiente:

> "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".

Veamos un ejemplo:

La empresa de retail "X" necesita llevar a cabo operaciones de tratamiento de datos personales de sus clientes, requiere saber sus compras, fechas de pago, despacho de productos, garantías reclamadas, productos devueltos después de la compra, gestión de claves y medios de pago que emplea regularmente. Para ello decide externalizar este servicio, contratando a la empresa de procesamiento de datos "Z", que operará como "procesador" de los datos o "encargado del tratamiento".

De cara al titular de los datos, siempre el responsable del tratamiento será el sujeto obligado a custodiar su información y utilizarla de acuerdo a la finalidad legítima informada, sin perjuicio que las operaciones de tratamiento las haya encargado a la empresa "Z". Lo mismo sucederá con las autoridades de control, quienes le requerirán al encargado de tratamiento el cumplimiento de los deberes legales asociados al tratamiento de datos personales.

2.3 Principios aplicables a la normativa de protección de datos

Atendido el reconocimiento de los avances de la técnica, tanto en Chile como en derecho comparado, las leyes de protección de datos se han estructurado en base a principios y estándares. De hecho, este punto es tan uniforme que las diversas autoridades de protección de datos del mundo se reunieron en la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en Madrid, y redactaron un documento conocido como "Estándares Internacionales sobre Protección de Datos Personales y Privacidad", o **Resolución de Madrid**.

A través de este documento, acordaron incluso una normalización del lenguaje aplicable a las legislaciones (equivalencia normativa) y los principios del tratamiento de datos para garantizar que, en cualquier lugar del planeta, tengan el mismo sentido y alcance. A estos principios nos referiremos en los siguientes acápites.

2.3.1 Principio general de legitimación

En la Resolución de Madrid se reconocen las siguientes condiciones legitimantes del tratamiento de datos personales:

- El consentimiento del interesado: que deberá ser libre, inequívoco e informado.
- Un interés legítimo de la persona que realiza el tratamiento (el "responsable") y que justifique dicha operación, salvo que prevalezcan los intereses, derechos y libertades de los titulares.
- Que el tratamiento sea necesario para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular (los contratos de suministro, por ejemplo, donde hay que saber a quién hay que prestarle determinado servicio y cobrarle por ello).
- Que el tratamiento de datos sea necesario para el cumplimiento de una obligación impuesta por ley.
- Que se trate del legítimo ejercicio de las competencias de un organismo de la administración pública.

— Cuando concurran situaciones excepcionales que pongan en peligro la vida, la salud o la seguridad del titular o interesado o de otra persona, como podría ser el caso de la necesidad de acceder al historial médico de quien ha resultado herido y no puede darse a entender, siendo necesario comprobar que no es alérgico a un determinado medicamento que pretenda suministrársele.

Sintetizando, el principio general de legitimación nos indica que el tratamiento de datos personales solo puede llevarse a cabo si existe el consentimiento del titular de los datos o si una ley lo autoriza. Y no hay más.

Precisamente, estos son los términos del artículo 4° de la Ley N° 19.628, de 1999: "El tratamiento de los datos personales solo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello".

Pero también está presente el principio de legitimación en el artículo 20, cuando la misma ley señala que "el tratamiento de datos personales por parte de un organismo público solo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes".

2.3.2 Principio de lealtad y legalidad

El tratamiento de datos de carácter personal se debe realizar de manera leal y respetando la legislación nacional y los derechos y libertades de las personas. Aunque el sentido de lealtad pudiera aquí resultar ambiguo, la Resolución de Madrid ayuda a determinar ese contenido al señalar expresamente que deben ser considerados desleales aquellos tratamientos de datos y carácter personal que den lugar a discriminaciones injustas o arbitrarias.

Este principio está recogido en nuestra ley en su primer artículo: "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 (…). 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 orde-

namiento 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".

2.3.3 Principio de finalidad

El tratamiento de datos de carácter personal deberá limitarse al cumplimiento de las finalidades legítimas e informadas al titular de los datos y/o las legalmente procedentes.

La Ley Nº 19.628 lo recoge en los siguientes términos:

> "Artículo 9°. Los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público".

Conforme a la ley, las fuentes accesibles al público, son los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes.

Todo esto significa que el responsable del tratamiento no puede llevar a cabo tratamientos incompatibles con las finalidades para las que hubiese recabado los datos de carácter personal, a menos que cuente con el consentimiento expreso del titular (en el texto que se debate, se cambia por "inequívoco") y, podríamos agregar, específico, de forma de privar de valor a declaraciones genéricas de consentimiento tan comunes de ser utilizadas en aplicaciones que descargamos e instalamos en nuestros dispositivos electrónicos.

2.3.4 Proporcionalidad

El tratamiento de datos de carácter personal deberá circunscribirse a aquellos que resulten adecuados, relevantes y no excesivos en relación con las finalidades legítimas e informadas, por lo que los responsables de su tratamiento deberán realizar esfuerzos razonables para limitar al mínimo necesario los datos de carácter personal tratados.

Sin embargo, la Ley Nº 19.628 no fue explícita al recoger este principio, y su existencia solo puede deducirse de la lectura del contenido de la misma, que nunca autoriza el tratamiento indiscriminado de datos personales sino solo de los estrictamente necesarios en relación

a la finalidad declarada de los mismos, estableciendo adicionalmente un deber de eliminación respecto de aquellos datos que no pueda justificarse su almacenamiento.

2.3.5 Calidad

El principio de calidad refiere tanto a los datos personales como a los procesos técnicos y administrativos asociados al tratamiento de los mismos, en todas sus fases. En clave de datos personales, "la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos" (art. 9º Ley Nº 19.628). Así, si los datos de carácter personal han dejado de ser necesarios para el cumplimiento de las finalidades que legitimaron su tratamiento, deberán ser eliminados o convertidos en anónimos.

Veamos un ejemplo:

Adelantando opinión, si los datos personales contenidos en los diarios o periódicos electrónicos han dejado ser necesarios para dar cumplimiento al objetivo de informar a la población, porque los hechos ya han dejado de ser noticia, veremos que esa publicación ha dejado de cumplir con los estándares de protección de datos.

2.3.6 Principio de transparencia

Conforme a este principio, toda persona responsable de tratamientos de datos personales deberá contar con políticas transparentes en lo que a ello se refiere. Además, deberá facilitar a los interesados, esto es a los titulares de los datos personales, la información acerca de su identidad, la finalidad para la que pretende realizar el tratamiento, los destinatarios a los que prevé ceder los datos de carácter personal, y el modo en que los interesados o titulares podrán ejercer los derechos de acceso, rectificación, cancelación o eliminación y oposición (que veremos con más detalle más adelante), así como cualquier otra información necesaria para garantizar el tratamiento leal de dichos datos de carácter personal.

2.3.6.1 Oportunidad

— Si los datos se obtienen directamente del titular, la información deberá ser facilitada en el momento de la recogida.

— Si los datos son obtenidos de terceros: Debe informarse en un plazo prudencial de tiempo, pero puede sustituirse este aviso por medidas alternativas cuando su cumplimiento resulte imposible o exija un esfuerzo desproporcionado.

2.3.6.2 Requisitos

La información no puede limitarse a la firma de una cláusula perdida entre los faldeos de un farragoso contrato tipo, sino que deberá proporcionarse en un lenguaje claro y sencillo; ahora bien, si los datos de carácter personal son recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones de transparencia podrán satisfacerse mediante la publicación de políticas de protección de datos fácilmente accesibles e identificables.

2.3.6.3 Consagración legal en Chile

El principio de transparencia es recogido en el artículo 3º de la Ley Nº 19.628, al proclamar que 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, se debe informar a las personas del carácter obligatorio o facultativo de las respuestas y el propósito para el cual se está solicitando la información.

Como contrapartida, y de acuerdo al artículo 12, toda persona tiene derecho a exigir a quien sea responsable del 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.

2.3.7 Principio de responsabilidad

Quienes tratan datos personales ajenos deben adoptar las medidas necesarias para cumplir con los principios y normas de la legislación, como también dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los titulares de datos como ante las autoridades competentes.

Es decir, no basta con afirmar que se cumple la ley, sino que se debe estar en condiciones de demostrarlo.

Este principio también está recogido por nuestra legislación, particularmente en el artículo 11, cuando señala que "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".

De hecho, la Ley Nº 19.628 establece todo un procedimiento judicial ante tribunales civiles para hacer efectiva la responsabilidad por el incumplimiento de los principios ya reseñados. Sin embargo, la misma ley no prevé que el responsable del tratamiento deba demostrar que ha hecho las cosas bien, sino que sigue las líneas clásicas en lo que se refiere a la carga de la prueba: el demandante debe demostrar la vulneración de las normas, lo que por complejidades tecnológicas y costos de los peritajes, no siempre está al alcance de quienes han sido vulnerados en sus derechos.

2.4 Los deberes de quienes realizan operaciones de tratamiento de datos

Finalmente, la Resolución de Madrid le dedica un acápite especial al tema de la seguridad, señalando que quienes realizan operaciones de tratamiento de datos personales tienen dos importantes deberes respecto de sus operaciones; uno de ellos es el **deber de seguridad**, entendido como el de proteger los datos de carácter personal que se sometan a tratamiento, mediante las medidas técnicas y organizativas que resulten idóneas en cada momento para garantizar la integridad, confidencialidad y disponibilidad de la información.

Esto deriva del hecho de que los responsables realizan operaciones de riesgo con posibles consecuencias negativas para los titulares de los datos, agravadas por el hecho de que muchos de los datos pueden ser de carácter sensible, lo que los obliga a poner especial cuidado en el estado de la técnica y del contexto en que se efectúa el tratamiento, así como de las obligaciones establecidas en las leyes.

Este deber de seguridad implica también informar a los titulares de datos de cualquier infracción de seguridad que pudiese afectar sus derechos patrimoniales o extrapatrimoniales, así como de las medidas adoptadas para su solución.

Ahora bien, la legislación chilena no lo consideró expresamente así, limitándose a señalar en el artículo 11 de la Ley Nº 19.628 que "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". Es por ello que uno de los aspectos medulares de este tipo de juicios es determinar si hubo debida diligencia del responsable del tratamiento de datos.

El tratar datos personales conlleva también, por parte del responsable, el **deber de confidencialidad**, esto es, que quienes intervengan en cualquier fase del tratamiento de datos de carácter personal deberán respetar la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el interesado.

El tratar datos personales conlleva también, por parte del responsable, el deber de confidencialidad, esto es, que quienes intervengan en cualquier fase del tratamiento de datos de carácter personal deberán respetar la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el interesado.

Nuestra legislación lo recoge de la manera siguiente en el artículo 7° de la Ley N°19.628: "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".

2.5 Los derechos de acceso, rectificación, cancelación y oposición (ARCO)

Por influjo de la estandarización normativa internacional, las diversas legislaciones en materia de protección de datos, incluida la chilena, han planteado que los titulares de datos o interesados tienen cuatro tipos de derechos diferentes en lo que a sus datos personales concierne.

Se trata de los derechos de acceso, de rectificación, de cancelación (eliminación) y de oposición, los que debido al acrónimo que se forma con sus respectivas iniciales son internacionalmente conocidos como **derechos ARCO**.[30] Por expresa disposición legal (art. 13 Ley Nº 19.628), no pueden ser limitados por medio de ningún acto o convención, ya que constituyen precisamente el núcleo del derecho fundamental a la protección de datos.

2.5.1 Derecho de acceso

Se ha establecido como derecho primario en materia de protección de datos el derecho de acceso, que implica que el responsable del tratamiento de datos debe proporcionar, cuando así se le solicite, información relativa a los concretos datos de carácter personal objetos de tratamiento, así como al origen de los mismos, las finalidades de los correspondientes tratamientos y los destinatarios o categorías de destinatarios a quienes se comunica o pretende comunicar dichos datos.

Sin embargo, también pesa sobre ellos la obligación de que cualquier información que se proporcione al interesado deba facilitarse de forma inteligible, esto es, empleando para ello un lenguaje claro y sencillo.

30 En la legislación chilena están expresamente consagrados en los artículos 5° y 6° de la Ley N° 19.628, con la particularidad de que no habla del derecho de oposición sino de bloqueo, entendiendo que es lo que procede cuando los datos son inexactos o incompletos: debe negarse la posibilidad de su consulta por terceros hasta obtener certeza respecto de los mismos.

A su turno, la Agencia de Protección de Datos española ha sostenido que este derecho consiste en la facultad o capacidad que se reconoce al afectado de recabar información de sus datos de carácter personal incluidos y tratados en los ficheros automatizados. El acceso podrá consistir en la mera consulta de los ficheros por medio de la visualización, o en la comunicación de los datos pertinentes por escrito, copia o telecopia, certificada o no; en cualquier caso, la información deberá ser legible e inteligible cualquiera sea el medio utilizado.

En nuestro país, el derecho de acceso está regulado en el artículo 12 de la Ley Nº 19.628, que establece que "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".

Adicionalmente, los interesados tienen la facultad de solicitar copia gratuita del registro que se tiene de ellos, pero solo pueden ejercer dicha facultad habiendo transcurrido a lo menos seis meses desde la anterior oportunidad en que hayan invocado y hecho uso de este derecho. Aparentemente, el legislador quiso cautelar también los intereses de quienes realizan operaciones de tratamiento de datos, especialmente de los prestadores de crédito, evitando que se les solicitara documentación gratuita en forma permanente.

Es síntesis, se puede ejercer el derecho de acceso en cualquier momento, el que bien puede satisfacerse por parte de los responsables de tratamiento de datos exhibiendo los datos en una pantalla; en cambio, para solicitar copias gratuitas del registro, deben haber transcurrido a lo menos seis meses desde la última vez que se haya solicitado.

2.5.2 Derecho de rectificación

El derecho de rectificación es el que tiene el titular de los datos para solicitar, a la persona responsable, la rectificación o modificación de aquellos datos de carácter personal que pudieran resultar incompletos o inexactos; es decir, se trata de un derecho emanado del principio de

calidad que obliga al que realiza el tratamiento de datos personales a mantener estos tan completos y actualizados como se requiera conforme a los fines.

En nuestra legislación se contempla en el artículo 12 inciso segundo de la Ley N°19.628, cuando establece que el titular de los datos "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 otras regulaciones particulares que inciden en la materia, como la gratuidad del ejercicio del derecho que ya se mencionara y el deber del responsable de comunicar esta rectificación a todos a quien se le haya entregado tales datos.

En suma, al titular de los datos consignados en registros o bases de datos personales le asiste el derecho de exigir al responsable del tratamiento la enmienda de aquellos datos que resulten inexactos o incompletos; y en todo caso, el responsable del tratamiento no puede exigir contraprestación alguna por realizar las rectificaciones de datos inexactos.

2.5.3 Derecho de cancelación o supresión

El derecho de cancelación otorga la facultad de exigir la eliminación o supresión de los datos de carácter personal que pudieran resultar innecesarios o excesivos, o cuya tenencia carezca del consentimiento del interesado o del fundamento legal que justifique su utilización.

Sin embargo, no procede la cancelación cuando los datos de carácter personal deban ser conservados para el cumplimiento de una obligación impuesta sobre la persona responsable del tratamiento por la legislación, o en su caso, por las relaciones contractuales entre la persona responsable y el interesado, o cuando existiera una obligación de conservar los datos.

No se puede, por ejemplo, entregar datos personales a una casa comercial para obtener un crédito y luego ejercer el derecho de cancelación de los datos, mientras la relación contractual persiste con dicha casa.

La obligación de suprimir datos debe ejercerse por el responsable de *motu proprio*, tan pronto como detecte que el almacenamiento de los mismos carece de fundamento legal, o cuando estuvieren caducos en relación a su finalidad, pues de lo contrario incurrirá en responsabilidad.

Y al igual que respecto del derecho de rectificación, no se podrá exigir contraprestación alguna por parte del responsable cuando un titular lo ejerza; es más, la obligación de suprimir datos debe ejercerse por el responsable de *motu proprio*, tan pronto como detecte que el almacenamiento de los mismos carece de fundamento legal, o cuando estuvieren caducos en relación a su finalidad, pues de lo contrario incurrirá en responsabilidad.

2.5.4 Derecho de oposición

Finalmente, el último de los derechos ARCO es el derecho de oposición, que habilita al titular de los datos a oponerse al tratamiento de sus datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación personal, salvo en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta sobre quien realiza el tratamiento de datos.

Para ilustrarlo con un ejemplo, imaginemos el caso de quien en Chile aparece como deudor en un registro de información crediticia como el Boletín Comercial (llamado desde antiguo "el Peneca verde"), por el no pago de un pagaré, cuando en realidad en los tribunales se está discutiendo la falsificación del pagaré de referencia. Entonces, en el ejercicio de sus derechos, el titular puede *oponerse* y exigir el retiro de la publicación, aduciendo que la información no reúne las necesarias condiciones de certeza, incumpliendo el principio de calidad.

También está contemplado el ejercicio de este derecho para cualquier titular de datos que desee oponerse a decisiones automatizadas que conlleven efectos jurídicos, basadas únicamente en un tratamiento automatizado de datos de carácter personal: un asunto de dignidad humana, si se considera que en el fondo es el juzgamiento de un hombre por una máquina.

En Chile, el derecho de oposición está contemplado en el artículo 3º inciso segundo de la ley sobre protección de la vida privada, aunque en términos ambiguos: "El titular puede oponerse a la utilización de sus datos personales con fines de publicidad, investigación de mercado o encuestas de opinión".

Sin embargo, es en la ley sobre acceso a la información pública (Ley Nº 20.285) donde presenta mayor consistencia, pues en su artículo 20 esta contempla que los organismos públicos, frente a una solicitud de entrega de información que puede afectar derechos de terceros, tienen la obligación de comunicárselo a esos terceros para el eventual ejercicio por parte de estos de "la facultad que les asiste para oponerse a la entrega de los documentos solicitados", entre otras razones, por contener datos de carácter personal.

Existe también en nuestra llamada "ley de protección de datos" la figura del bloqueo, que es una consecuencia del ejercicio del derecho de oposición y consiste en "la suspensión temporal de cualquier operación de tratamiento de los datos almacenados" (art. 2º letra b), operando respecto de los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.

Continuando con el ejemplo de más arriba, el Boletín Comercial puede, ante la impugnación de una información que no reúne los requisitos de calidad dada la falta de certeza (como la disputa judicial sobre la validez del pagaré), bloquear la información hasta que exista una sentencia a firme sobre el punto; no debería cancelarla, dado que su misión legal es, precisamente, dar cuenta de este tipo de asuntos.

2.6 Cambios en el ámbito de los derechos a partir de la entrada en vigencia del RGPD

El panorama internacional de los derechos de las personas en materia de protección de datos, que había sido estable en el tiempo, cambió el 25 de mayo de 2018 con la entrada en vigor del Reglamento General de Protección de Datos (RGPD), que introdujo algunas innovaciones.

La primera de ellas es que el derecho de cancelación de datos, manteniendo su contenido, pasó a llamarse "de supresión", evitando con ello ciertas confusiones con la figura de la cancelación propia del ámbito del derecho civil, que es la constancia que deja el acreedor de un determinado título cuando la deuda ha sido pagada.[31]

Otra innovación fue la incorporación de un nuevo derecho de las personas, como es el "derecho a la portabilidad de los datos", el cual faculta a las personas a exigir a quienes realizan operaciones de tratamiento de datos que les entreguen sus datos personales en un formato estructurado y de uso común, o que los transmitan a otro responsable del tratamiento, bajo determinadas condiciones.[32]

Por supuesto que el RGPD estableció algunos otros derechos en favor de las personas, como el de la limitación del tratamiento en ciertas condiciones especiales, o que las personas no sean objeto de decisiones basadas en tratamientos automatizados[33], pero los

31 Parece algo complejo, pero en realidad es sumamente simple y se da en el día a día de los pequeños comercios que venden "fiado": cuando al final del mes el cliente paga, el comerciante cancela, esto es, tacha o borra del listado de lo que se le debe lo que efectivamente le ha sido pagado.

32 Desde luego, el derecho a la portabilidad de los datos personales no ha sido incorporado a la legislación chilena, pero el Segundo Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, de 16 de marzo de 2020, recaído en el proyecto de ley que se recoge en los boletines Nº 11.092-07 y Nº 11.144-07 (refundidos), establece el derecho a la portabilidad de los datos personales, por el cual el titular de datos tiene derecho a solicitar y recibir una copia de los datos personales que le conciernen, que haya facilitado al responsable, en un formato estructurado, genérico y de uso común, que permita ser operado por distintos sistemas y, a comunicarlos o transferirlos a otro responsable de datos, en determinados supuestos que el proyecto detalla.

33 "El RGPD amplía el catálogo de derechos que la Directiva 95/46/CE reconocía. Dicha ampliación es, por un lado, cuantitativa, puesto que se reconocen explícitamente nuevos derechos; por otro lado también es cualitativa, dado que se intentan adaptar a la realidad digital –con más o menos éxito– tanto los nuevos derechos como los que ya existían", afirma Adrian di Pizzo Chiaccio en *La expansión del derecho al olvido digital*, Atelier, Barcelona, 2018; p. 267.

recién señalados son los fundamentales: portabilidad, rectificación, oposición, supresión y acceso, que en adelante pasan a ser conocidos por el acrónimo que forman sus primeras letras: **derechos PROSA**.

Más que memorizar siglas, es importante tener presente que estas definiciones, principios, derechos y deberes constituyen el núcleo esencial de los estándares internacionales de protección de datos y la amplia generalidad de ellos están presentes en la legislación nacional y, por tanto, tienen la fuerza normativa y exigibilidad prevista para las leyes.

Si bien el reglamento europeo no tiene aplicación directa en Chile, hay al menos dos vías en que incide en nuestro país: la primera de ellas es a través del proyecto de ley de reforma a la Ley Nº 19.628 (boletines refundidos Nº 11.144-07 y Nº 11.092-07), que lo recoge prácticamente en su totalidad; la segunda, a través de contratos y convenios de empresas y organizaciones europeas que hacen entrega de datos personales a empresas e instituciones chilenas, pero obligan contractualmente a estas últimas a cumplir con los principios y normas del RGPD, estableciendo cláusulas indemnizatorias para el caso de que en Europa se establezcan sanciones por operaciones de tratamiento de datos que incumplan el reglamento y hayan sido realizadas por las empresas chilenas a las cuales se les entregó datos personales de ciudadanos europeos.

Hay un argumento adicional sobre por qué para Chile es relevante el Reglamento General de Protección de Datos de Europa: nuestro país suscribió un tratado internacional vigente llamado "Acuerdo por el que se establece una Asociación entre la Comunidad Europea y sus Estados miembros, por una parte, y la República de Chile, por otra"[34], cuyo artículo 202 dice textualmente: "Las Partes acuerdan otorgar un elevado nivel de protección al procesamiento de datos personales y de otra índole, compatible con las más altas normas internacionales".

34 Decreto N°28 de 2003 del Ministerio de Relaciones Exteriores, publicado en el Diario Oficial el 1 de febrero de 2003.

¿Cuál es la más alta norma internacional en la materia? El Reglamento General de Protección de Datos que entró a regir el 25 de mayo de 2018, aplicable directamente a Europa y exigible a los países que han obtenido el reconocimiento de país con un nivel adecuado de protección de datos, como Argentina, Canadá, Israel, Japón, Nueva Zelanda y Uruguay; es decir, a partir del año 2018 los estándares deben encontrarse en la lectura del RGPD, pues así reza el acuerdo de nuestro país con la entonces Comunidad Europea, hoy Unión Europea.

Adicionalmente, en derecho comparado se especifican y desarrollan otros derechos, que están siendo considerados en el proyecto de ley de adecuación de nuestra actual legislación y revisaremos en los siguientes acápites.

2.6.1 Derecho de oposición

Si bien la ley vigente no distingue expresamente este derecho, lo esboza con motivo de la cancelación de datos personales, en cuanto a la manifestación de voluntad del titular de no continuar figurando en un banco de datos al cual proporcionó su información de manera voluntaria.

En el RGPD este derecho se regula en su artículo 21. Si bien las hipótesis dicen relación a algunas de las causales previstas en Chile, se agrega la posibilidad de oponerse a la elaboración de perfiles, definidos estos últimos como "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física" (artículo 4 numeral 4 RGPD).

2.6.2 Derecho a no ser objeto de decisiones automatizadas

El reglamento europeo pone especial atención en este aspecto, regulado en el artículo 22. Al respecto, y en lo que nos interesa, se exime de la prohibición cuando la decisión sea necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable de tratamiento, como podría ser el caso del contrato de trabajo.

2.6.3 Derecho a la limitación del tratamiento (derecho de bloqueo de los datos personales)

Regulado en el artículo 18 del RGPD, sus hipótesis se relacionan con el derecho de supresión o cancelación, previéndose que en el tiempo intermedio entre la solicitud y la resolución de procedencia, los datos personales no puedan ser objeto de tratamiento.

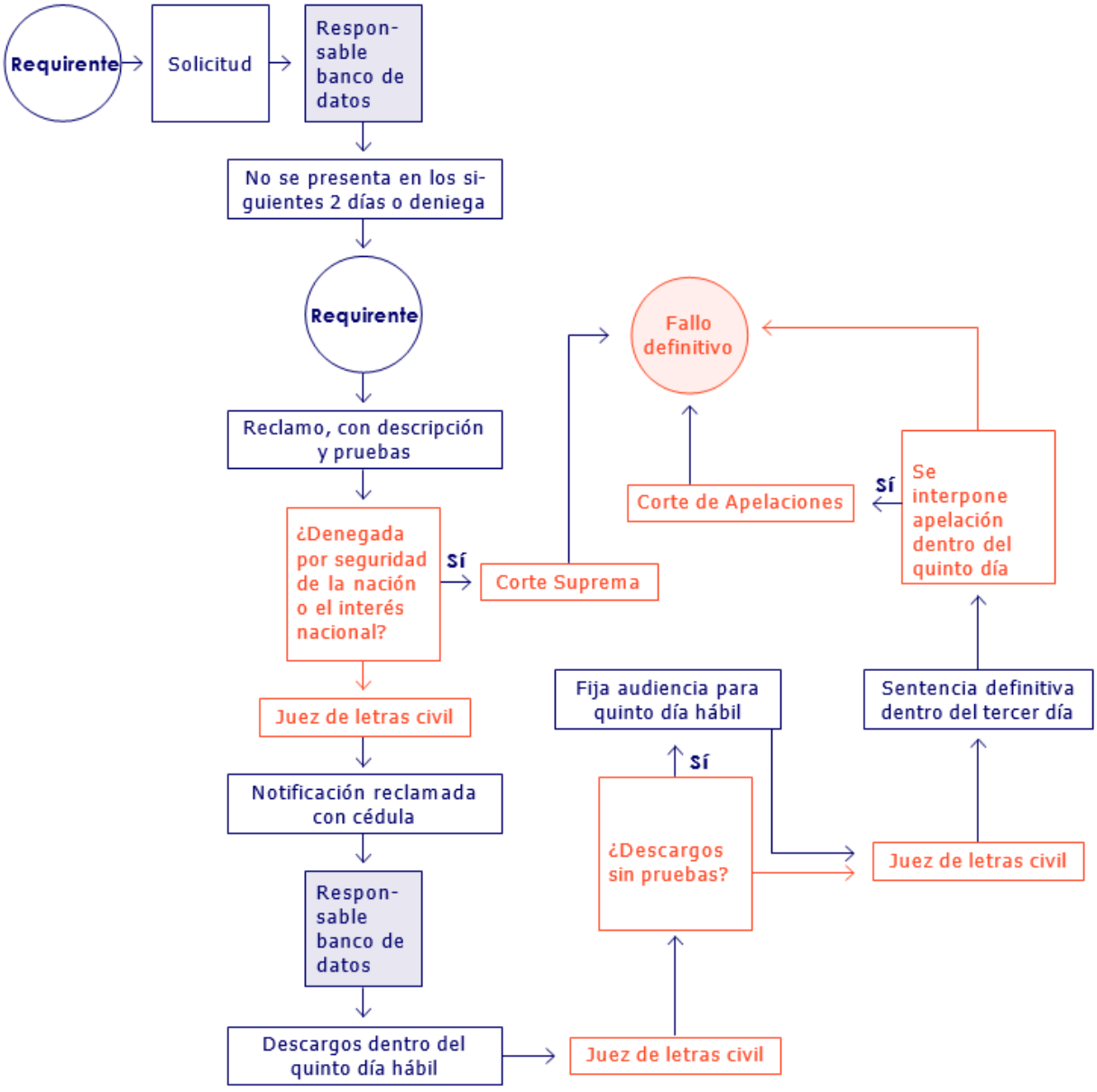
2.6.4 Derecho a la portabilidad de los datos personales

Tratándose de aquellos casos en que el titular deba trasladar los datos a otro responsable de registro o banco de datos.

2.7 El procedimiento de *habeas data* en la jurisprudencia civil

La ley de protección de datos estableció como mecanismo de tutela efectiva la acción de *habeas data*, basada en el recurso de protección, pero que fue radicada en los tribunales civiles. La tramitación de esta acción se encuentra regulada en el artículo 16 de la Ley Nº 19.628.

En el siguiente esquema se puede apreciar su tramitación:



Si el titular del registro o banco de datos no responde dentro de ese plazo, la respuesta resulta insatisfactoria o se deniega la solicitud, la persona podrá entablar el *habeas data*.

Como podemos apreciar, el requirente presenta su solicitud al responsable del banco de datos, quien tiene dos días hábiles para responder a la solicitud (ejercicio de los derechos de acceso, rectificación, cancelación, bloqueo u oposición). Si el titular del registro o banco de datos no responde dentro de ese plazo, la respuesta resulta insatisfactoria o se deniega la solicitud, la persona podrá entablar el *habeas data*.

Para determinar cuál es el tribunal competente para ello, habrá de analizarse si la causal de denegatoria adujo la seguridad de la nación, interés nacional u otra causa.

En caso de que la causal de denegatoria no fuera una de las antes señaladas, el tribunal competente será el juzgado de letras en lo civil del domicilio del responsable del banco de datos, el que se encuentre de turno según las reglas correspondientes. Se ha criticado esta regla, por cuanto agrega una carga al demandante al exigirle que se dirija al tribunal del domicilio del demandado, en circunstancias de que resultaría más apropiado, desde la óptica de garantizar la titula efectiva, que la persona pudiera elegir si dirigirse al tribunal de su domicilio o al del demandado.

En este caso, el procedimiento será el siguiente:

a. Relación de los hechos, la infracción cometida y acompañamiento de los medios de prueba que los acrediten, en su caso. Esta exigencia se ha criticado por las dificultades que entraña que el afectado por el tratamiento de datos personales cuente con los medios de prueba que le permitan acreditar los hechos en que se basa la infracción que se imputa al responsable del banco de datos, sobre todo si consideramos que en muchos casos se trata de datos, programas y sistemas que se encuentran en poder del demandado. Ello, máxime si se considera las facilidades que se otorgan al demandado como se podrá apreciar a continuación.

b. Luego, el tribunal dispondrá que se notifique por cédula al responsable del banco de datos correspondiente, quien deberá presentar sus descargos dentro de quinto día hábil.

c. A diferencia del demandante, al demandado se le reconoce la opción de presentar las pruebas que acreditan los hechos que esgrima en su libelo conjuntamente con este, o alegar que no dispone de ellos y, en ese caso, el tribunal fijará una audiencia para dentro del quinto día hábil a fin de recibir la prueba ofrecida y no acompañada.

d. La sentencia definitiva deberá dictarse dentro de tercero día desde que haya vencido el plazo para oponer descargos, en caso de que el demandado nada diga, o una vez vencido el plazo de prueba, en caso que se haya decretado audiencia de prueba.

e. La sentencia definitiva será apelable en ambos efectos, debiendo interponerse dentro del término de 5 días contados desde la notificación por cédula de la sentencia a la parte que lo entabla, y deberá contener los fundamentos de hecho y de derecho en que se apoya y las peticiones concretas que se formulan.

f. Deducida la apelación, los autos serán elevados de inmediato a la Corte de Apelaciones respectiva, quien conocerá en cuenta, gozando de preferencia y sin esperar la comparecencia de ninguna de las partes.

g. El fallo dictado en apelación no será susceptible del recurso de casación.

Si la causal invocada fuera seguridad de la nación o interés nacional, el tribunal competente será la Corte Suprema y se sujetará al siguiente procedimiento:

a. Recibida la acción, la Corte solicitará informe al recurrido fijándole un plazo al efecto, transcurrido el cual resolverá en cuenta la controversia.

b. 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.

c. La Corte Suprema conocerá en sala en primera instancia, pudiendo deducirse apelación ante la Corte de Apelaciones, la cual asimismo se conocerá en sala.

d. La sala de una u otra instancia 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 sala de que se trate. La audiencia respectiva tendrá el carácter de reservada.

2.8 El régimen infraccional en la Ley Nº 19.268

De acuerdo a la ley, el titular del registro o banco de datos deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquearlos de acuerdo a lo requerido por el titular de los datos que se sienta afectado por el tratamiento indebido o, en su caso, por lo ordenado por el tribunal.[35]

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 de la ley, 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.[36]

El monto de la indemnización será establecido prudencialmente por el juez, considerando las circunstancias del caso y la gravedad de los hechos.[37] En tal sentido la jurisprudencia ha establecido indemnizaciones del daño moral a los titulares de datos en montos de fluctúan entre un mínimo de $5.000.000[38] a $7.000.000[39], con una media de $25.000.000[40] y un máximo de $70.000.000[41] por cada persona afectada.

35 Cfr. Ley Nº 19.628, artículo 23.
36 Ídem.
37 Ídem.
38 "A.V.A. con Supermercado CENCOSUD", rol N° C-22.197-2007, 14° Juzgado Civil de Santiago, confirmado por la Corte de Apelaciones de Santiago, rol de ingreso N° C-6742-2010. Inexistencia de transacción comercial, falta de diligencia o cuidado en la verificación de identidad del tarjetahabiente.
39 "C.U.F. con Corpbanca", Excma. Corte Suprema 2005. Juicio por negación de crédito hipotecario preaprobado, el daño moral causado por violación a la buena fe en la etapa precontractual.
40 Excma. Corte Suprema, rol N° 3901-2005, autos "L.I.H.B. con CMR Falabella S.A.", publicación indebida de un pagaré en base de datos, acoge demanda, resolvió: "Se acoge la demanda de indemnización de perjuicios por $25.000.000.- por concepto de daño moral".
41 "R.S.H. con Corpbanca", Excma. Corte Suprema, rol N° 587-2009. Negación de crédito aduciendo deuda inexistente.

Adicionalmente, de acogerse la reclamación en sede de *habeas data*, la sentencia:

- Fijará un plazo prudencial para dar cumplimiento a lo resuelto.
- Podrá aplicar una multa de 1 a 10 Unidades Tributarias Mensuales (UTM), en forma genérica, por cualquier infracción a la Ley Nº 19.628 y la Ley Nº 20.575.
- Podrá aplicar una multa de 10 a 50 UTM si la infracción es cometida a lo dispuesto en el artículo 17, es decir, sobre datos patrimoniales de naturaleza económica, financiera, bancaria o comercial de acceso restringido para el comercio establecido, con la finalidad del proceso de crédito, y las entidades que participen de la evaluación de riesgo comercial para el fin de evaluación de riesgo comercial; o al artículo 18, es decir, por comunicar datos del artículo 17 luego de transcurridos 5 años desde que la obligación se hizo exigible o después de haber sido pagada o haberse extinguido por otro modo legal; sin perjuicio de la comunicación a los tribunales de justicia de la información que requieran con motivos de juicios pendientes. (Estos artículos se refieren al tratamiento de datos de carácter económico, bancario, financiero y comercial.)

El artículo 16 de la Ley 19.628, agrega además, una infracción por el incumplimiento de lo ordenado por el tribunal, en el inciso final, que dispone:

> "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".

2.9 La acción de protección del derecho a la protección de datos personales

La Ley Nº 21.096, de artículo único y publicada el 16 de junio de 2018, introdujo con un par de líneas una sustancial reforma a la Constitución Política de la República, estableciendo que esta asegura a todas las personas "la protección de sus datos personales".

A continuación indica que el tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley, pero esa ley ya estaba dictada desde el año 1999, cual es la Ley Nº 19.628. Es decir, el contenido de este nuevo derecho constitucional debemos encontrarlo no directamente en la Constitución, sino que por expresa remisión de la misma en la Ley Nº 19.628, cuyo contenido ya hemos revisado.

Lo anterior implica que, al momento de entrar a conocer una acción de protección por privación, perturbación o amenaza al derecho a la protección de datos personales, los jueces de la instancia deben asumir que el pleno respeto de la garantía constitucional pasa por verificar la efectiva no vulneración de los principios establecidos en la señalada ley, así como el efectivo respeto de los derechos de acceso, rectificación, cancelación y oposición en el marco del tratamiento de datos personales.

A nuestro parecer, el legislador no fue especialmente cuidadoso al compatibilizar las diferentes acciones judiciales que contempla nuestro sistema jurídico ante la vulneración del derecho a la protección de datos: a partir del año 2018 se puede accionar de protección ante los tribunales superiores de justicia, pero, por los mismos hechos, también es posible recurrir al procedimiento especial ante los tribunales civiles de primera instancia.

Por supuesto, si una persona se siente agraviada por la vulneración de sus derechos fundamentales puede solicitar el amparo constitucional de los mismos, lo que generará un procedimiento rápido y expedito, cuestión que ordinariamente no ocurrirá si plantea el problema ante los tribunales civiles.

De hecho, procesalmente podría resultar ventajoso nunca utilizar el procedimiento de *habeas data* de la Ley Nº 19.628, sino obtener rápidamente una sentencia favorable vía acción de amparo y luego iniciar un procedimiento ordinario de indemnización de perjuicios, utilizando la sentencia de las Cortes como prueba irrefutable de que la vulneración del derecho ha ocurrido, limitándose el juicio a acreditar el monto del perjuicio.

Como se recordará, en un procedimiento de *habeas data* ante los tribunales civiles el demandante debe probar todos los hechos, pero en una acción de protección el actor solo debe probar que la vulneración ha ocurrido, siendo de cargo del recurrido el demostrar a través de un informe que ello no es así o que no le es imputable.

Bajo ese predicamento, en la generalidad de los casos acudir a un procedimiento de *habeas data* de la Ley Nº 19.628 carecerá de sentido.

Criminalidad informática

← Índice de contenidos

3.1 Los problemas de la falta de tipificación y su incorporación en leyes extravagantes

Las tecnologías de la información y la comunicación han planteado desafíos en todos los ámbitos. Tratándose del ámbito penal, ingente ha sido la discusión en cuanto a la adaptación de las figuras delictivas tradicionales a los denominados delitos tecnológicos, sobre todo considerando que conforme a la normativa penal, debe producirse una subsunción exacta de la conducta en la norma penal para que recién se pueda sostener que estamos en presencia de un "hecho que reviste carácter de delito", que autorice su investigación.

Esta precisión reviste especial interés, por cuanto la rapidez del avance tecnológico nos impone un especial cuidado al momento de redactar las normas sustantivas, de forma tal que los preceptos que en definitiva sean aprobados no contengan fórmulas excesivamente particulares y/o condicionadas a una tecnología específica, conforme a lo que se planteó sobre neutralidad tecnológica.

En el ámbito penal, se han visualizado ilícitos penales en que la informática es objeto del delito, y otros en que el medio comisivo supone el uso o abuso de medios informáticos.

Las principales normas en Chile son la Ley Nº 19.223; la Ley Nº 20.009, de clonación de tarjetas mercantiles; la Ley Nº 17.336, de propiedad intelectual, en que se tipifican los delitos de piratería informática, y el Código Penal, respecto de los delitos de pornografía infantil.

Sin embargo, la persecución efectiva de estas conductas se ha visto afectada, en un primer momento por la falta de normativa y más tarde por deficiencias de la Ley Nº 19.223 y por la dispersión normativa, al tratarse esta de una ley extravagante respecto del Código Penal.

3.2 Directrices político-criminales

La doctrina ha sido especialmente cuidadosa al momento de pronunciarse acerca del tratamiento que se debe dar a los delitos cometidos mediante el uso de una computadora. De lo que no cabe duda, es acerca de la necesidad de estudiar la adecuación del derecho penal a estas nuevas tecnologías, en aras, por cierto, de la protección de bienes jurídicos esenciales para la comunidad.

Una especial dificultad en esta materia dice relación con la velocidad del avance de las tecnologías, que dificultan al derecho mantenerse "a la altura de las circunstancias", cuestión especialmente relevante en materia penal, donde no hay delito ni pena sin una ley previa que lo establezca. Es así como, a vía ejemplar, el profesor Miguel Ángel Davara sostiene que antes de la dictación del Código Penal de 1995, en España no existía el delito informático.[42]

Una especial dificultad en esta materia dice relación con la velocidad del avance de las tecnologías, que dificultan al derecho mantenerse "a la altura de las circunstancias", cuestión especialmente relevante en materia penal, donde no hay delito ni pena sin una ley previa que lo establezca.

Si bien en Chile optamos por dictar dos leyes especiales, la Nº 19.223 y la Nº 20.009, en un enfoque diferente se ha planteado la posibilidad de analizar las figuras penales tradicionales y, en aquellos casos que sea necesario, introducirles las modificaciones que les permita adecuarse a las nuevas tecnologías. Esto es lo que hizo, en parte, el legislador español en 1995, cuando optó por revisar y adaptar los delitos contenidos en su Código Penal; o la solución adoptada por Francia, que optó por la introducción de un nuevo título en el Código Penal.

Bajo este enfoque, propio de una mínima intervención, solo se crearán nuevos tipos penales en aquellos casos en que los tipos tradicionales, ni siquiera con adaptaciones, sean capaces de incluir las nuevas conductas.

42 DAVARA, Miguel Ángel, *Derecho Informático*, Ed. Aranzadi, 1993.

Adicionalmente, se ha criticado a la ley chilena por haber optado por una óptica fenomenológica, según algunos incurriendo en un excesivo casuismo que impediría la adecuación del tipo a nuevos avances hoy quizás inimaginables.

Otras problemáticas que han debido enfrentarse al momento de tomar decisiones criminológicas a este respecto son aquellas derivadas del principio de oportunidad, en cuanto hay conductas cuya lesividad no justifica el empleo de un medio tan gravoso como el derecho penal. Tal es el caso, por ejemplo, del llamado "hurto de uso de computador"[43], ya que atendida la masificación del uso de estas máquinas, la velocidad de proceso y el bajo costo que hoy día tienen en el mercado, hace irrelevante para el titular del sistema informático el menoscabo patrimonial que lleva ínsito, no obstante hace algunos años este perjuicio representaba límites muy superiores.

Adicionalmente, en relación al principio de oportunidad, se ha criticado la aplicación efectiva de la ley por la enorme cifra negra que hay en la persecución de estos delitos, principalmente debido a las dificultades para su detección y prueba, a lo que se suma la reticencia del afectado a denunciar el hecho.

43 En tal sentido, véase PÉREZ-LUÑO, Antonio E., *Manual de informática y derecho*, Ed. Ariel, Barcelona, 1996; p. 73.

3.3 El bien jurídico protegido y las características comunes a este tipo de delitos

Existen opiniones divididas en cuanto al bien jurídico protegido en los delitos relacionados con la informática. Prima la posición que entiende este tipo de ilícitos como pluriofensivos, en el sentido de que en cada una de las figuras pueden verse afectado diversos y múltiples bienes jurídicos. Esto es lo que le da a este fenómeno su carácter macrosocial.

A mayor abundamiento, debemos considerar que en cada uno de los delitos se verá afectada tanto la información propiamente tal, pues como vimos antes las hipótesis comisivas incluyen alteraciones, daños o pérdidas de información, y adicionalmente podrán verse afectados los bienes jurídicos asociados a los ámbitos a que dichas informaciones se refieren, entre los cuales el que ha tenido mayor impacto social es el patrimonio.

No obstante lo anterior, parte de la doctrina ha pretendido identificar en estos delitos un bien jurídico general, tales como el "orden público económico", que incluiría a la fiabilidad del sistema financiero y seguridad en el tráfico económico, o como en el caso de la legislación chilena, en que el legislador declaró que en la Ley Nº 19.223 se está protegiendo un nuevo bien jurídico protegido: "la pureza e idoneidad de la información contenida en un sistema de tratamiento de la información".

Esto es coincidente con parte de la doctrina que estima que la correcta operación de los sistemas informáticos y la fe colectiva que rodea a su correcto funcionamiento es un bien jurídico digno de protección penal en la sociedad red. En este sentido se pronuncia Reyna: "Así podemos decir que el interés social digno de tutela penal sería: La información almacenada, tratada y transmitida a través de sistemas informáticos, como valor económico de la actividad de la empresa". [44]

44 REYNA ALFARO, Luis Miguel, *Los delitos informáticos: aspectos criminológicos, dogmáticos y de política criminal*, Jurista Ed., Lima, 2002; pp. 238–239.

Desde este punto de vista, el autor concibe los delitos informáticos como un delito socioeconómico y al bien jurídico protegido como colectivo, lo cual no obsta para que estas acciones "puedan afectar además intereses patrimoniales individuales", dado que "el bien jurídico propuesto está dirigido a resguardar intereses colectivos, cercanamente relacionados al orden público económico, aunque puedan concurrir a su vez intereses individuales (...)".

En cambio, los países que han optado por actualizar su legislación penal no han alterado la estructura de bienes jurídicos protegidos que ya contenían sus normativas penales, lo que ha facilitado la aplicación de estas normas por parte de los tribunales de justicia. En este enfoque, a continuación nos referiremos al concepto y tipología de delitos informáticos.

Por nuestra parte, estimamos que la real novedad de estos tipos de delitos no está en el bien jurídico protegido sino en el medio comisivo –las TIC y sus potencialidades como "instrumento" que se utiliza para perpetrar el ilícito–, mientras que el bien jurídico protegido en cada caso será el que corresponda a la naturaleza de la infracción cometida, de acuerdo a los bienes jurídicos tradicionales.

En aquellos casos en que los medios informáticos sean el "objeto" de estos ilícitos, la propiedad podrá verse afectada, ya sea sobre el medio informático o la que recaiga sobre la información contenida en dicho sistema y, en consecuencia, habrán de efectuarse las valoraciones que sean del caso para su avaluación.

En otros casos, podrá verse afectada la privacidad cuando se produzcan intromisiones ilegítimas que expongan datos calificados como "privados", etcétera. Con ello queremos evidenciar nuestra posición en el sentido de que no es efectivo que exista un bien jurídico nuevo, sino un *riesgo* nuevo de afectación a los bienes jurídicos tradicionales, básicamente por la importancia que ha adquirido en la sociedad actual el tratamiento de la información a través de sistemas informáticos.

Siguiendo este razonamiento, parte de la doctrina sostiene que no es acertado señalar, como bien jurídico que se protege con la tipificación de un delito informático, la "pureza e idoneidad de la información

contenida en un sistema de tratamiento automatizado". Fundan su opinión en que, más que el bien jurídico protegido, la información y los sistemas automatizados de tratamiento son el objeto específico de estas conductas.

Es así como, si atendemos al bien jurídico protegido en cada caso, primeramente veremos que habrá a) delitos contra la intimidad de las personas (acceso indebido a la información); b) delitos contra la propiedad y el patrimonio (falsificación de documentos privados electrónicos y de tarjetas de crédito, débito o pago, fraude informático, obtención indebida de servicios de telecomunicaciones, daño a datos o programas informáticos, obstaculización del funcionamiento de sistemas de tratamiento automatizado de la información), y c) delitos contra la fe pública y la fe mercantil (delito de falsificación de instrumentos públicos electrónicos, forjamiento de cheques y tarjetas de crédito).

Pero más allá de considerar inadecuada la decisión de nuestro legislador, lo cierto es que en nuestra ley vigente sí se ha considerado como bien jurídico la "pureza e idoneidad de la información contenida en un sistema de tratamiento automatizado" y, en consideración a que puede ser objeto de atentados, le otorga amparo penal en los términos siguientes: "Todo atentado que signifique desviar el correcto desempeño del Sistema de Tratamiento de Información (automático o manual) con la finalidad de producir un perjuicio que redunde en un beneficio material o moral para sí o para otro, deberá constituir el elemento que dé la característica del delito en su manifestación más común".[45]

Esto es importante, por cuanto las figuras penales que establece la ley deben ser analizadas a la luz de este nuevo bien jurídico protegido, lo que ha entrañado asimismo dificultades en su aplicación.

45 VERA QUILODRÁN, Alejandro, *Delito e informática*, Ed. La Ley, Santiago,1996; p. 190.

3.4 Problemas dogmáticos y procesales que se presentan en el conocimiento y resolución de los delitos informáticos

3.4.1 Concepto de delito informático

Resulta interesante hacer el esfuerzo de conceptualizar los delitos informáticos, a fin de acotar el objeto de estudio. Autores como Miguel Ángel Davara Rodríguez lo hacen en términos amplios, como un 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 esta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos en alguna de sus fases de ejecución.[46]

Otro sector de la doctrina, en cambio, restringe la conceptualización a aquellos ilícitos que *incluyen* los medios informáticos en alguna de las fases de ejecución de la conducta lesiva. Tal es el caso de Klaus Tiedemann, quien en su libro *Poder económico y delito*[47] los define como "todos los actos antijurídicos que según la Ley Penal vigente (o socialmente reprochables, por lo que se estima factible su penalización futura) son realizados con empleo de máquinas automáticas de procesamiento de datos".

Tal es asimismo la opción que en su momento adoptó el catedrático Antonio E. Pérez-Luño, quien por la novedad de la problemática y el vertiginoso avance de la tecnología, amplía el concepto no solo a "las conductas incriminadas de *lege lata*, sino de propuestas de *lege ferenda*, o sea, a programas de política criminal y legislativa, sobre aquellos comportamientos todavía impunes que se estima merecen la consiguiente tipificación penal".[48] Así fue reconocido de hecho por el Consejo de Europa, que en su resolución Nº 12, de 1981, los definió como "todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos

46 DAVARA, Miguel Ángel, *Derecho informático*, Ed. Aranzadi, 1993.
47 TIEDEMANN, Klaus, *Poder económico y delito*, Ed. Ariel Derecho, Barcelona, 1985.
48 PÉREZ-LUÑO, Antonio Enrique, *Manual de informática y derecho*, Ed. Ariel, Barcelona, 1996.

y/o transmisión de datos". De ahí que, en un primer momento, la doctrina se refiriera más bien a criminalidad informática que a delitos informáticos propiamente tales, tema que abordaremos en un próximo acápite.

Ahora bien, a poco andar se ha ido descartando el tipificar como figuras especiales aquellos casos en que la informática es el *objeto* del delito, restringiéndose el concepto a aquellos casos en que las TIC son el *instrumento* para cometerlo.

3.4.2 Generalidades sobre de la criminalidad informática[49]

Las conductas que nos ocupan, es decir aquellas en que la informática es el medio comisivo, presentan ciertas características objetivas y subjetivas que las distinguen y sobre las cuales la doctrina ha reparado especialmente.

Desde la óptica subjetiva, se ha destacado que los sujetos activos de estas figuras ilícitas son personas cualificadas, al menos, en el área informática. Esta característica, que ya fuera enunciada por Romeo Casabona en la obra citada, ha sido especialmente considerada al momento de tipificar estas figuras, y ha llevado a que por regla general la legislación considere elementos subjetivos del tipo, ya sea en los tipos base o se incluya como agravante el que el sujeto que comete la acción típica y antijurídica sea el responsable del sistema.

Una segunda característica, estrechamente ligada a la anterior, es que como regla general se penaliza solo la conducta dolosa y no las culpables, incluso considerando un dolo específico.

A este respecto, una de las aristas polémicas de estos tipos penales dice relación con las conductas de Hacking, en que sujetos denominados *outsiders* o ajenos al sistema muchas veces actúan motivados más bien por un afán lúdico, o incluso por un "desafío intelectual"; lo mismo sucede con aquellas personas con conocimientos avan-

49 Ídem, pp. 72 y ss. Véase además a ROMEO CASABONA, Carlos María, *Poder informático y seguridad jurídica*, Ed. Fundesco, Madrid, 1985.

zados en la materia, que realizan operaciones informáticas con un ánimo de investigación científica, o de investigación en el ámbito de seguridad informática, y no por afán de perjuicio propiamente tal o de lucro económico. En estos casos, la polémica dice relación con la posibilidad de excluir estas conductas de los tipos penales que se establezcan.

3.4.3 Características objetivas de los delitos informáticos

En este punto, analizaremos los principales tipos de conductas delictivas realizadas a través de medios informáticos que atañen a la consulta realizada.

3.4.3.1 Conductas defraudatorias

Tienen por objeto interferir o distorsionar los datos procesados en sistemas informáticos, ya sea introduciendo datos falsos (*data diddling*), modificando el software empleado, o introduciendo rutinas o instrucciones aparentemente inocuas que alteran el funcionamiento del sistema informático, modalidad normalmente utilizada para desviar fondos, autorizar pagos o emitir documentos de pago a clientes ficticios.

Asimismo, se ha empleado para que, en el proceso financiero, por medio del sistema se realicen redondeos de sumas de dinero en cantidades pequeñas y la desviación del total hacia una cuenta destinada al efecto.

Se entiende, entonces, por estas conductas, la "incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de tercero".[50]

50 ROMEO CASABONA, Carlos María, *Poder informático y seguridad jurídica*, Ed. Fundesco, Madrid, 1988; p. 47.

Una de las principales dificultades para encuadrar estas conductas en los tipos penales tradicionales dice relación con la imposibilidad de dar satisfacción al requisito "engaño" ínsito en ellas, por cuanto no es posible atribuir la cualidad de "engañada" a una máquina.

Una de las principales dificultades para encuadrar estas conductas en los tipos penales tradicionales dice relación con la imposibilidad de dar satisfacción al requisito "engaño" ínsito en ellas, por cuanto no es posible atribuir la cualidad de "engañada" a una máquina.

En efecto, si bien el derecho penal se ha hecho cargo de la problemática, dado que con la informática en el sistema financiero se han reemplazado muchos de los documentos tradicionales en papel por "anotaciones en cuenta" o registros lógicos realizados en los sistemas informáticos, sin un soporte impreso o con reflejos en papel meramente informativos o secundarios, unánimemente se ha sostenido que las conductas defraudatorias tradicionales no cubren las manipulaciones informáticas destinadas a la distracción de fondos.

De ahí que la doctrina haya centrado el estudio del problema desde el enfoque de las manipulaciones de datos informatizados, planteando la necesidad de crear nuevos tipos penales y/o de modificar los existentes. De lo contrario, no podrá sostenerse que dichas conductas sean punibles.

En este sentido, el informe de la Organización para la Cooperación y el Desarrollo Económico (OCDE, 1983-1985) recomendó penalizar, en lo que nos interesa:

> "1) La entrada, alteración, destrucción y/o supresión de datos informáticos y/o programas de ordenador, realizadas intencionadamente con el fin de cometer una transferencia ilegal de bienes o de cualquier otra cosa con valor.
>
> 2) La entrada, alteración, destrucción y/o supresión de datos informáticos y/o programas de ordenador, realizadas intencionadamente con el fin de cometer una falsedad".[51]

51 ROMEO CASABONA, Carlos María, *Poder informático y seguridad jurídica*, Ed. Fundesco, Madrid, 1988; p. 105.

En todo caso, como podemos apreciar, las propuestas normativas no contemplan la posibilidad del delito culposo y a su turno establecen un dolo específico, cual es el ánimo de lucro, que en el caso en estudio no se vislumbra sino que se aprecia más bien un ánimo de criticar el sistema informático, destacando las inconsistencias y riesgos de seguridad que en ellos se detectan y el ánimo específico de dar a conocer esta información al titular del sitio web de comercio electrónico afectado, como se analizará más adelante.

3.4.3.2 Conductas de sabotaje

La doctrina entiende que, a través de este tipo de conductas, se busca penalizar la inutilización de los sistemas informáticos mediante el daño a los programas (soporte lógico del sistema), puesto que aquellas conductas que significan la alteración y/o destrucción del sistema de tratamiento de la información en sí (daños físicos que conllevan la destrucción, alteración o inutilización del sistema) no serían calificables como delito informático propiamente tal, sino más bien sino un delito de daños en que el objeto afecto es un sistema de tratamiento de la información.

Una de las primeras formas de comisión que se conocieron consiste en la introducción de programas o de rutinas que, dadas ciertas circunstancias, se ejecutan detonando una especie de "bomba lógica" que inutiliza el sistema total o parcialmente. Este tipo de delitos fue cometido generalmente por empleados del sistema informático, quienes, despechados con sus empleadores, introducían rutinas que operaban como bombas lógicas como medio de venganza. Otra de las modalidades más comunes es la introducción de virus informáticos (programas que poseen una secuencia de instrucciones que tienen la virtud de adicionarse e "infectar" aquellos programas que entren en contacto con él, propagando así sus efectos dañosos).

En la literatura jurídica nacional, Marcelo Huerta Miranda define el delito de sabotaje informático como "toda conducta típica, antijurídica y culpable que atenta contra la integridad de un sistema automatizado de tratamiento de información o de sus partes componentes, su funcionamiento o de los datos contenidos en él".[52]

Por su parte, Rodolfo Herrera Bravo sostiene que el sabotaje informático es "toda acción típica, antijurídica y dolosa destinada a destruir o inutilizar el soporte lógico de un sistema computacional, empleando medios computacionales".[53]

Pareciera ser más acertado este último concepto, pues se hace cargo de la necesidad de que a través de esta conducta lo afectado sea el soporte lógico y no la destrucción del hardware o soporte físico, lo cual, como dijimos, debiera ser considerado como un delito de daños convencional, que está o debe estar contemplado en la legislación penal.

3.4.3.3 Espionaje informático

En este caso, se trata de figuras delictivas a través de las cuales se accede y/o divulga indebidamente la información y se fundamenta en el valor económico que la misma representa en la sociedad actual. Este tipo de delitos es cometido principalmente con la finalidad de obtener un beneficio económico, pero se incrementan los casos en los que se busca información con fines políticos, e incluso personales.

Más adelante se entrará en el estudio de los tipos adoptados por el legislador y las dificultades que entraña el que, en este último caso, el bien sustraído sea la información, bien inmaterial que dadas sus especiales características no implica un cese de la posesión de su titular, pese a la sustracción efectuada.

52 HUERTA MIRANDA, Marcelo, "Figuras delictivo informáticas tipificadas en Chile", en Anuario Facultad de Ciencias Jurídicas Universidad de Antofagasta, año 2000 Nº 8.

53 HERRERA BRAVO, Rodolfo, "Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena Nº 19.223" (1998). Disponible en línea [consulta: 12/08/2021].

3.4.3.4 Intrusiones ilegítimas

Corresponden a una vulneración de los sistemas de seguridad del sistema informático o, tratándose se sujetos entendidos en la materia o conocedores del sistema específico del que se trata, mediante el uso de "puertas falsas" (*trap door*) o sistema "indocumentado" de un programa, previsto para el ingreso y recuperación de información en caso de fallos del sistema. Debe señalarse aquí también la existencia de programas especialmente destinados a desencriptar o "abrir", cual llave maestra, los sistemas informáticos, como es el caso del "*superzapping*".

Finalmente, una parte de la doctrina estima que para calificar como informático un ilícito se debe atender la funcionalidad del sistema informático, esto es, su operatividad. Serán tales, en consecuencia, aquellos que se refieran a esta característica, ya sea en la fase de entrada (*input*), procesamiento o salida (*output*) de datos.

3.5 El marco jurídico internacional: Convenio de Budapest sobre Ciberdelincuencia (2001)

El Convenio de Budapest (en adelante "el Convenio") fue adoptado el 23 de noviembre de 2001 en la ciudad de Budapest, Hungría, por el seno del Consejo de Europa. Luego de largos años de análisis y discusión, Chile lo promulgó como ley de la República a través del Decreto Nº 83, de 28 de agosto de 2017, del Ministerio de Relaciones Exteriores.

Este Convenio tiene dos ámbitos específicos. Uno sustantivo que trata de los delitos informáticos y uno procesal, especialmente dedicado a las medidas de investigación y cooperación internacional en la persecución de estos delitos.

3.5.1 Ámbito sustantivo

En el ámbito sustantivo, destaca que como regla general los tipos penales que prevé el Convenio incluyen, como elemento subjetivo del tipo, que se trate de acciones deliberadas e ilegítimas, excluyendo con ello las conductas culposas y el dolo eventual.

En segundo lugar, el Convenio prevé que se adopten las medidas legislativas y de otro tipo que resulten necesarias para que se persiga tanto la responsabilidad de personas naturales como de personas jurídicas, en las siguientes hipótesis:

> "1. Cuando estos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:
>
> a. un poder de representación de la persona jurídica;
>
> b. una autorización para tomar decisiones en nombre de la persona jurídica;
>
> c. una autorización para ejercer funciones de control en el seno de la persona jurídica.

> 2. Cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada antes haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad".

En los siguientes acápites, veremos los delitos que se prevén en el Convenio.

3.5.1.1 Acceso ilícito (art. 2)

Consiste en el **acceso deliberado e ilegítimo** a todo o parte de un sistema informático. El Convenio admite que los Estados decidan si exigirán que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático. En este caso, se prevé la sanción para autores y cómplices.

Una de las formas comisivas de este delito se denomina *phishing*, esto es, la captura de claves a través de un ardid que puede consistir en páginas web falsificadas o mensajes de correo fraudulentos. Asimismo, caben dentro de esta figura los delitos de espionaje informático, por ejemplo, para revelar secretos industriales, secretos de Estado y acceso a otro tipo de datos confidenciales.

3.5.1.2 Interceptación ilícita (art. 3)

Consiste en "la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos".

En este caso, se sanciona tanto la autoría como la complicidad "deliberada", y no solo el delito consumado, sino además la "tentativa deliberada".

3.5.1.3 Ataque a la integridad de datos (art. 4)

Consiste en "todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves".

Al respecto, debemos entender por sistema informático todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Por dato informático, entendemos toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

En este caso, se sanciona tanto la autoría como la complicidad "deliberada", y no solo el delito consumado, sino además la "tentativa deliberada".

3.5.1.4 Ataque a la integridad del sistema (art. 5)

Se entiende por tal la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

3.5.1.5 Abuso de dispositivos (art. 6)

Se entiende por tal el uso de un sistema informático o sus componentes para efecto de cometer ilícitos. Al respecto, el Convenio considera las siguientes hipótesis:

a. La **producción, venta, obtención** para su utilización, importación, difusión u otra forma de puesta a disposición de:

   — **cualquier dispositivo,** incluido **programa informático,** concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del Convenio.

- una **contraseña, código de acceso** o **datos informáticos** similares que permitan acceder a todo o parte de un sistema informático con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5 del Convenio.

b. La **posesión** de alguno de los elementos contemplados en los dos incisos del apartado a. precedente, con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5 del Convenio. Las partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

En estos casos, se sanciona la complicidad deliberada de cometer este delito. de cualquier modo, para estas figuras Chile reservó que "no aplicará el párrafo 1 del mismo artículo, en la medida que ello no afecte la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 A) ii) del citado artículo 6".

Sobre este punto, el Convenio señala una regla de interpretación relevante respecto de este artículo en su párrafo 2:

> "No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, como en el caso de las pruebas autorizadas o de la protección del sistema informático".

3.5.1.6 Falsificación informática (art. 7)

Se entiende por tal "la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean

legibles o inteligibles directamente. Las partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal".

Tal y como sucede en las figuras anteriores, se sanciona la complicidad deliberada y la tentativa deliberada.

3.5.1.7 Fraude informático (art. 8)

En este caso, se sanciona los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

a. La introducción, alteración, borrado o supresión de datos informáticos.

b. Cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Tal y como sucede en las figuras anteriores, se sanciona la complicidad deliberada y la tentativa deliberada.

3.5.1.8 Delitos relacionados con la pornografía infantil (art. 9)

Al respecto, se señala que será tal la comisión deliberada e ilegítima de los siguientes actos:

— la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

— la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;

— la difusión o la transmisión de pornografía infantil a través de un sistema informático;

— la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;

— la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

Se sanciona tanto a autores como a cómplices y la complicidad deliberada de cometer este delito y, en cuanto al grado de consumación, se incluye la sanción a la tentativa deliberada de cometer este delito.

A este respecto, se establece que se entenderá por "pornografía infantil" todo material pornográfico que contenga la representación visual de:

- un menor adoptando un comportamiento sexualmente explícito;
- una persona que parezca un menor adoptando un comportamiento sexualmente explícito;
- imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

Para estos efectos, el "menor" es toda persona menor de 18 años, aun cuando se prevé que los Estados podrán exigir un límite de edad inferior, que deberá ser como mínimo 16 años.

Sobre esta materia, Chile formuló una reserva en el sentido de que no se compromete a aplicar los apartados b. y c. del párrafo 2 del artículo 9 del Convenio, esto es, las representaciones de pornografía donde una persona que parezca un menor adopte un comportamiento sexualmente explícito, y aquellas imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

3.5.1.9 Delitos relacionados con la propiedad intelectual (art. 10)

Al respecto, el Convenio establece que cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno:

> "1. (…) las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París, de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del tratado de la OMPI sobre el derecho de Autor, a excepción de

cualquier derecho moral otorgado por dichos convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. (…) las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Invención Internacional sobre la protección de los artistas, intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del tratado de la OMPI sobre Interpretación o Ejecución y fonogramas, a excepción de cualquier derecho moral conferido por dichos convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático".

En este caso, asimismo, se prevé que se sancione la complicidad deliberada y la tentativa deliberada.

3.5.2 Ámbito adjetivo o normas procesales

El Convenio prevé medidas de investigación y cooperación en el ámbito procesal, las que alcanzan no solo los tiempos penales previstos en su texto, sino cualquier otro delito cometido por medio de un sistema informático. Sobre este ámbito nos referiremos más adelante, en el capítulo sobre medidas procesales y probatorias.

3.6 La Ley Nº 19.223 sobre delitos informáticos y el contenido de su reforma

3.6.1 Antecedentes

La Ley N° 19.223, de fecha 7 de junio de 1993, que tipifica figuras penales relativas a la informática, se originó en la moción presentada ante la Cámara de Diputados por el diputado señor José Antonio Viera-Gallo en la 19ª sesión, de 16 de julio de 1991, publicada en el Boletín de la Cámara de Diputados Nº 412-07.

En su moción, Viera-Gallo sostiene lo siguiente:

> "El vertiginoso desarrollo de las tecnologías de la información ha convertido a ésta en uno de los más preciados recursos. Ya no existe organización social compleja que pueda prescindir de la utilización de sistemas automatizados de tratamiento de la información, mediante computadores o redes de computadores, a fin de respaldar sus procesos de adopción de decisiones.
>
> Nadie discute en la actualidad los grandes beneficios que la introducción de las referidas tecnologías ha producido, en términos de mejor aprovechamiento de energías y recursos. Sin embargo, la creciente importancia que ha adquirido la informática ha hecho patente la vulnerabilidad de las sociedades y de las organizaciones que las utilizan. Son muchos los abusos que, recurriendo a los avances de la ciencia de la información pueden cometerse".[54]

Con ello se quiso evidenciar la importancia de legislar en la materia, a fin de precaver la impunidad de conductas realizadas a través de los sistemas informáticos. En definitiva, y luego de una ardua tramitación legislativa, se dicta la Ley Nº 19.223, con un total de cuatro artículos.

54 Boletín Oficial Nº 412-07, de la Honorable Cámara de diputados y Senado de Chile.

3.6.2 El bien jurídico protegido en la Ley Nº 19.223

En la historia de la ley, se dejó constancia expresa de que su establecimiento tenía por objeto "proteger un nuevo bien jurídico que ha surgido con el uso de las modernas tecnologías computacionales: la calidad, la pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan".[55]

Con ello se reconoce, en consecuencia, un nuevo bien jurídico en nuestro ordenamiento, cual es "la calidad, pureza e idoneidad de la información contenida en Sistemas de Tratamiento de la misma, así como de los productos provenientes de la operación de dichos sistemas". Por tanto, las figuras que crea el legislador buscan proteger al sistema en sí mismo, su funcionamiento conforme a lo previsto por sus titulares y la información que es objeto de tratamiento.

El legislador al momento de establecer la Ley Nº 19.223 trata de proteger la información, evitando que esta se convierta en objeto de atentados que la alteren o destruyan, sin embargo no considera que no toda información tiene el mismo valor y consideración.

En todo caso, esta postura del legislador ha sido ampliamente criticada, porque además de restar coherencia al sistema jurídico-penal creando artificiosamente un nuevo bien jurídico protegido, olvida que la información es "comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada"…"conocimientos así comunicados o adquiridos" (RAE) y, visto así, no es un bien en sí misma sino que su representación podrá tener diversas connotaciones, ya sean patrimoniales, familiares, morales, etcétera.

En efecto, el legislador al momento de establecer la Ley Nº 19.223 trata de proteger la información, evitando que esta se convierta en objeto de atentados que la alteren o destruyan, sin embargo no considera que no toda información tiene el mismo valor y consideración. A vía de ejemplo, para la ley es indiferente que lo que se destruya, altere, etcétera, sea un archivo con los secretos industriales de una fábrica o las recetas de cocina de una ama de casa, o que la

55 Boletín Oficial Nº 412-07, de la Honorable Cámara de Diputados y Senado de Chile. Historia fidedigna de la Ley Nº 19.223, sesión 19ª, martes 16 de julio de 1991.

información a la que se accede indebidamente sean la fórmula de una bebida famosa, las conversaciones privadas de dos personas por un chat o una red social.

Siendo así, consideramos que la única forma de que la Ley Nº 19.223 y sus modificaciones tengan una mayor aplicación práctica, es que los operadores jurídicos vinculen las figuras que en ella se establecen no solo al bien jurídico para el cual fueron creadas, sino a la serie de bienes jurídicos que se pueden ver afectados a través de las conductas que establece, a saber: la propiedad, la intimidad y la seguridad del tráfico mercantil, entre otros.

3.6.3 El objeto del delito

Como se señaló antes, los objetos de estos delitos son "la información" y "los sistemas de tratamiento automatizado" de la misma.

Según la RAE, un "sistema" es un conjunto de reglas o principios sobre una materia racionalmente enlazados entre sí, y también un conjunto de cosas que, relacionadas entre sí, ordenadamente contribuyen a determinado objeto. "Tratar", para la RAE, es manejar una cosa o usarla materialmente, en tanto "informática" es el conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automatizado de la información por medio de computadoras.

De estos conceptos entendemos que el objeto del delito es tanto el conjunto de partes y piezas que conforman el soporte físico (*hardware*), como el conjunto de programas (*software*) que determinan las reglas o principios conforme a las cuales el hardware funcionará, los procesos que desarrollarán, etcétera.

La información propiamente tal corresponde a los datos que son objeto de tratamiento a través o mediante el empleo del sistema, esto es, los datos que son objeto de procesamiento.

La información propiamente tal corresponde a los datos que son objeto de tratamiento a través o mediante el empleo del sistema, esto es, los datos que son objeto de procesamiento.

Tales datos podrán ser afectados en distintas fases: en la fase de entrada de la información, mediante el ingreso de datos falsos; durante el procesamiento, mediante la alteración de rutinas de programa, o en la salida, alterando los resultados emanados de un procesamiento correcto.

Por su parte, el legislador lo que busca es proteger el sistema de las posibles manipulaciones que afecten su normal funcionamiento o que lo inutilicen total o parcialmente, que dañen o alteren la información, o que afecten la seguridad de la información a través de accesos ilegítimos al sistema o revelaciones indebidas de datos.

En todo caso, estimamos que debemos entender el objeto protegido a la luz de las consideraciones que hiciéramos acerca del bien jurídico protegido en estos delitos, de acuerdo al legislador de la Ley Nº 19.223, esto es, "la pureza e idoneidad de la información contenida en un sistema de tratamiento de la información". Al hacerlo, se consideró la importancia que en todo orden de cosas ha cobrado el procesamiento automatizado de la información. Eso nos lleva a concluir que el legislador se puso en el supuesto de que los sistemas de tratamiento de la información funcionan correctamente, sin errores de proceso que afecten por sí mismos la idoneidad de la información.

Lo anterior se desprende además de la protección al sistema mismo, a su integridad mediante el establecimiento del delito de sabotaje, lo que no es del todo efectivo pues los sistemas tienen errores de configuración o de programación que afectan a la información en desmedro de su calidad e idoneidad.

Sabido es que en el estado actual del avance de la técnica, en general, el legislador radica en quien usa la informática para comunicarse o interactuar con terceros el deber de velar por el correcto funcionamiento del sistema de tratamiento de la información, estableciendo una especie de responsabilidad agravada, derivada precisamente de los necesarios conocimientos para desarrollar proyectos de esta envergadura.

Estimamos que no es esta, la de los delitos informáticos, una excepción a la regla. El derecho no puede proteger a quien, sabiendo o debiendo saber los errores de que adolece su sistema de tratamiento de la información, no toma los debidos resguardos para su corrección.

3.6.4 El sujeto activo de los delitos de la Ley Nº 19.223

En relación con el sujeto activo de la conducta punible, la ley no exige la concurrencia de ningún tipo de exigencia específica, lo cual se deduce de la escueta expresión "El que..." usada en los cuatro artículos de la ley.

Con todo, la ley prevé una circunstancia agravante en el caso del delito de espionaje informático tipificado en el artículo 4º, para el caso en que "quien incurre en estas conductas es el responsable del sistema de información".

Nuevamente, en esta norma vemos evidenciada la especial consideración de los conocimientos necesarios para desarrollar la conducta punible. Tratándose del responsable del sistema de información, además del deber de custodia que le cabe al respecto, se trata de una persona que está al tanto de los detalles del funcionamiento del sistema.

3.6.5 Los elementos subjetivos de los tipos penales de la Ley Nº 19.223

La ley no admite el delito culposo sino que, en cada uno de los tipos penales que establece, exige la concurrencia de un dolo específico. Así, en los artículos 1º, 3º y 4º utiliza la expresión "maliciosamente", que se entiende como la intención solapada y maligna con la cual se dice o hace algo con la intención positiva de infligir un daño a la persona y/o propiedad de otro.

De su parte, el artículo 2º hace referencia a "indebidamente", es decir ilícito, injusto o falto de equidad, haciéndose cargo así de la definición que se acuñara en el seno de las Naciones Unidas respecto de los delitos informáticos, como acciones contrarias a la ética (no solo la normativa jurídico-penal) y representadas por la utilización abusiva de conocimientos de la técnica informática, con el objetivo de vulnerar las medidas de seguridad de un sistema hasta lograr ingresar a él a fin de utilizar para propio beneficio la información que allí se contiene.

Esta malicia o actitud indebida, en la lógica del legislador, debiera ir encaminada a producir un daño o menoscabo al objeto del delito, cual es el sistema de tratamiento de la información, sus partes o componentes y/o a la información contenida en el sistema, sin perjuicio de los otros bienes que pudieran verse afectados con la acción.

Todas estas reflexiones resultan especialmente relevantes, por cuanto en el ámbito informático los especialistas suelen realizar acciones que afectan a los sistemas de tratamiento de la información, pero con un ánimo muy diferente al requerido por la ley. En efecto, es de común ocurrencia que se ensayen formas de acceder a sistemas de tratamiento de la información y/o se desarrollen actividades destinadas a testear el funcionamiento de los mismos, con el expreso interés de verificar las condiciones de funcionamiento del sistema y en particular si estas son idóneas y/o seguras, sin que en estos casos sea posible sostener que se está cometiendo delito.

Una interpretación contraria vulneraría no solo el espíritu de la ley, sino también su texto expreso, además de constituirse en un indeseado freno al desarrollo científico y tecnológico.

3.6.6 Análisis del artículo 1° de la Ley N° 19.223

En su texto, el primero de los cuatro artículos que contiene la ley dispone lo siguiente:

> "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".

Como podemos apreciar, estamos frente a la figura de "sabotaje informático", que comprende los siguientes verbos rectores:

a. **Destruir** un sistema de tratamiento de información, sus partes o componentes. Este verbo rector, conforme al Diccionario de la Real Academia de la Lengua, conlleva "deshacer, arruinar o asolar una cosa material", por tanto solo puede aplicarse al hardware como objeto del delito y conlleva la pérdida total del mismo.

b. **Inutilizar** un sistema de tratamiento de información o sus partes o componentes. En este caso, el verbo rector, según el mismo diccionario, supone la pérdida de utilidad del sistema de tratamiento de la información, sus partes o componentes, vale decir la pérdida de la cualidad conforme a la cual presta servicio, trae o produce provecho, comodidad, fruto o interés. Se trataría de la pérdida de capacidad del sistema de servir para aquella función para la cual fue creado, sin que esta pérdida involucre la destrucción material del mismo.

c. **Impedir** el funcionamiento de un sistema de tratamiento de información, sus partes o componentes. Conforme a la RAE, impide lo que estorba o imposibilita la ejecución de una cosa. Nuevamente, se trata de una pérdida total de las posibilidades de prestar servicios, del sistema de tratamiento de la información, una incapacidad del sistema para ejecutar sus funciones propias sin que necesariamente implique su destrucción física.

d. **Obstaculizar** el funcionamiento de un sistema de tratamiento de información, sus partes o componentes. Este verbo rector implica "impedir o dificultar la consecución de un propósito" (RAE). Es decir, si bien el sistema puede cumplir su función de tratar la información, lo hace de manera dificultosa, con la consecuente ineficiencia en el proceso de tratamiento.

e. **Modificar** el funcionamiento de un sistema de tratamiento de información, sus partes o componentes. Verbo que significa "limitar, determinar o restringir las cosas a cierto estado en que se singularicen y distingan unas de otras", "transformar o cambiar una cosa mudando alguno de sus accidentes". Como se aprecia, en este caso el sistema sigue funcionando y prestando utilidad, pero no según los procedimientos previstos por su titular.

Como regla general, la doctrina entiende que el sabotaje informático abarca a aquellas conductas que afectan el soporte lógico del sistema de tratamiento de la información. En el caso chileno, el legislador extiende la protección a quienes destruyan o inutilicen el equipo o aparato computacional y sus partes, piezas o componentes.

A continuación, el inciso segundo del artículo 1° contempla una figura agravada para el caso en que, a consecuencia de las acciones descritas en el inciso primero, se afectaren los datos contenidos en el sistema. A ello se suma que para el sujeto activo del tipo es posible prever que, como consecuencia de la realización de las acciones del inciso primero, los datos contenidos en el sistema pueden resultar alterados, dañados o destruidos, con los consecuentes perjuicios al titular del sistema.

Como regla general, la doctrina entiende que el sabotaje informático abarca a aquellas conductas que afectan el soporte lógico del sistema de tratamiento de la información. En el caso chileno, el legislador extiende la protección a quienes destruyan o inutilicen el equipo o aparato computacional y sus partes, piezas o componentes.

En cualquier caso, este alcance ha tenido escasa aplicación, principalmente porque tanto la doctrina como la jurisprudencia han entendido que el aparato computacional o hardware se encuentra protegido por la vía de delitos establecidos en nuestra legislación criminal, como lo son el robo, el hurto, la apropiación indebida, o los daños.

Es más, en nuestra literatura jurídica se ha enfatizado que la Ley Nº 19.223 "en vez de actualizar el tipo tradicional contenido en el Código Penal, –que habría sido lo correcto– crea una supuesta nueva figura. El problema que produce es comparable con la situación de considerar como delitos distintos el robo de una lámpara y el de una impresora, pese a que se trata de un mismo delito".[56]

Otro problema es que la ley no especifica qué componentes o partes del sistema de tratamiento de información está protegiendo, y por tanto extiende el amparo de esta figura al soporte físico o hardware, desnaturalizando el objetivo del proyecto de ley que le dio origen. Este era el de recoger mediante nuevas figuras solo aquellos atentados que no se encontraran regulados en figuras tradicionales, como

56 HERRERA BRAVO, Rodolfo, "Reflexiones sobre los Delitos Informáticos motivadas por los desaciertos de la Ley Chilena Nº 19.223" (1998). Disponible en línea [consulta: 12/08/2021].

lo serían aquellos actos cometidos en contra de soportes lógicos o programas y en los datos contenidos en ellos, atentando así contra el sistema jurídico penal nacional.

Ahora bien, el tipo penal del artículo 1º considera dos tipos de conductas, a saber:

- Atentados contra un **sistema de tratamiento de la información o de sus partes componentes**. Tipificado en la primera parte del artículo primero. Previendo como circunstancia agravante que como resultado de esta conducta se vean afectados los datos contenidos en un sistema automatizado de tratamiento de la información.
- Atentados contra el **funcionamiento de un sistema de tratamiento de la información.** Tipificado en la segunda parte el artículo primero. Previendo la misma circunstancia agravante anterior.

Estimamos que, para que se configuren los delitos de los artículos 1º y 3º de la Ley Nº 19.223, debe afectarse el sistema de tratamiento de la información, sus partes o componentes, ya sea alterando su forma de funcionamiento, destruyéndolo, inutilizándolo o modificándolo.

Revisemos ahora cómo han abordado este problema otros países suscriptores del Convenio de Budapest.

En primer lugar, Alemania[57] abordó el fenómeno de los delitos informáticos en la Segunda Ley para la lucha contra la criminalidad económica, promulgada con fecha 15 de mayo de 1986, que modificó el Código Penal en materia de delitos informáticos. En su artículo 303.b, el Código Penal tipifica el delito de sabotaje informático en los términos siguientes:

> "Quien destruya una elaboración de datos que sea de esencial importancia para una industria ajena, una empresa ajena o una autoridad,

57 UNIDAD DE APOYO AL PROCESO LEGISLATIVO BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. 2002. Derecho Comparado, Delito informático.

1. cometiendo el hecho de acuerdo al párrafo 303.a.II, o

2. 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" (303b).

La finalidad perseguida por la legislación alemana, al crear el tipo de sabotaje informático diferenciado del tipo de alteración de datos, fue proteger especialmente los procesos de datos 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 este tipo penal es aplicable asimismo a quien arremete a equipos o soportes de datos propios en los que terceros 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.

Francia[58] por su parte, dictó en enero de 1988 la ley relativa al fraude informático, también llamada "*loi Godfrain*", mediante la cual se regularon los delitos informáticos agregando un capítulo al Código Penal bajo el título "Sobre ciertas infracciones en materia informática". Los artículos 323-2 y 323-3 de este cuerpo legal se refieren al sabotaje informático en los términos siguientes:

"El hecho de obstaculizar o alterar el funcionamiento de un sistema de tratamiento automatizado de datos será castigado con cinco años de prisión y 75.000 euros de multa"; y

"El hecho de introducir datos de manera fraudulenta en un sistema de tratamiento automatizado o de suprimir o modificar

58 UNIDAD DE APOYO AL PROCESO LEGISLATIVO BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. Ob. cit.

> fraudulentamente los datos que contenga será castigado con cinco años de prisión y 75.000 euros de multa", respectivamente.

El Código Penal español vigente también contiene normas específicas relativas a conductas que tienen como objeto de ataque o como instrumento del delito a sistemas o a elementos informáticos. El delito de sabotaje está tipificado en el artículo 264.1, que dispone:

> "El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años".

Para luego establecer algunas figuras agravadas de este mismo delito, a saber:

- Que se hayan cometido en el marco de una organización criminal.
- Que se hayan ocasionado daños de especial gravedad o afectado un número elevado de sistemas informáticos.
- Que se hayan perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad.
- Que se haya afectado a sistemas informáticos de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o un Estado Miembro de la Unión.

En conclusión, las conductas de sabotaje, tanto en Chile como en derecho comparado, exigen que se atente contra el sistema de tratamiento, ya sea inutilizándolo o alterando su funcionamiento.

3.6.7 Análisis del artículo 3º de la Ley Nº 19.223

> "Artículo 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".

En este caso, el objeto afectado por las conductas previstas es la veracidad, claridad, pureza y/o alcance de la información contenida en un sistema de tratamiento de la información. Las conductas concretas que se penalizan son las siguientes:

- El que maliciosamente "**altere**" los datos, entendiendo por alterar "cambiar la esencia o forma de una cosa", configurando así la conducta el ingreso o introducción de datos erróneos o "*data diddling*"; el borrado de datos verdaderos, por cualquier medio; las transformaciones y desfiguraciones de los datos, por ejemplo mediante la introducción de virus informáticos, y en general toda conducta que implique cambiar la información contenida en un sistema de tratamiento de la misma sin destruirla.
- El que maliciosamente "**dañe**" los datos contenidos en el sistema de tratamiento, entendiendo por la acción de dañar "maltratar o echar a perder una cosa", por lo que en este caso lo afectado es la integridad de la información. Sin embargo, lo que distingue al daño de la destrucción es que en esta última el resultado es irreversible y permanente. Por lo tanto, si la información o datos es posible recuperarla a través de instrucciones o comandos como "*unerase*","*undelete*" u otros, o se dispone de programas de respaldo (*back up*), estaremos frente a un daño informático y no una destrucción.
- El que maliciosamente "**destruya**" los datos contenidos en un sistema de tratamiento de información, entendiendo por destruir "deshacer, arruinar o asolar una cosa", y por tanto implica una pérdida irreversible y permanente de los datos.

En derecho comparado, el delito de alteración de datos ha sido tratado por países como Alemania, Austria y Francia.

El Código Penal alemán[59], en su artículo 303.a, protege tanto al que almacena datos como al afectado por el contenido de estos. El tipo en cuestión menciona cuatro acciones: 1) Borrado (hacer desaparecer los datos de manera completa e irrecuperable); 2) Ocultamiento (privar

59 UNIDAD DE APOYO AL PROCESO LEGISLATIVO BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. Ob. cit.

el acceso a los datos a las personas autorizadas a ello); 3) Inutilización (daño de los datos de manera que no pueden cumplir con su fin), y 4) Alteración (transformación de los datos, borrado parcial o puesta en relación con otros datos).

Austria[60] por su parte solo trata el delito de destrucción de datos en el artículo 126 del Código Penal, artículo modificado por la ley de reforma al Código Penal de 22 de diciembre de 1987. Este tipo penal abarca tanto la destrucción de datos personales como los no personales y los programas.

En tercer lugar, la legislación francesa[61] sanciona la destrucción de datos y la modificación de estos mediante la introducción fraudulenta de datos en un sistema de tratamiento automatizado de la información, en el artículo 323-3 de su Código Penal.

60 UNIDAD DE APOYO AL PROCESO LEGISLATIVO BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. Ob. cit.
61 UNIDAD DE APOYO AL PROCESO LEGISLATIVO BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. Ob. cit.

3.7 Otras leyes que prevén delitos de relevancia a efectos informáticos

3.7.1 Delitos contra la propiedad intelectual y pirateo informático

Como es sabido, la ley de propiedad intelectual protege tanto al autor como al productor y a los intérpretes y ejecutantes, respecto de los derechos patrimoniales y morales que se les reconoce por el ordenamiento jurídico nacional.

Los derechos morales son aquellos que emanan de la paternidad de la obra, conforme a los cuales el autor podrá permiten reivindicar esa paternidad, oponerse a deformaciones, mutilaciones y modificaciones no consentidas de la obra, y mantener la obra inédita, principalmente.

En lo que nos interesa, el artículo 3º Nº 16 de la Ley Nº 17.336, de propiedad intelectual, establece que la protección que otorga esa ley comprende "los programas computacionales, cualquiera sea el modo o forma de expresión, como programa fuente o programa objeto, e incluso la documentación preparatoria, su descripción técnica y manuales de uso".

A renglón seguido, en el Nº 17 de ese mismo artículo, se prevé que se protegerán también "las compilaciones de datos o de otros materiales, en forma legible por máquina o en otra forma, que por razones de la selección o disposición de sus contenidos, constituyan creaciones de carácter intelectual. Esta protección no abarca los datos o materiales en sí mismos, y se entiende sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales contenidos en la compilación".

La ley define programa computacional en los siguientes términos: "Conjunto de instrucciones para ser usadas directa o indirectamente en un computador a fin de efectuar u obtener un determinado proceso o resultado, contenidas en un cassete, diskette, cinta magnética u otro soporte material". Y copia de programa computacional como

"soporte material que contiene instrucciones tomadas directa o indirectamente de un programa computacional y que incorpora la totalidad o parte sustancial de las instrucciones fijadas en él".

Los derechos patrimoniales, en cambio, se refieren a la posibilidad de explotar las obras en el tráfico económico. Los delitos, en esta ley, están previstos entre los artículos 78 y 82, estableciendo, en lo que nos interesa, los siguientes:

- La utilización de obras de dominio ajeno protegidas por la ley sin estar facultado para ello (art. 79 letra a, Ley Nº 17.336).
- El cobro de derechos u otorgamiento de licencias respecto de obras careciendo de autorización del titular de los derechos o de la ley (art. 79 letra e, Ley Nº 17.336).
- La falsificación de obras protegidas por esa ley, la edición reproducción o distribución ostentando falsamente el nombre del editor autorizado suprimiendo o cambiando el nombre del autor o el título de la obra, o alterando maliciosamente su texto (art. 79 bis, Ley Nº 17.336).

3.7.2 Delitos de pornografía infantil a través de medios computacionales

La pornografía infantil es uno de los problemas persistentes en la red. Por ello, de manera temprana nuestro Código Penal se actualizó para los efectos de recoger figuras penales que sancionaran estas conductas.

3.7.3 Grooming, bullying y otras formas de discriminación en línea

Conforme a su artículo 1º, la Ley N° 20.609 "tiene por objeto fundamental instaurar un mecanismo judicial que permita restablecer eficazmente el imperio del derecho toda vez que se cometa un acto de discriminación arbitraria".[62]

62 Ley N° 20.609. Establece medidas contra la discriminación. Subsecretaría General de Gobierno, Chile, 24 de julio de 2012; art. 2°.

Según el diccionario de la Real Academia Española de la lengua, discriminar es "seleccionar excluyendo" y, a su turno, excluir no necesariamente es una expresión negativa.

Siendo así, nuestra legislación agrega que esta discriminación debe ser arbitraria para ser ilícita, vale decir, aquella que "carezca de justificación razonable" y que cause privación, perturbación o amenaza en el ejercicio legítimo de un derecho de la persona. Consideramos que el *grooming* y el *bullying* son especies dentro de este concepto más amplio.

3.7.3.1 Bullying

El *bullying* o acoso escolar consiste en una forma de maltrato psicológico, verbal o físico producido entre escolares de forma sostenida y a lo largo de un tiempo determinado. Se afirma que es una "forma de comportamiento agresivo que suele ser lesivo y deliberado, persistente y a veces, continuado durante semanas, meses e incluso años", y que subyacente a este comportamiento estarían el abuso de poder y deseo de dominar e intimidar[63], aun cuando "una conducta acosadora puede lesionar distintos bienes jurídicos: libertad, libertad sexual, salud, honor, intimidad o integridad moral".[64]

Entre las características del *bullying*, los diversos autores coinciden en las siguientes[65]:

- Hay una diferencia de poder entre aquellos que están siendo acosados y aquellos que acosan. Esta diferencia puede deberse a la superioridad numérica, física (tamaño y fuerza del acosador), social (tener más amigos, ser más popular), capacidad económica, edad, e incluso a la red de contactos al interior del colegio.[66]

63 SUCKLING, A. y TEMPLE, C., *Herramientas contra el acoso escolar. Un enfoque integral*. Madrid, España, Ed. Morata, 2006; p. 79. Citando a SHARP y SMITH, 1994

64 MENDOZA C. Silvia, *El derecho penal frente al acoso a menores: Bullying, cyberbulliyng, grooming y sexting*. Valencia, España, Tirant Lo Blant (868), 2013; p. 17

65 Bullying.org <http://www.bullying.org> [consulta: 4 de diciembre 2014].

66 Fundación Pro Bono. El bullying y sus implicancias legales: manual para los colegios. Disponible en línea [consulta: 12-08-2021].

- Involucra comportamientos dañinos que son repetidos e intencionales.
- No se trata de un conflicto escolar que necesite ser resuelto, en el *bullying* el problema se radica en el odio y desdén de quienes detentan poder respecto de aquellos compañeros más débiles a los que se intenta herir.

La Ley Nº 20.536, sobre violencia escolar, en su artículo 16 B define el acoso escolar como: "(…) toda acción u omisión constitutiva de agresión u hostigamiento reiterado, realizada fuera o dentro del establecimiento educacional por estudiantes que, en forma individual o colectiva, atenten en contra de otro estudiante, valiéndose para ello de una situación de superioridad o de indefensión del estudiante afectado, que provoque en este último, maltrato, humillación o fundado temor de verse expuesto a un mal de carácter grave, ya sea por medios tecnológicos o cualquier otro medio, tomando en cuenta su edad y condición".

El *bullying* puede ser verbal, físico, social o, en lo que interesa a este trabajo, a través de medios tecnológicos, conducta que se conoce como *ciberbullying* y se caracteriza por "la utilización de tecnologías de información y comunicación, para sostener comportamientos hostiles, deliberada y repetidamente por un individuo o grupo, que intenta dañar a otros".[67]

Sin perjuicio de la ley en comento, en el Código Penal existe una serie de tipos penales que podrían configurarse a través de conductas de *ciberbullying*. Es el caso de las injurias y calumnias, que podrían realizarse por escrito y con publicidad cuando se difunden mensajes a través de blogs, chat colectivos, correos electrónicos virales o redes sociales.[68]

67 Cyberbullying.org.

68 Véase el art. 422 del Código Penal, conforme al cual "la calumnia y la injuria se reputan hechas por escrito y con publicidad cuando se propagaren por medio de carteles o pasquines fijados en los sitios públicos; por papeles impresos, no sujetos a la ley de imprenta, litografías, grabados o manuscritos comunicados a más de cinco personas, o por alegorías, caricaturas, emblemas o alusiones reproducidos por medio de la litografía, el grabado, la fotografía u otro procedimiento cualquiera".

3.7.3.2 Grooming

Se entiende que la expresión *grooming* abarca cualquier acción que tenga por objetivo minar y socavar moral y psicológicamente a una persona, con la finalidad de conseguir su control a nivel emocional. Esta conducta es especialmente grave si el objetivo es controlar a un menor con el fin de obtener algún tipo de conducta sexual de parte de este. La Ley Nº 20.526 modificó el Código Penal para efectos de tipificar estas conductas.

El *grooming* incluye el *grooming online*, que es "el proceso por el cual un adulto, valiéndose de los medios que le ofrecen las tecnologías de la información y la comunicación (TIC), entra en la dinámica de persuadir y victimizar sexualmente a un menor, tanto de manera física como a través de internet, mediante la interacción y la obtención de material sexual del menor".[69] Si bien el *modus operandi* no es único, los agresores suelen identificar a sus víctimas potenciales en sistemas en línea tales como redes sociales, y luego del acceso tratan de ganarse la confianza de los menores, normalmente con ardides, para en una tercera fase iniciar el acercamiento hacia los aspectos sexuales, ya sea abriendo el diálogo sobre preferencias o lisa y llanamente enviándoles o solicitándoles videos de connotación sexual.

Aunque la modificación al Código Penal no incluyó la expresión *grooming*, sí se incluyeron conductas compatibles con el concepto que señalamos antes. A vía ejemplar, el artículo 366 quáter prevé expresamente que "las penas señaladas en el presente artículo se aplicarán también cuando los delitos descritos en él sean cometidos a distancia, mediante cualquier medio electrónico". Con ello, se extiende los efectos de dicho artículo a la realización de las conductas que prevé a través de los medios que nos interesan.

En este caso, el término "delante" contenido en el artículo 366 quáter del CP no se refiere a una necesidad física de que el partícipe del ilícito esté presencialmente al frente del menor, sino a que el otro

69 SANTIESTEBAN Patricia y otro, "Estrategias de persuasión en *grooming online* de menores: un análisis cualitativo con agresores en prisión". En *Psychosocial Intervention* Vol. 26 Nº 3, Madrid, diciembre de 2017. Disponible en línea [consulta: 22.12.2020].

pueda ser testigo de la acción sexual, en el sentido de que pueda observarlo u oírlo. Esto puede perfectamente ser llevado a cabo a través de medios tecnológicos, y la aplicación de la expresión "delante" en términos amplios no constituiría una infracción al principio de la ilegalidad ni a la prohibición de analogía, por cuando es del espíritu de la ley punir a quienes pongan en peligro el "libre desarrollo de la autodeterminación del menor", lo cual se estaría llevando a cabo igualmente siendo este hecho presencial o bien a través de cámara, grabación de voz, teléfono u otro medio tecnológico.

3.7.3.3 Jurisprudencia nacional

En autos rol Nº 9.875-11, la Corte de Apelaciones se refirió a actos constitutivos de *bullying* en un colegio de Santiago, estimando que si bien la cancelación de matrícula o situación de condicionalidad de un alumno que incurre en conductas contrarias a la política del colegio pueden legítimamente ser reguladas a través del reglamento interno, esto no significa que por ello no deban adaptarse a los estándares nacionales sobre debido proceso, en el sentido de que debe existir derecho a defensa. Debe entenderse, por tanto, que para la prueba del *bullying* tampoco puede ser tomada en cuenta aquella que haya sido obtenida de forma contraria a las leyes y derechos fundamentales de las personas.

Debe entenderse, por tanto, que para la prueba del *bullying* tampoco puede ser tomada en cuenta aquella que haya sido obtenida de forma contraria a las leyes y derechos fundamentales de las personas.

En el año 2020, la Corte Suprema confirmó la sentencia de la CA de Chillán, que desestimó la reclamación de un colegio de esa ciudad que fue condenado a una multa de 51 UTM, impuesta por la Superintendencia de Educación. Si bien el caso no se refiere a *ciberbullying* sino a acoso escolar físico, cobra relevancia que la Corte se refiera a la obligación del colegio de aplicar el protocolo de actuación frente a situaciones de *bullying*, lo que lo "obligaba a la constitución del Comité, la recolección de información, la designación del responsable, efectuar entrevistas al acosado, al acosador y demás involucrados y apoderados del acosado y acosador, y la adoptación de medidas correctivas, reparatorias y de protección a la víctima".

3.8 El singular problema de la llamada "estafa informática"

Ni la Ley Nº 19.223 ni el Código Penal entregan herramientas para enfrentar una conducta singular, o mejor dicho no tipificada, pero de gran interés penal: la estafa informática, internacionalmente conocida como fraude informático.

Se trata de aquella conducta consistente en actos deliberados e ilegítimos que causan perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos, o que se produce por cualquier interferencia en el funcionamiento de un sistema informático con la intención de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

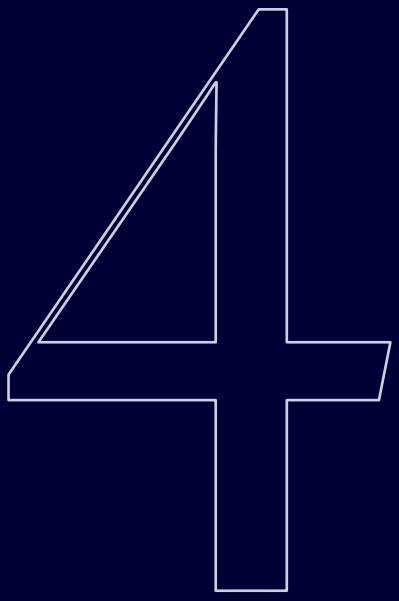
Nuestra legislación penal cubre las hipótesis de estafas y otros engaños, pero todos los tipos penales relacionados suponen que hay alguien, en concreto una persona, que es engañada, y por eso se castiga a "el que defraudare a otro". Y ello no ocurre en este tipo de fraudes, pues ninguna persona es directamente burlada.

Poniéndolo en blanco sobre negro, la estafa informática es aquella manipulación sobre variables que manejan las máquinas, a efectos de que ellas hagan "algo" en beneficio de quien no deben (usualmente unido al perjuicio de un tercero). Tal fue el caso de las personas que alteraron las tarjetas BIP del sistema de transporte público a fin de que en dicho monedero electrónico aparecieran cifras que nadie había depositado, de manera que los torniquetes de acceso los dejaran pasar, descontando cifras imaginarias.

Pero como dice el título de este acápite, se trata de un problema singular: nuestra legislación penal cubre las hipótesis de estafas y otros engaños, pero todos los tipos penales relacionados suponen que hay alguien, en concreto una persona, que es engañada, y por eso se castiga a "el que defraudare a otro". Y ello no ocurre en este tipo de fraudes, pues ninguna persona es directamente burlada.

Las máquinas, además de no ser personas, no son susceptibles de ser engañadas, pues sencillamente ejecutan reglas de programación y, si se dan las condiciones previstas por el programador, llevan a cabo las instrucciones que se les ha dado, y no hay más. Como consecuencia, esta conducta no tipificada en nuestra legislación, por regla general, no será sancionada aun cuando ella cause perjuicios, pues ningún humano ha sido engañado y, sin embargo, ha ocurrido perjuicio.

Este tipo de conducta sí es considerado como delito por el Convenio de Budapest y, tras su adhesión por Chile, se introdujo la figura del fraude informático en el proyecto de ley que pretende reformar la legislación a este respecto, esto es, el Boletín Nº 12.192-25.



Documento electrónico y firma electrónica avanzada

← Índice de contenidos

Esta ley tuvo como propósito principal equiparar los documentos electrónicos a aquellos que constan en papel, como soporte escrito de actos y contratos, para lo cual declara que estos últimos tienen que entenderse como escritos para todos los efectos legales.

Gracias a internet y los servicios de la sociedad red, la formación del consentimiento entre ausentes puede concretarse de forma instantánea, y lo mismo sucede en general con la suscripción remota de documentos, que tienen plena eficacia legal aun cuando nunca consten en formato papel.

Ello nos lleva a estudiar la Ley Nº 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación, así como su normativa complementaria.

Esta ley tuvo como propósito principal equiparar los documentos electrónicos a aquellos que constan en papel, como soporte escrito de actos y contratos, para lo cual declara que estos últimos tienen que entenderse como escritos para todos los efectos legales. Su aporte es otorgar certeza jurídica a las personas e instituciones que desarrollan sus relaciones jurídicas en internet.

4.1 Marco general de la Ley Nº 19.799, sus reformas y reglamentos

Tradicionalmente, se entendía que un documento era necesariamente un papel y una firma un trazo escrito realizado por una persona a través de su propia mano. Y aunque a través de la innovación tecnológica esto ha cambiado sustancialmente, la "percepción" ciudadana sigue estimando necesario que el contenido del documento y la firma del mismo conste en un papel.

Sin embargo, el legislador por regla general es neutral al momento de referirse a la firma (no define la forma específica que debe adoptar), y solo cuando quiso que esta fuera otorgada de puño y letra del signatario lo dijo expresamente de esa forma.

Por regla general también, el legislador chileno, en particular el del Código Orgánico de Tribunales, nunca dice en qué debe consistir una firma y tampoco señala que el documento debe constar en papel, aun cuando de la lectura de diversas disposiciones legales podría inferirse ello; sin embargo, su redacción también puede dar lugar a documentos y firmas electrónicas.

Es en este marco que se publica, el 12 de abril de 2002, la Ley Nº 19.799, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, que apartó definitivamente las dudas y, más todavía, estableció la equivalencia funcional entre medios tradicionales y medios tecnológicos en lo que a esta materia se refiere, proscribiendo la discriminación entre una y otra. Particularmente, en su artículo 3º:

> "Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito. (…) La firma electrónica, cualquiera sea

> su naturaleza, se mirará como firma manuscrita para todos los efectos legales, sin perjuicio de lo establecido en los artículos siguientes".

Solo hace un alcance en particular: si bien no se discrimina entre firma ológrafa y firma electrónica, cuando se trate de documentos que tengan la calidad de instrumento público y sean electrónicos, "deberán suscribirse mediante firma electrónica avanzada".

4.2 Conceptos generales: documento electrónico, firma electrónica y prestadores de servicios de certificación

¿Qué es esto de la firma electrónica avanzada? ¿Acaso hay firmas electrónicas "primitivas" o "no avanzadas"? Contestar esto nos lleva a las cuestiones de conceptualización general, que explicaremos aquí brevemente.

Primero tenemos que recordar qué es un "documento", cuestión relativamente sencilla si nos apoyamos en la inestimable ayuda del diccionario de la Real Academia Española, que nos dice que es una cosa que sirve para testimoniar un hecho o informar de él y, también, el escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.

¿Y el documento electrónico, entonces, qué es? El diccionario de la RAE no tiene una acepción al respecto, pero sí la propia Ley Nº 19.799, que nos dice que "es 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" (art. 2º).

¿Significa esto acaso que un documento escrito en un programa procesador de texto como Microsoft Word es un documento electrónico? Desde luego. ¿Y si luego lo convierto en archivo PDF sigue siendo documento electrónico? Por supuesto que sí.

Y si digitalizo una escritura pública con la ayuda de un escáner, ¿también es un documento electrónico? No, porque no se corresponde con la definición legal, que señala que tiene que haber sido **creado, enviado y comunicado por medios electrónicos**, en circunstancias de que la escritura pública de nuestro ejemplo nació a la vida en ese extraño formato no estandarizado que llamamos "oficio chileno", con firmas ológrafas ya incluidas. Lo que nos lleva al tema de las firmas.

Nuestro Código Orgánico de Tribunales no define legalmente lo que es una firma, por lo que tendremos que recurrir nuevamente al diccionario de la RAE, que nos dice que en un rasgo o conjunto de rasgos,

realizados siempre de la misma manera, que identifican a una persona y sustituyen su nombre y apellidos para aprobar o dar autenticidad a un documento. Por cierto, tal definición se corresponde con la firma manuscrita u ológrafa solamente, pero no con la firma electrónica.

La Ley Nº 19.799 no habla de solo una firma electrónica, sino que dos de ellas y con características asaz distintas: a una se le llama "avanzada" y a la otra sencillamente "firma electrónica", pero la doctrina denomina "simple" a esta última, para distinguirla de la avanzada.

Y así, la firma electrónica *simple* es cualquier sonido, símbolo o proceso electrónico que permite al receptor de un documento electrónico identificar al menos formalmente a su autor. Por ejemplo, cuando se escribe un correo electrónico y al final del mismo uno escribe su nombre, eso es de acuerdo a la ley una firma electrónica, pues son símbolos que permiten identificar al autor. Es más, si el correo electrónico fuera, por ejemplo, juan.pablo.gonzalez@gmail.com, perfectamente podríamos entender que estamos ante una firma electrónica simple, pues se trata de símbolos que nos permiten identificar que nos ha escrito un tal "Juan Pablo González".

Se trata de una firma "certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control", y que tiene la particularidad de permitir la detección de cualquier modificación de la misma, así como verificar la identidad de quien firma, impidiendo que pueda desconocer la falta de integridad del documento.

Sin embargo, cuando hablamos de firma electrónica avanzada, no se trata sencillamente de la misma firma simple con algún proceso tecnológico más sofisticado, sino de una realidad completamente distinta. Se trata de una firma "certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control", y que tiene la particularidad de permitir la detección de cualquier modificación de la misma, así como verificar la identidad de quien firma, impidiendo que pueda desconocer la falta de integridad del documento (no puede alegar que sí firmó, pero al documento le faltan hojas) y tampoco la autoría del mismo.

¿Cómo se logra todo esto? Hay un elemento distinto en la firma electrónica avanzada que hace toda la diferencia: existe un tercero, un particular denominado "prestador de servicios de certificación", que es una entidad habilitada para ejercer la función por la Subsecretaría de Economía y Empresas de menor tamaño, en su rol de entidad acreditadora de dichos prestadores de servicios de certificación.

Los documentos electrónicos con firma electrónica avanzada pueden presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, constituyen plena prueba de acuerdo con las reglas generales aplicables a los documentos.

Y en una apretada síntesis, esta actividad de certificación consiste en verificar que la persona que suscribe un documento con firma electrónica avanzada es, inequívocamente, quien dice ser.

¿Y por qué alguien recurriría a estos prestadores para certificar su firma?[70] Por una diferencia abismal entre los efectos probatorios de suscribir un documento con firma electrónica avanzada o hacerlo con firma electrónica simple: los documentos electrónicos con firma electrónica avanzada pueden presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, constituyen plena prueba de acuerdo con las reglas generales aplicables a los documentos.

Con todo, hay una excepción, derivada de un error legislativo: las firmas electrónicas ligan al documento con el contenido del mismo y con su autor, pero el legislador omitió referirse al tema de la fecha, de manera que la firma electrónica avanzada por sí sola no da fe de la fecha en que se suscribió un documento, por lo que se requiere contratar con los señalados prestadores un servicio adicional llamado "*time stamping*" o servicio de sellado de tiempo.

Ahora bien, ¿por qué es homologable la firma electrónica avanzada a la firma manuscrita? A continuación revisaremos las razones.

4.2.1 Identidad de los contratantes

La firma electrónica avanzada considera, en el procedimiento de **otorgamiento de certificado** de firma a una persona, la verificación fehaciente de la identidad de la misma. Esto se logra a través de la exigencia de comparecencia personal del titular del certificado, ya sea ante el prestador de servicios de certificación, o ante un oficial de registro civil o ante un ministro de fe (por ejemplo un notario) al momento de la obtención de la firma. A partir de la entrada en vigor del Decreto N° 24, de 22 de febrero de 2019, también se hace mediante el empleo de Clave Única del Estado, provista por el Servicio de Registro Civil e Identificación.

70 Al mes de enero de 2021, y de acuerdo al sitio web oficial, en Chile existen ocho empresas habilitadas para certificar firmas electrónicas.

En este último caso, además de integrarse técnicamente con los sistemas del Servicio de Registro Civil e Identificación, el proveedor de servicios de certificación deberá implementar un mecanismo complementario de comprobación de identidad del solicitante para la emisión del Certificado de Firma Electrónica Avanzada. A ello agrega que "el o los mecanismos complementarios que decida implementar el Certificador o Prestador de Servicios de Certificación deberán declararse en las Políticas y Prácticas de Certificación, conforme a lo dispuesto en el artículo 6º del decreto supremo Nº 181, de 2002, del Ministerio de Economía, Fomento y Turismo, con expresa mención de la fiabilidad que estos mecanismos tienen", entendiéndose que así se cumplen los requisitos previstos en el artículo 12 letra e de la Ley Nº 19.799, sobre comprobación fehaciente de la identidad de la persona.

Si bien la verificación fehaciente de la identidad del titular del certificado es un requisito en su otorgamiento, la Ley Nº 19.799 exige además que dicho dispositivo se encuentre bajo el exclusivo control del firmante. A estos efectos, la normativa, en su inicio exigía que los datos de creación de firma (clave privada) se encontraran almacenados en un dispositivo físico que permaneciera en poder del firmante, pero el Decreto Nº 24, en su artículo 5º, autoriza la posibilidad de que se encuentren bajo custodia del proveedor de servicios de certificación, al disponer lo siguiente:

> "Los certificados de firma electrónica avanzada, que se emitan utilizando el medio de comprobación de identidad referido en esta norma técnica, **podrán ser almacenados en dispositivos, individuales o masivos**, que cumplan con el estándar FIPS PUB 140-2: Security Requirements for Cryptographic Modules (mayo 2001). Los datos de creación de firma, almacenados en dispositivos masivos, **deberán encontrarse protegidos mediante un segundo factor de seguridad** que permita al titular controlar que el acceso y utilización de éstos **únicamente pueda ser realizado por él.** Estos factores de seguridad deberán encontrarse declarados de manera clara en las Políticas y Prácticas de Certificación, con expresa mención de la fiabilidad que éstos tienen".

De esta manera, la firma electrónica avanzada resuelve el problema de la identidad de las personas y su comparecencia personal al acto de firma. Estos sistemas se han potenciado con la implementación de técnicas de encriptación, que garantizan que los mecanismos de firma no serán conocidos indebidamente por terceros.

4.2.2 Integridad y autenticidad del documento

La integridad del documento se ha resuelto técnicamente a través de los sistemas de encriptación, que también garantizan que el mensaje no ha sido modificado en el tiempo/espacio mediante entre su envío (entendiendo por tal la salida de la esfera de control técnico del autor del mensaje) y recepción (entendiendo por tal la llegada al destinatario final y no actos técnicos de intermediación).

Tengamos en cuenta que un dato, computacionalmente hablando, constituye una unidad básica de información. Un dato puede contener voz, imagen o texto. A su vez, un mensaje es un conjunto de datos vinculados y destinados a ser transferidos mediante un sistema telemático. Finalmente, la transferencia electrónica de mensajes de datos implica el envío de un mensaje de datos desde una computadora a otra, sirviéndose de alguna red telemática. Estos conceptos aplican con independencia del sistema informático que se utilice.

Un mensaje de datos en materia contractual puede estar inserto en un proceso de formación del consentimiento (oferta, contraoferta, aceptación, rechazo) o en la fase de ejecución de un contrato, mediante entrega del bien en soporte digital (un software, una canción o una colección de canciones, un video, tratándose de transacciones de comercio electrónico directo). También podría contener "dinero digital" o ajustes en estados de cuenta. Este modelo es replicable tanto en la esfera de lo público como entre privados.

Técnicamente, es factible determinar los computadores de entrada y salida de los mensajes de datos. Asimismo, mediante sistemas auxiliares de identificación, tales como la firma digital y/o los sistemas biométricos, puede identificarse a la persona que manipuló el equipo computacional correspondiente a efectos de enviar o recibir el mensaje. Finalmente, mediante sistemas de encriptación de información es posible asegurar la integridad del mensaje.

4.3 Principios jurídicos de la Ley Nº 19.799 y su aplicación

En cuanto a su naturaleza jurídica, esta ley vino a dar certeza en el ámbito del tráfico jurídico en línea, sin una alteración sustancial de las condiciones legales y reglamentarias vigentes, ni el establecimiento de condiciones extremadamente gravosas para su implementación por parte de los actores que se desenvuelven en su prestación y uso.

Asimismo, reconociendo las condiciones transnacionales de las redes de telecomunicaciones, se procuró que el marco regulador fuera compatible con lo ya establecido en otros entornos y la homologación de certificados emitidos en el extranjero.

La ley se basa en los siguientes principios: a) neutralidad tecnológica, b) libertad de prestación de servicios, c) libre competencia, d) compatibilidad internacional, y e) equivalencia del soporte electrónico respecto del soporte papel. Además, conforme argumentó el Ministerio de Economía en su tramitación, obedece al principio de intervención mínima. La misma ley dispone que toda interpretación de sus normas deberá guardar armonía con estos principios.

En aplicación de la garantía de libre ejercicio de cualquier actividad económica (art. 19 Nº 21 CPR), y conforme al principio de **neutralidad tecnológica,** la ley no limita los sistemas de identificación o integridad en uso al momento de su dictación, sino que deja abierta la puerta a las nuevas aplicaciones a que dé lugar el desarrollo tecnológico. Lo contrario, además de limitar las decisiones que a este respecto deben tomar los distintos sectores productivos, generaría barreras de entrada al mercado de certificación, desincentivaría a los privados para realizar la actividad económica prevista en la norma, y dificultaría la entrada de Chile a los beneficios de la sociedad red.

Como una manifestación de las libertades económicas consagradas en la Constitución, la ley declara los principios de **libre prestación de servicios** y **libre competencia**, conforme a los cuales la prestación de servicios de certificación de firma electrónica no está sujeta al control previo de la autoridad, salvo en el caso de la firma electróni-

ca avanzada, que requiere previa acreditación del prestador ante la Subsecretaría de Economía y Empresas de menor tamaño. Tengamos en cuenta al respecto que, reiteradamente, la jurisprudencia de la Corte Suprema ha considerado que "el derecho a desarrollar cualquier actividad económica constituye una manifestación del orden público económico, el que es regulado por el poder público".

Otro principio reconocido es el de **compatibilidad internacional,** que impone que nuestro derecho adopte aquellas categorías que se reconocen en otros entornos, a fin de asegurar seguridad jurídica en un mundo globalizado. En virtud de este principio, los proveedores nacionales de servicios de firma electrónica podrán homologar certificados de firma electrónica avanzada emitidos en el extranjero, con lo cual dichos certificados tendrán plena eficacia en Chile.

Finalmente, el principio de **equivalencia funcional** no es sino una expresión del principio de igualdad ante la ley, que impone reconocer iguales efectos al acto o contrato que conste en medios electrónicos o a la firma suscrita por estos medios, a los que tendría si constara en otros medios más tradicionales o la firma fuera ológrafa o autógrafa.

Manifestaciones de este principio es el reconocimiento de la validez y eficacia jurídica de los documentos firmados con firma electrónica, tanto constitutivo como acreditativo, otorgando incluso el valor de **plena prueba** a los documentos firmados con firma electrónica avanzada. El desconocimiento de esta cualidad representaría una discriminación ilegal y arbitraria en los términos previstos por el texto constitucional.

4.4 Impacto de la Ley Nº 19.799 y su ámbito de aplicación

Esta ley tiene **aplicación general** y no está limitada al ámbito comercial o mercantil. Su aplicación abarca tanto los actos de los organismos públicos como los de entes y personas privadas. Así está previsto en su artículo 1º inciso primero, al señalarse:

> "La presente ley regula los documentos electrónicos y sus efectos legales, la utilización en ellos de firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso".

No hay eximentes ni tampoco establece cláusulas de exclusión para notarios, conservadores, archiveros u otros auxiliares de la administración de justicia.

Por otra parte, en cuanto a su aplicación a los sistemas de redes cerradas de transferencia de datos, la ley de firma electrónica no afecta su validez ni aplicación. Esto por diversas razones, a saber: a) técnicamente se estima que los sistemas cerrados dan mayores garantías de ser resguardadas de ataques o intrusiones ilegítimas; y b) jurídicamente, en nuestro derecho uno de los pilares fundamentales es la autonomía de la voluntad, garantizada constitucionalmente a través del artículo 1º incisos primero y tercero y 19 Nº 21 y Nº 23 de la Constitución Política de la República, garantía que ampara los acuerdos entre particulares que establecen estos sistemas. Para impedirlos, por tanto, debería dictarse una norma expresa en tal sentido, la que debiera fundarse en una razón de orden público, por representar una restricción de la referida garantía.

Recordemos que nuestro ordenamiento jurídico no define un documento en cuanto tal, sino que se alude, primero, a los instrumentos públicos como aquellos que son otorgados con las solemnidades legales y ante el competente funcionario, y segundo, a los instrumentos privados, que en general tendrán eficacia entre las partes.

Respecto del soporte en que consta un documento, el artículo 422 del Código Orgánico de Tribunales dispone que las copias de una escritura pública podrán ser "manuscritas, dactilografiadas, impresas, fotocopiadas, litografiadas o fotograbadas. En ellas deberá expresarse que son testimonio fiel de su original y llevarán la fecha, la firma y sello del funcionario autorizante". De su parte, el artículo 428 dispone que "las palabras que en cualquier documento notarial aparezcan interlineadas, enmendadas o sobrepasadas, para tener valor deberán ser salvadas antes de las firmas del documento respectivo, y en caso de que no lo sean, se tendrán por no escritas".

En sede tributaria, el artículo 30 inciso final del Código Tributario dispone que "la impresión en papel que efectúe el Servicio de los informes o declaraciones presentadas en los referidos medios, tendrá el valor probatorio de un instrumento privado emanado de la persona bajo cuya firma electrónica se presente". Mucho antes, el artículo 71 bis del DS 55 de 1977, del Ministerio de Hacienda, había previsto que "la Dirección del Servicio de Impuestos Internos podrá autorizar la emisión de facturas, facturas de compra, liquidaciones, notas de débito y notas de crédito impresas por medios computacionales. Los mencionados documentos deberán imprimirse en formularios previamente timbrados por dicho Servicio y deberán emitirse en los ejemplares y con las especificaciones que determine su Dirección. En uso de estas facultades podrá autorizarse que el envío de los ejemplares que correspondan al cliente se efectúe por medio de la impresión de ellos directamente en su sistema computacional, simultáneamente con la impresión de los ejemplares que debe conservar el emisor y usándose los mismos medios tecnológicos".

Todas estas normas, anteriores a la Ley Nº 19.799, si bien no lo dicen expresamente, parten de la base de que un documento consta en papel. Sin embargo, no debemos olvidar que se refieren a actos a los que el legislador les ha dado algún grado de solemnidad.

En materia de derecho privado, en cambio, conforme al principio de autonomía de la voluntad, los actos y contratos de esta naturaleza se rigen en general por el consensualismo; en consecuencia, el solo consentimiento de las partes basta para perfeccionar el contrato, con

independencia de que conste o no por escrito y en soporte papel (art. 1545 CC) y la formalidad de escrituración contemplada en los artículos 1708 y 1709 del Código Civil, se establece por vía de prueba.

Técnicamente, un documento generado o que consta en un soporte informático constituye un conjunto de bits, una combinación de dígitos 0 y 1 que, descifrados por una máquina capaz de ello, representan imágenes, sonidos o textos que dan cuenta de datos atribuibles a ciertos hechos. Su representación digital constituye un formato que le sirve de soporte. Este podrá ser almacenado en sistemas ópticos, digitales o magnéticos, podrá ser copiado, o transmitido a través de sistemas telemáticos. Estas características no afectan la funcionalidad del documento, sino solo su forma de representación y soporte. De ahí que el artículo 2º letra d de la Ley Nº 19.799 defina documento electrónico 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", definición que solo adapta el concepto tradicional de documento al nuevo entorno tecnológico, sentando las bases de la equivalencia funcional a la que nos hemos referido antes.

El reconocimiento expreso de la **equivalencia funcional y no discriminación** de los documentos suscritos con firma electrónica están previstos en los artículos 3º y 7º de la Ley Nº 19.799, en los términos siguientes:

> "Artículo 3º. Los actos y contratos otorgados o celebrados por personas naturales o jurídicas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten de ese modo, y en todos aquellos casos en que la ley prevea consecuencias jurídicas cuando constan igualmente por escrito".
>
> "Artículo 7º. Los actos, contratos y documentos de los órganos del Estado, suscritos mediante firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los expedidos por escrito y en soporte de papel.

Documentos que según la ley no pueden suscribirse electrónicamente aunque sean suscritos por personas privadas: a) aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico; b) aquellos en que la ley requiera la concurrencia personal de alguna de las partes, y c) aquellos relativos al derecho de familia.

> Con todo, para que tengan la calidad de instrumento público o surtan los efectos propios de éste, deberán suscribirse mediante firma electrónica avanzada".

Esta equivalencia, en todo caso, se rompe tratándose de los documentos que según la ley no pueden suscribirse electrónicamente aunque sean suscritos por personas privadas: a) aquellos en que la ley exige una solemnidad que no sea susceptible de cumplirse mediante documento electrónico; b) aquellos en que la ley requiera la concurrencia personal de alguna de las partes, y c) aquellos relativos al derecho de familia.

Ahora bien, es importante tener presente que la ley considera que el documento electrónico firmado con FEA y que cumple las condiciones y requisitos para ser plena prueba es aquel que ha sido creado, generado, firmado y almacenado de manera posterior en medios electrónicos.

Respecto de las copias impresas, el Decreto Nº 181 de 2002 dispone:

> "Artículo 45. Los documentos electrónicos suscritos por medio de firma electrónica avanzada deberán contener un mecanismo que permita verificar la integridad y autenticidad de los mismos al ser impresos".

Se ha entendido que este mecanismo es un código de verificación que permite consultar, contra el repositorio, que se trata de un documento válidamente firmado, que la firma se encuentra vigente y que no ha sido alterado con posterioridad al proceso de firmado.

Ahora, la firma es un mecanismo previsto para la identificación de la persona que concurre a la generación de un documento, y que al ser "estampada" en este se constituye en señal de aceptación de sus términos. Según la definición de la Real Academia, es el nombre y apellido o título de una persona, que esta pone al pie de un documento escrito de mano propia o ajena para darle autenticidad, para expresar que se aprueba su contenido, o para obligarse a lo que en él se dice.

No obstante, y como ya hemos señalado, la legislación chilena no prevé una definición general de firma, sino que encontramos diversas alusiones a esta institución cuando regula actos formales o solemnes, o se refiere a la prueba de las obligaciones y/o la actuación de ciertos órganos públicos en el ejercicio de sus funciones.

A vía de ejemplo se puede señalar el artículo 434 Nº 4 del CPC (títulos ejecutivos). Asimismo, en el Código Civil se hace alusión a la firma en distintos artículos referidos a la suscripción de documentos, tales como testamento (arts. 1018, 1020, 1029, 1042, 1048 CC); inventario (arts. 380, 1766, 1791 CC); transferencia de bienes raíces (art.690 CC); pago por consignación (art. 1600 CC); documentos (arts. 1701, 1703, 1704, 1705 CC); cesión de derechos (art. 1903 CC); arrendamiento (art. 1921 CC); mandato (art. 2166 CC, en que además se utiliza la formulación "de su mano si el mandatario lo exigiere"); inscripción de hipoteca (art. 2432 CC).

En el Código de Comercio se hacen alusiones al respecto en los artículos 56 y 71, referido a las obligaciones de los corredores; 174, referido a carta de porte; 344 y 346, sobre ciertas autorizaciones a los dependientes de comercio; 372, sobre firma por poder del mandatario; 378, relativo a la oportunidad de entero de aportes a sociedad; 549, sobre contrato de seguro; 785, sobre carta de crédito; 805, en cuanto a firma del prestamista en pagaré, confesando deuda; 832, sobre contratos sobre naves; 913, bitácora; 923, documentos de embarque; 1014, conocimiento de embarque.

Otros ejemplos son el artículo 1024, sobre acuerdos de definición de competencia arbitral, y entre ellos cabe destacar de nuevo el artículo 2166 del Código Civil, referido a la que emana del mandante en que se exige que sea "de su mano si el mandatario lo exigiere".

Todo esto nos lleva a presumir que, cuando el legislador quiso que la firma se estampe en el documento directamente de la mano del firmante, lo dijo expresamente.

En este contexto, el reconocimiento de la firma electrónica avanzada con valor de plena prueba denota que puede satisfacer las funciones esenciales de la firma, cuales son el identificar al suscriptor del

documento y ser señal de aceptación de las declaraciones que en él se contienen. A estas funciones esenciales agrega la de garantizar la integridad de los documentos o mensajes.

Si bien no era estrictamente necesario, la Ley Nº 19.799 define firma electrónica en su artículo 2º letra f como "cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor". A continuación, en la letra g define firma electrónica avanzada como "aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría".

Esta definición funcional de firma, unida a la asimilación de los efectos jurídicos de la firma electrónica a la ológrafa, simplifican este punto en tanto se construye un marco normativo en torno a este único concepto, permitiendo de esta forma un tratamiento más uniforme y transparente, con las consecuentes externalidades positivas en cuanto a la seguridad y certeza jurídica.

En cuanto al momento en que se realiza el acto de firma, el Decreto 181 del Ministerio de Economía dispone que los servicios de sellado de tiempo deberán ajustarse a los siguientes estándares:

> "ETSI TS 102 023, v.1.2.1 y v.1.2.2. Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities.
>
> ETSI TS 101 861 V1.3.1 Time-stamping profile.
>
> ISO/IEC 18014-1:2008 Information technology - Security techniques - Time-stamping services - Part 1: Framework.
>
> ISO/IEC 18014-2:2009 Information technology - Security techniques - Time-stamping services - Part 2: Mechanism producing independent tokens.

ISO/IEC 18014-3:2009 Information technology - Security techniques - Time-stamping services - Part 3: Mechanisms producing linked tokens.

RFC 3161 Internet X.509 Public Key Infrastructure Time - Stamp Protocol (TSP) (2001), RFC 5816 (update), ANSI ASC X 9.95.

RFC 3628 Requirements for Times Stamping Authorities.

NIST Special publication 800-102, Sept. 2009".

4.5 El certificado de firma electrónica y la actividad de certificación

Si bien no es obligatorio acreditarse, conforme a lo que dispone el artículo 2º letra c y en concordancia con el artículo 11 de la Ley 19.799, nos referiremos a los proveedores del servicio de certificación de firma electrónica avanzada (FEA).

Se trata de empresas tecnológicas que se han sometido a un proceso de acreditación ante la Subsecretaría de Economía y Empresas de menor tamaño, el cual consiste en la verificación de su adecuación a los estándares técnicos vigentes, al análisis de sus prácticas de certificación, mantención de un seguro de responsabilidad civil, entre otras exigencias legales y reglamentarias (art. 15 inciso segundo, Ley Nº 19.799).

Estas empresas proveen a los usuarios un "certificado de firma digital", esto es, un archivo digital que atestigua que un par de claves, pública y privada, corresponden a una persona natural o jurídica o a una entidad determinada, que tienen presencia en la red. En términos aún más simples, es un documento electrónico que da cuenta de una clave y de los datos de identificación de su titular.

Estos proveedores podrán emitir certificados y además homologar certificados emitidos por entidades extranjeras, haciéndose responsables de dichos certificados tanto frente al titular como a terceros que contraten con ellos. Entre los certificados que emiten, destacan los siguientes:

Certificados de servidores	Certificado de pertenencia de un servidor a una determinada persona natural o jurídica y de los identificadores correspondientes a dicho servidor.
Certificados personales	Aquellos que certifican claves públicas de usuarios de la red, normalmente personas naturales.
Certificados de fabricantes de programas computacionales	Aquellos que certifican claves públicas de fabricantes de software, utilizados normalmente para garantizar que los "paquetes" no han sido objeto de alteraciones ilegítimas (tales como introducción de virus).

En todo caso, la actividad principal de estos prestadores es la de emitir certificados de firma electrónica de persona natural, definidos en la letra b del artículo 2º de la Ley Nº 19.799 como la "certificación electrónica que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica". El certificado de firma electrónica avanzada es aquel certificado que da fe del vínculo entre el firmante o titular del certificado y los datos de creación de la firma electrónica avanzada.

En cuanto a las menciones de los certificados que se emiten, conforme al artículo 15 de la ley, deberán contener al menos las siguientes:

> "a) Un código de identificación único del certificado, que en definitiva se traduce en un número de serie único por prestador
>
> b) Identificación del prestador de servicio de certificación, con indicación de su nombre o razón social, rol único tributario, dirección de correo electrónico, y, en su caso, los antecedentes de su acreditación y su propia firma electrónica avanzada;
>
> c) Los datos de la identidad del titular, entre los cuales deben necesariamente incluirse su nombre, dirección de correo electrónico y su rol único tributario, y
>
> d) Su plazo de vigencia".

Sin perjuicio de lo anterior, son menciones generalmente aceptadas y que se contienen en los certificados la identificación del protocolo utilizado y número de versión; algoritmos y parámetros de encriptación utilizados por el certificador; el período de validez; información sobre la clave pública; algoritmo, parámetros y la llave pública propiamente dicha. Esto, sin perjuicio de otras menciones que expresamente permite la legislación, tales como limitaciones de responsabilidad del prestador o límites a la firma (ya sea en razón de poderes o montos de las actuaciones firmadas a través de él).

4.5.1 La validez de los certificados

En cuanto a la validez de los certificados, la ley prevé distintas circunstancias por las cuales estos pierden sus efectos. En primer lugar, podrá producirse una suspensión temporal del certificado, fundada en problemas técnicos. En segundo lugar, atendido que los certificados no podrán tener un plazo de vigencia mayor a tres años, podrán extinguirse por el vencimiento del plazo para el cual fueron otorgados; adicionalmente, podrían extinguirse porque el proveedor los revoca fundado en a) la solicitud del titular del certificado; b) el fallecimiento del titular del certificado si es persona natural, o por su disolución tratándose de persona jurídica; c) por orden de tribunal competente mediante resolución judicial debidamente ejecutoriada; o d) por incumplimiento de las obligaciones del usuario, cuales son brindar declaraciones exactas y completas respecto de sus datos de identidad personal u otras circunstancias objeto de certificación; actualizar esta información en la medida que sus datos vayan cambiando, y custodiar adecuadamente los mecanismos de seguridad del funcionamiento del sistema de certificación que les proporcione el certificador.

En este caso, el prestador de servicios, previo a revocar el certificado, deberá informar al titular del mismo de los antecedentes que fundan su decisión.

En todo caso, habrá de tenerse en cuenta que la suspensión temporal o definitiva de los certificados será inoponible a terceros mientras no sea comunicada al público en general, a través de la publicación respectiva en el repositorio público que los prestadores deben mantener en su sitio web.

4.5.2 La acreditación fehaciente de la identidad del titular del certificado

Como hemos señalado, la ley impone a los proveedores de servicios de certificación de firma electrónica que en el otorgamiento de FEA deben comprobar fehacientemente –esto es, de manera indubitada– la identidad del firmante.

Este procedimiento se debe consignar en las prácticas de certificación transparentes, no discriminatorias, las que deben estar escritas en idioma castellano. Entre su contenido esencial y en lo que nos interesa sobre este punto, destaca lo siguiente:

> "c. Identificación y autenticación, debiendo describirse tanto los procesos de autenticación aplicados a los solicitantes de certificados, como los procesos para autenticar a los mismos cuando piden suspensión o revocación de certificado.
>
> d. Requerimientos operacionales, debiendo contener información operacional para los procesos de solicitud de certificado, emisión de certificados, suspensión y revocación de certificados, procesos de auditoría de seguridad, almacenamiento de información relevante, cambio de datos de creación de firma electrónica, superación de situaciones críticas, casos de fuerza mayor y caso fortuito, y procedimiento de término del servicio de certificación".
>
> "Artículo 30. Tratándose de un certificado de firma electrónica avanzada, deberá el prestador de servicios de certificación comprobar fehacientemente la identidad del solicitante antes de la emisión del mismo, de conformidad con las normas técnicas.
>
> Dicha comprobación la hará el prestador de servicios de certificación, ante sí o ante notario u oficial del Registro Civil, requiriendo la comparecencia personal y directa del solicitante o de su representante legal si se tratare de una persona jurídica".

Asimismo, hemos sostenido que el Decreto N° 24 de 2019 autoriza que este proceso se entienda cumplido al momento de la obtención de la Clave Única del Estado, en la medida que se utilice además un segundo factor de autenticación.

Veamos cómo se desarrolla el proceso de enrolamiento a efectos de cumplir con esta exigencia:

> a) Comparecencia personal del solicitante del certificado de firma ante el proveedor de servicios de certificación, un oficial de registro civil u otro ministro de fe. Tratándose de las personas

que cuentan con clave única, se entiende que este requisito se retrotrae al momento de obtener esta clave.

b) Fotografía de la persona y registro de la foto en la ficha de la persona asociada al certificado de FEA.

c) Verificación de validez y vigencia de la cédula de identidad a través de integración de servicios con el Servicio de Registro Civil e Identificación.

d) Fotocopia y registro de la cédula de identidad en la ficha de la persona asociada al certificado de FEA.

e) Tratándose de la verificación de identidad a través de clave única, mediante el empleo de un segundo factor de autenticación, tal como preguntas que solo la persona conoce, mediante servicio de integración con Registro Civil, pruebas de vida en que se constate que la persona se encuentra frente a la pantalla y no es un robot, y otras semejantes.

f) Enrolamiento informático de la persona, creando esta su propia clave de activación.

g) Entrega del control exclusivo del mecanismo de creación de firma.

Recién entonces la persona quedará en condiciones de firmar con el certificado de FEA.

Todos estos pasos, estandarizados en normas ISO, han sido recogidos en los decretos asociados a la ley de firma electrónica, especialmente el Decreto 181 de 2002, del Ministerio de Economía, de acuerdo a modificación introducida en 2012 mediante Decreto 154 de esa misma cartera:

"ETSI TS 102 042 V1.1.1 (2002-04). Technical Specification. Policy requirements for certification authorities issuing public key certificates.

NCh2805.Of2003 Tecnología de la Información - Requisitos de las políticas de las autoridades certificadoras que emiten certificados de claves públicas".

4.6 El proceso de firma de documentos

Luego, el proceso posterior es asimismo mejor asegurado, en cuanto a la certeza jurídica, a través de sistemas informáticos como se describe a continuación:

a) Al momento de firmar, el sistema en primer lugar verifica que la persona se encuentre frente al sistema y no se trate de un robot, para ello le pide pruebas de vida.

b) Luego, superada esta prueba, la persona puede proceder a firmar, para ello debe conocer su usuario y clave.

c) Solo después de que la persona cumple los requisitos de usuario y clave se activará el proceso de firma.

d) Una vez firmado el documento, de manera personal por el titular del certificado, aquel es remitido al notario para que constate que todo el proceso se cumplió de manera segura, sin interferencias de tercero. Para eso se utiliza un canal seguro.

e) El notario a su vez debe utilizar su propia firma electrónica avanzada.

f) De todo lo anterior queda registro auditable en los sistemas del notario, a diferencia de los instrumentos privados físicos, en que la persona se los lleva sin que quede registro alguno de que se haya procedido conforme a la ley, debiendo en ese caso solo hacerse fe de las declaraciones del notario. Este registro se mantiene bajo el exclusivo control del notario, sin que se trate de algún gestor documental compartido, lo cual acota la responsabilidad y riesgo de manipulaciones indebidas.

Mientras los certificados de firma electrónica avanzada se encuentran vigentes, otorgarán el valor de plena prueba a los documentos que se suscriba a través de ellos.

Mientras los certificados de firma electrónica avanzada se encuentran vigentes, otorgarán el valor de plena prueba a los documentos que se suscriba a través de ellos.

4.7 Responsabilidad de los prestadores del servicio de certificación

Los proveedores de servicios de certificación están sujetos a la **obligación de publicidad**, en virtud de lo cual deben contar con prácticas de certificación objetivas y no discriminatorias, las que deben estar escritas de manera clara y en idioma castellano.

Además deben someterlas al análisis del regulador y mantenerlas en sus sitios web en un lugar visible, para que cualquier persona pueda revisarlas. Esto es consistente con lo que prevé la ley de protección a los consumidores.

Adicionalmente deben mantener un repositorio, también de libre acceso, de los certificados que han emitido y de los que vayan quedando sin efecto, incluyendo su vigencia y los datos de identificación de su titular, de forma tal que las personas puedan verificar si estos tenían validez y vigencia al momento de la firma. Al repositorio podrá accederse por medios electrónicos, de manera regular y continua. La publicación habrá de mantenerse durante a lo menos seis años desde la emisión inicial de cada certificado.

En caso de cese voluntario de actividades, el proveedor debe comunicar con dos meses de antelación a los usuarios y –tratándose del proveedor acreditado– a la Subsecretaría de Economía. En este plazo, los usuarios podrán oponerse al traspaso de sus datos y certificados a un tercer proveedor. Frente al silencio del usuario o su aceptación expresa, el proveedor deberá traspasar los certificados a un tercero.

En virtud del **deber de responsabilidad,** los proveedores tienen la obligación de indemnizar los perjuicios que hayan causado a los usuarios en el ejercicio de sus funciones. Para ello, los prestadores de servicios de certificación acreditados deben además mantener un seguro de responsabilidad civil.

Asimismo, es importante considerar que la ley prevé una **inversión en la carga de la prueba**, en el sentido de que es el prestador de servicios de certificación quien debe acreditar que actuó con debida

diligencia. Sin embargo, tratándose del proveedor acreditado, la ley establece en su favor una presunción de haber obrado con el debido cuidado, como una manifestación de reconocimiento de la acreditación como verificación de la idoneidad de sus procesos y sistemas.

El artículo 13 de la Ley Nº 19.799 precisa cuáles son los deberes del prestador de servicios de certificación, y en seguida el artículo 14 dispone que el cumplimiento de las obligaciones señaladas en las letras a, b, c, d y j del artículo precedente, por parte de los prestadores no acreditados de los servicios de certificación de firma electrónica, son antecedentes que el juez va a tener a la vista para los efectos de entender que actuó con la debida diligencia, de lo que se desprende el carácter facultativo de estas obligaciones tratándose de los proveedores no acreditados.

En lo que nos interesa, los proveedores acreditados deben cumplir los siguientes deberes:

> "a) Contar con reglas sobre prácticas de certificación que sean objetivas y no discriminatorias y comunicarlas a los usuarios de manera sencilla y en idioma castellano.
>
> b) En el otorgamiento de certificados de firma electrónica avanzada, comprobar fehacientemente la identidad del solicitante, para lo cual el prestador requerirá previamente, ante sí o ante notario público u oficial del registro civil, la comparecencia personal y directa del solicitante o de su representante legal si se tratare de persona jurídica;
>
> c) Mantener un repositorio de certificados, en los términos que se analizara antes.
>
> d) En el caso de cesar voluntariamente en su actividad, comunicarlo previamente, con una antelación mínima de dos meses al cese efectivo de la actividad, a cada uno de los titulares de firmas electrónicas certificadas por ellos, de la manera que establecerá el reglamento: En ella deberá informar a los usuarios acerca si tiene planificado traspasar los certificados a otros prestador y en la afirmativa cuales son los datos de la entidad que recibiría los

certificados y su derecho a oponerse al traspaso de los datos de sus certificados a otro prestador de servicios, en la fecha en que el cese se produzca.

e) En caso de cancelación de la inscripción en el registro de prestadores acreditados, el prestador deberá comunicar inmediatamente esta circunstancia a cada uno de los usuarios, indicándole si traspasará los certificados a otro prestador y en la afirmativa los datos del mismo y hacerle presente su derecho a oponerse al traspaso de los certificados de que es titular;

f)) En caso de existir oposición al traspaso de certificados en los casos antes previstos, deberán dejar sin efecto los certificados afectados por esta negativa.

g) Solicitar la cancelación de su inscripción en el registro de prestadores acreditados llevado por la Entidad Acreditadora, con una antelación no inferior a un mes cuando vayan a cesar su actividad, y comunicarle el destino que dará a los datos de los certificados, especificando, en su caso, si los va a transferir y a quién, o si los certificados quedarán sin efecto;

h) Publicar en sus sitios de dominio electrónico las resoluciones de la Entidad Acreditadora que los afecten;

i) Pagar el arancel de la supervisión, el que será fijado anualmente por la Entidad Acreditadora y comprenderá el costo del peritaje y del sistema de acreditación e inspección de los prestadores;

j) Indicar a la Entidad Acreditadora cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, el inicio de un procedimiento de quiebra o que se encuentre en cesación de pagos, y

k) Cumplir con las demás obligaciones legales, especialmente las establecidas en esta ley, su reglamento, y las Leyes Nº 19.496, sobre Protección de los Derechos de los Consumidores, y Nº 19.628, sobre Protección de la Vida Privada".

El certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites a sus posibles usos, siempre y cuando dichos límites sean reconocibles por terceros, en cuyo caso el proveedor de servicios de certificación quedará eximido de responsabilidad sobre los daños y perjuicios causados por el uso que exceda dichos límites.

En materia de indemnización de perjuicios, el artículo 14 de la ley dispone:

> "Los prestadores de servicios de certificación serán responsables de los daños y perjuicios que en el ejercicio de su actividad ocasionen por la certificación u homologación de certificados de firmas electrónicas. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.
>
> Sin perjuicio de lo dispuesto en el inciso anterior, los prestadores no serán responsables de los daños que tengan su origen en el uso indebido o fraudulento de un certificado de firma electrónica.
>
> Para los efectos de este artículo, los prestadores acreditados de servicios de certificación de firma electrónica deberán contratar y mantener un seguro, que cubra su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por aquellos homologados en virtud de lo dispuesto en el inciso final del artículo 15".

Recordemos, en todo caso, que el certificado de firma electrónica provisto por una entidad certificadora podrá establecer límites a sus posibles usos, siempre y cuando dichos límites sean reconocibles por terceros, en cuyo caso el proveedor de servicios de certificación quedará eximido de responsabilidad sobre los daños y perjuicios causados por el uso que exceda dichos límites.

Asimismo, otra norma esencial en esta materia es la que dispone que, en ningún caso, la responsabilidad que pueda emanar de una certificación efectuada por un prestador privado acreditado comprometerá la responsabilidad pecuniaria del Estado.

Como podemos apreciar, las normas reseñadas establecen una especie de *responsabilidad agravada* respecto de los proveedores de servicios de certificación no acreditados, si consideramos que lo normal es que las partes de un contrato respondan hasta culpa leve y que, conforme al principio de buena fe, ha de presumirse que la parte actuó en forma diligente.

4.8 La Subsecretaría de Economía como entidad acreditadora

Las autoridades de control en el entorno tecnológico son órganos de carácter público, a los que el ordenamiento jurídico reconoce ciertas atribuciones de superintendencia en una determinada actividad. En concreto, y en nuestro caso, del mercado de certificación de firmas electrónicas.

En Chile, esa función está radicada en la Subsecretaría de Economía del ministerio del ramo y sus funciones esenciales son efectuar la acreditación de entidades de certificación y revocar dichas acreditaciones, llevar un registro de entidades acreditadas y fiscalizar el funcionamiento y desarrollo de la actividad de certificación en Chile. Entre sus funciones destacan las que se detallan en los próximos acápites.

4.8.1 Acreditación

Se trata del proceso a través del cual el prestador da cuenta a la autoridad del cumplimiento de los estándares exigidos para proveer los servicios de firma electrónica avanzada. Esto es, que cuenta con las instalaciones, sistemas, programas informáticos y los recursos humanos necesarios para otorgar los certificados en los términos que se establecen en la ley y en el reglamento.

Se inicia a través de un escrito de petición fundada presentado ante la entidad acreditadora, acompañando los antecedentes que acrediten lo siguiente:

a) Su servicio es confiable;

b) Cuenta con un servicio seguro de consulta del registro de certificados emitidos;

c) Emplea personal calificado para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados;

A los usuarios les asiste la confianza legítima de la adecuación de los procesos y sistemas, amparada en la vigencia del respectivo decreto de acreditación.

d) Utiliza sistemas y productos confiables que garanticen la seguridad de sus procesos de certificación;

e) Ha contratado y mantiene un seguro que cubra su eventual responsabilidad civil, por un monto equivalente a cinco mil unidades de fomento, como mínimo, tanto por los certificados propios como por los homologados, y

f) Cuenta con la capacidad tecnológica necesaria para el desarrollo de la actividad de certificación.

Este proceso finaliza con una resolución de autoridad en que acoge o rechaza la solicitud de acreditación.

A los usuarios les asiste la confianza legítima de la adecuación de los procesos y sistemas, amparada en la vigencia del respectivo decreto de acreditación.

4.8.2 Registro

Consiste en la inclusión de los datos de identificación de la entidad cuya solicitud de acreditación haya sido acogida, en un registro público que mantendrá la entidad acreditadora.

4.8.3 Fiscalización

Consiste en una verificación del cumplimiento, en el tiempo, de los requisitos y condiciones para mantener la condición de proveedor acreditado.

Al respecto, la ley dispone que la acreditación podrá quedar sin efecto por una resolución de cancelación de la misma emitida por la entidad acreditadora, fundada en alguna de las siguientes circunstancias:

a) Por la solicitud del prestador de servicios acreditado. Como vimos antes, esta solicitud debe efectuarse con al menos un mes de antelación a la fecha del cese efectivo de funciones, mediante escrito en que se da cuenta del destino que se dará a los certificados emitidos y vigentes.

b) Por la pérdida de las condiciones que sirvieron de fundamento a su acreditación. Esta circunstancia será calificada por los funcionarios o peritos de la entidad acreditadora, en el proceso de inspección periódica a que se refiere la ley, en virtud del cual se les podrá requerir información y ordenar visitas a sus instalaciones por parte de funcionarios o peritos especialmente contratados para estos efectos por la subsecretaría.

c) Por el incumplimiento grave o reiterado de las obligaciones que establece la ley y su reglamento.

La cancelación deberá ser informada a los usuarios titulares de certificados de firma electrónica emitidos por el prestador a quien se ha cancelado su inscripción, a fin de que estos ejerzan su derecho de oposición al traspaso del certificado a otra entidad certificadora.

En todo caso, se debe tener presente que uno de los deberes de la entidad acreditadora es mantener accesible al público un registro de las entidades acreditadas y en consecuencia, dictada la resolución de cancelación, debiera eliminarse del registro al prestador correspondiente.

4.9 El documento electrónico firmado comomedio de prueba y su valor probatorio

El problema probatorio en los documentos electrónicos cobra extraordinaria importancia a la hora de analizar si es factible a un notario o a un juez desconocer sus efectos jurídicos. En Chile, la prueba instrumental está reglada en los artículos 342 a 355 del Código de Procedimiento Civil (CPC), y en los artículos 1701 y siguientes del Código Civil (CC).

El CPC distingue entre instrumentos públicos y privados, señalando en cada caso su valor probatorio y oportunidad de presentación e impugnación. Esto, sin perjuicio de que en cada procedimiento se establecen normas sobre apreciación judicial de las pruebas acompañadas.

Este sistema entrega los elementos suficientes para que el tribunal aprecie en cada caso el valor de los documentos que se hacen valer en juicio, y la ley de firma electrónica no lo altera substancialmente. En efecto, en su artículo 5º, el CPC dispone:

> "Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes:
>
> 1) Los Instrumentos públicos suscritos con firma electrónica avanzada, harán plena prueba de acuerdo con las reglas generales, y
>
> 2) Los que posean la calidad de instrumento privado harán plena prueba en cuanto hayan sido suscritos mediante firma electrónica avanzada.
>
> 3) Los instrumentos privados suscritos con firma electrónica simple, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales, esto es, bajo el apercibimiento de tenérselos por reconocidos si no fueren objetados dentro de sexto día".

El artículo 1701 del CC agrega: "La falta de instrumento público no puede suplirse por otra prueba en los actos y contratos en que la ley requiere esa solemnidad; y se mirarán como no ejecutados o

celebrados aun cuando en ellos se prometa reducirlos a instrumento público dentro de cierto plazo, bajo cláusula penal: esta cláusula penal no tendrá efecto alguno".

A ello suma que si el documento público adolece de algún requisito de forma, o es otorgado por funcionario incompetente, valdrá como instrumento privado si está firmado por las partes. En consecuencia, el límite a la prueba documental nuevamente lo encontramos en aquellos casos en que la ley requiera de instrumento público para el perfeccionamiento del acto o contrato de que se trate.

En cuanto a la forma como se acompañan, el CPC dispone que el instrumento público deberá acompañarse con citación y el instrumento privado, bajo apercibimiento del artículo 346 N° 3.

Donde estimamos que la Ley Nº 19.799 aporta novedad, es lo relativo a las causales de impugnación, especialmente cuando el documento es suscrito con firma electrónica avanzada, por las razones que siguen.

El artículo 342 del CPC, modificado por la Ley Nº 20.217 de 2007, dispone expresamente lo siguiente:

> "Serán considerados como instrumentos públicos en juicio, siempre que en su otorgamiento se hayan cumplido las disposiciones legales que dan este carácter (…)
>
> 6°. Los documentos electrónicos suscritos mediante firma electrónica avanzada".

Adicionalmente, hay condiciones intrínsecas de los documentos electrónicos que se debe tener en cuenta, a saber:

> a) Tratándose de documentos electrónicos, no es posible hablar de originales y copias, sino más bien de matrices y documentos de primera, segunda, tercera emisión, etcétera. Es decir, estamos siempre frente a originales y por tanto habrá de tenerlos como tales para efectos probatorios. Por tanto, siempre que se presente un instrumento público en juicio, su apreciación se regirá por el

artículo 342 Nº 1 y por tanto no cabrá a su respecto la objeción a que alude el Nº 2 de ese artículo.

b) Sin perjuicio de lo anterior, aunque consideráramos que el documento agregado al juicio es una copia y que el original es el que permanece en el computador del emisor, el artículo 342 del CPC señala que las copias podrán ser objetadas por inexactitud dentro de tercero día, por la parte contra la cual se presentan. Creemos que esta objeción no es posible tratándose de los instrumentos públicos electrónicos, en cuanto estos documentos deben ser firmados con firma electrónica avanzada, la que entrega plenas garantías respecto de la exactitud del documento.

c) Tratándose de un instrumento privado, creemos que si estos están suscritos mediante firma electrónica avanzada no cabrán las objeciones de falsedad ni de falta de integridad que prescribe el artículo 346 N° 3 del CPC, por lo que resulta ocioso acompañarlos bajo esta norma, sin perjuicio de que en el estado normativo actual es la única manera de acompañarlos.

d) Respecto de los demás instrumentos privados, esto es, aquellos que sean suscritos mediante firma electrónica simple, a su respecto será perfectamente posible objetarlos por las causales antes señaladas.

Creemos que la única objeción que puede caber respecto de un instrumento firmado a través de firma electrónica avanzada es aquella que se refiere a defectos del soporte en que conste.

Dadas las consideraciones anteriores, creemos que la única objeción que puede caber respecto de un instrumento firmado a través de firma electrónica avanzada es aquella que se refiere a defectos del soporte en que conste. De ahí que tantas legislaciones se hayan detenido en el establecimiento de medidas de seguridad en la conservación del documento electrónico, sin embargo se estima que esta será una cuestión a apreciar en cada caso concreto.

En todo caso, incluso antes de la Ley Nº 19.799, los tribunales habían optado por dar aplicación a la normativa general en materia de apreciación del valor probatorio de los documentos electrónicos.

Es el caso del fallo de la Excma. Corte Suprema dictado en 1991, recaído en autos rol Nº 4956, en que se ha considerado que:

> "Al apreciar las pruebas según la sana crítica, el tribunal laboral deberá expresar las razones jurídicas y las simplemente lógicas, científicas, técnicas o de experiencia en cuya virtud les designe valor y las desestime. Si se limita a señalar que le resta valor a un instrumento computacional de liquidación de remuneración sin firma, analizado de acuerdo a las reglas de la sana crítica, no se da cumplimiento a la exigencia señalada, máxime si el merecido documento no mereció reproche de la demandada en cuanto a su autenticidad. Conteniendo dicho documento computacional los nombres del empleador y del trabajador, merece un estudio más profundo del tribunal, ya que es el único medio de prueba para acreditar la remuneración del actor".

A su turno, la Ley Nº 19.799 dispone al respecto:

> "Artículo 5º. Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes:
>
> 1) Los señalados en el artículo anterior (instrumentos públicos firmados con FEA), harán plena prueba de acuerdo con las reglas generales, y
>
> **2) Los que posean la calidad de instrumento privado, en cuanto hayan sido suscritos con firma electrónica avanzada, tendrán el mismo valor probatorio señalado en el número anterior. Sin embargo, no harán fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador acreditado.**
>
> En el caso de documentos electrónicos que posean la calidad de instrumento privado y estén suscritos mediante firma electrónica, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales".

Contraviene el texto expreso de la ley, cometiendo una discriminación ilegal y arbitraria, el notario u otra persona o autoridad le niega valor a los documentos electrónicos suscritos con FEA.

Por tanto, contraviene el texto expreso de la ley, cometiendo una discriminación ilegal y arbitraria, el notario u otra persona o autoridad le niega valor a los documentos electrónicos suscritos con FEA.

4.10 El repositorio documental del notario considerando los estándares de la Ley Nº 19.799

Entendemos que, tratándose de los repositorios electrónicos, habrá de seguir los lineamientos de la ley y el reglamento de firma electrónica. Al respecto, el artículo 43 inciso final de dicho reglamento dispone lo siguiente:

> "La seguridad, integridad y disponibilidad del Repositorio deberán estar caracterizadas por:
>
> a) Medidas de seguridad y barreras de protección, frente al acceso no autorizado de usuarios.
>
> b) Contar con monitoreo y alarmas que se activen cuando ocurra un evento no autorizado o fuera de programación, para el caso de eventuales fallas de las medidas de seguridad al acceso.
>
> c) La sustitución de la información, por la versión más reciente que se disponga, en el menor tiempo posible, en casos de alteración no programada de aquella.
>
> d) La existencia de un programa alternativo de acción que permita la restauración del servicio en el menor tiempo posible, en caso que el Repositorio deje de operar por razones no programadas".

De acuerdo al Decreto 181 de 2002, en su texto actualizado, el repositorio debe ajustarse a los estándares siguientes:

> "NCh2832.Of2003 Tecnología de la información - Protocolos operacionales de infraestructura de clave pública LDAPv2 para Internet X.509.
>
> RFC 2559 Boeyen, S. et al., «Internet X.509 Public Key Infrastructure. Operational Protocols LDAPv2", abril 1999.
>
> RFC 3377 LDAPv3: Technical Specification, September 2002, Lightweight Directory Access Protocol (v3): Technical".

Derecho informático y medios de prueba

← Índice de contenidos

5.1 Aspectos generales de las imágenes y videos digitales como medios de prueba

Como su nombre lo sugiere, hablamos de videovigilancia respecto de aquella modalidad de vigilancia llevada a cabo a través de la captación y eventualmente conservación de imágenes y videos.

Su uso normalmente se encuentra asociado al control de un cierto espacio respecto del cual se considera relevante dejar registro de lo que suceda en él, ya sea para garantizar la seguridad de las personas y los bienes que existan en el lugar, o controlar los comportamientos de las personas que desarrollan sus actividades en la zona sujeta a estas medidas.

Desde una perspectiva técnica, la RAE la define como "vigilancia a través de un sistema de cámaras fijas o móviles"[71]; luego, el mismo diccionario define "video" como "sistema de grabación y reproducción de imágenes, acompañadas o no de sonidos, mediante cinta magnética u otros medios electrónicos" y "vigilancia" como "cuidado y atención exacta en las cosas que están a cargo de cada uno".

La capacidad de grabación y fidelidad de los resultados dependerá de las potencialidades de la tecnología empleada. En efecto, es muy distinto un sistema rudimentario de grabación –que en muchos casos fue lo tenido a la vista a la hora de regular– que los sofisticados sistemas que cuentan con cámaras de alta definición, capacidades de grabación nocturna, analizadores biométricos, capacidades de seguimiento de activo, gracias a que procesan información de forma tal que permiten ejercer control y seguimiento de objetivos específicos, los cuales podrán ser objetos fijos o móviles y sujetos determinados.[72]

71 Revisado en línea [consulta: 19.09.2020].

72 A vía ejemplar, sobre los avances de la captación de imágenes vía infrarrojos, véase al respecto CORREA O., Carolina, "Iluminando lo invisible: nueva fuente de radiación infrarroja para la adquisición de imágenes digitales en el espectro infrarrojo". En *Conserva* Nº 16, 2011.

La revitalización de medidas de control en los espacios públicos, tales como instalación de cámaras de vigilancia e implementación de sistemas de vigilancia activa, corresponden a una "visión higienista de los espacios ciudadanos o, más precisamente, determinados espacios ciudadanos, a los que se quiere preservar de la pretendida pérdida de imagen, atractivo y, en ocasiones, sensación de seguridad que sufren cuando en ellos interactúan determinadas personas o se realizan determinados comportamientos".[73]

Estas labores se han visto potenciadas con el empleo de sistemas de control intensivos tales como cámaras fotográficas, videocámaras y ahora drones y otros sistemas "activos" de captación de información.

73 CEREZO D., Ana Isabel y DIEZ R., José Luis, *Videocámaras y prevención de la delincuencia en lugares públicos: análisis jurídico y criminológico*. Ed. Tirant , Valencia, 2011; p. 11.

5.2 La captación de registros a través de cámaras y drones y los problemas de legalidad asociados

Nos hemos acostumbrado a que los cielos de nuestras ciudades sean sobrevolados por aparatos denominados "drones", expresión que proviene de la voz inglesa *drone*, cuya traducción literal es "zángano".

Bajo esta expresión se agrupa a distintos tipos de "naves sin piloto a bordo", esto es, pilotadas a distancia a través de un control remoto. Así lo ha definido la RAE, al referirse a ellos como "aeronave no tripulada" o RPA (abreviatura en inglés de "*remotely piloted aircraft*"), aunque si revisamos las referencias en distintos ámbitos, esta denominación será más precisa tratándose de drones para finalidades civiles.

Asimismo, cuando se trata de estos aparatos y sus usos dentro del ámbito militar, la expresión que más encontramos es "vehículos aéreos no tripulados" o UAV (del inglés "*unmanned aerial vehicle*".

Dentro de este concepto podemos encontrar naves de distinta envergadura y modelos, tamaños, pesos y capacidades, tanto drones propiamente tales como globos, aviones, helicópteros e incluso pequeños aparatos semejantes a un insecto. De nuestra parte, a efectos de nuestro estudio nos interesan aquellos que tienen capacidades de captura de información de su entorno y que se emplean dentro de finalidades civiles.

Consecuentemente con su naturaleza de naves, su operación debe cumplir con la normativa dictada por las autoridades de aeronáutica civil[74], la cual se refiere tanto a las condiciones propias de los equipos,

74 A vía ejemplar, en España, el Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las naves pilotadas a control remoto y se modifica el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea, y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea, además del Real Decreto ley 8/2014, de 4 de julio, tramitado como ley 18/2014, de 15 de octubre.

tales como su peso, medidas y requisitos técnicos de mantención, como a los requisitos de formación de sus operadores y a los lugares y modalidades en que pueden operar.

Con su implementación, se promueve el fortalecimiento de mecanismos de vigilancia, dotando a los gobiernos locales de nuevas herramientas que les permitan mantener a raya a delincuentes y a sujetos "desordenados" que pudieran poner en riesgo la zona. Adicionalmente, con ello se busca controlar en general a la población, bajo la premisa de la necesidad de garantizar la gobernanza del territorio.[75]

Jurisprudencia y drones

En Chile, la jurisprudencia no ha sido generosa con los drones como medio de prueba en juicio.

Es así como en sentencia dictada en autos RUC Nº 1901382973-2, RIT Nº 54-2020, del Tribunal de Juicio Oral de Santa Cruz, de fecha 15 de diciembre de 2020, absolvió a los acusados del delito del tráfico ilícito de drogas (sentencia validada por la Corte de Apelaciones de Rancagua en causa rol Nº 1685-2020), en circunstancias que el principal medio de prueba eran imágenes obtenidas desde drones.

En este caso, el tribunal consideró ilegal la prueba obtenida a través de un dron por no contarse con una autorización judicial previa a la operación del aparato en un espacio privado, cual era la vivienda de los imputados. El tribunal con ello deja en claro que en materia penal no basta la necesariedad de la prueba, sino que además se deben respetar las garantías procesales, estableciendo la necesidad de una orden judicial previa para su licitud.

75 Al respecto véase BECKETT, Katherine y HERBERT, Steve, "Dealing with Disorder: Social Control in the Post-Industrial City", en *Theoretical Criminology* 12(1): 5-30 (2008).

> Lo anterior, pese a que el dron registró a los acusados mientras se encontraban manipulando drogas al interior de su domicilio. Esto, por cuanto tanto el tribunal como la Corte estimaron que un dron es un elemento tecnológico de carácter intrusivo, desde el punto de vista de la protección de la vida privada, garantizada por la Constitución Política de la República en el artículo 19 Nº 4.

5.3 Internet de las cosas (IoT) como medio de prueba

Nos hemos referido antes a la "sensorización", entendiendo por ello la aplicación masiva de etiquetas (*tag*) en personas y objetos, lo que permite realizar el seguimiento de su ubicación, además de obtener información acerca de sus características, titulares y otros datos relevantes para el "observador".

El desarrollo de estas etiquetas y de los lectores electrónicos a los que están asociadas permiten que prácticamente cualquier cosa o persona sea objeto constante de control tecnologizado. Los sistemas relacionados tienen amplias capacidades de proceso y son capaces de analizar los datos aunque no estén estructurados, además de ser capaces de aprender e incluso generar nuevo conocimiento.

En la base de la sensorización encontramos los sistemas RFID ("*Radio Frequency Identification*"), que se traducen como identificación por radiofrecuencia y consisten en sistemas de almacenamiento y recuperación de datos de manera remota, empleando dispositivos denominados "*target*" o etiquetas, que operan como transpondedores RFID y cuyo principal objetivo es transmitir información, principalmente sobre la identidad de un objeto (similar a un número de serie único), mediante ondas de radio o "radiofrecuencia" desde la etiqueta al lector.

Este sistema permite la captura y/o grabación de datos sin contacto entre el lector y etiqueta, eliminando así la necesidad de un contacto visual directo.[76] Se trata de tecnología que en ningún caso puede considerarse nueva, pues sus orígenes se remontan a la II Guerra Mundial cuando se comenzó a utilizar el radar: "Este consistía en un transmisor que envía pulsos de ondas de radio de alta frecuencia, las cuales rebotan contra los objetos y regresan a la antena parabólica; la

76 OBSERVATORIO REGIONAL DE LA SOCIEDAD DE LA INFORMACIÓN (ORSI), *Estudio RFID: Tecnología de identificación por radiofrecuencia*. Junta de Castilla y León, 2007. Disponible en línea [consulta: 10.06.2019].

finalidad de esto es que permitía la detección de aviones a kilómetros de distancia, pero no así la identificación de estos. Siendo este el primer método de RFID pasiva". [77]

"En paralelo, los ingleses trabajaban en un proyecto secreto que sería el primer sistema activo de RFID. El proyecto fue liderado por Robert Watson Watt, quien introdujo un transmisor en los aeroplanos británicos y que al recibir la señal del radar enviaba de vuelta a la estación una señal particular que identificaba a la aeronave como amiga o enemiga".[78]

77 PORTILLO, Javier y otros, "Informe de vigilancia tecnológica Madrid. Tecnología de identificación por radiofrecuencia (RFID): aplicación en el ámbito de la salud". Fundación Madrid para el Conocimiento, Madrid, 2008; p. 21.

78 RAMIREZ L. Rodrigo, "Aplicaciones del RFID como herramienta para el proceso de marketing". Universidad de Chile, Santiago, 2006; p. 24. Tesis disponible en línea [consulta: 12.08.2021].

5.4 Vigilancia, perfiles y big data

Entendemos por perfilamiento "una forma de control indirecto de los individuos sobre la base de la explotación de informaciones obtenidassobre ellos".[79]

Los sistemas de cámaras fijos y móviles instalados en nuestras ciudades alimentan los algoritmos a efectos de construir estos perfiles, sumándose aquellos a los cuales ya estamos medianamente acostumbrados, tales como los basados en la información extraída de nuestra navegación en internet o en los sistemas que dan cuenta de nuestros comportamientos de consumo y de pago.

A esta creciente observación a la que somos sometidos por medio la sensorización de nuestro entorno, se suman la captura de nuestros desplazamientos e interacciones en la vía pública. Todo ello gracias a la interoperación de los sistemas de cámaras de videovigilancia, fijas o activas, con los demás sistemas preexistentes.

A través del *big data* y procesamiento automatizado en base a sistemas de inteligencia artificial, se puede obtener un "habitante promedio", "transeúnte peligroso", un "consumidor habitual" y así, una serie de perfiles que permiten al observador predecir el comportamiento futuro (inmediato o de mediano plazo) de la persona.

A partir de estas observaciones se ordenan las tiendas de un centro comercial, los productos del supermercado, y se adoptan una serie de decisiones respecto de la persona. Un caso que señala habitualmente un profesor experto en estos temas es el del padre que recibe un regalo de la tienda comercial felicitándolo porque será abuelo. El problema es que este padre de una menor de 16 años no sabía que su hija estaba embarazada, y lo más notable es que su hija tampoco.[80]

79 MATTELART, Armand y otro, *De Orwell al Cibercontrol*. Gedisa, Barcelona, 2015; p. 13.

80 Juan Velásquez Silva es Doctor en Ciencias de la Computación por la Universidad de Tokio y postdoctorado en la misma disciplina por la Universidad de Oxford.

¿Cómo es posible que esto suceda? Los algoritmos de búsqueda y tratamiento de información construyen árboles de decisión y, a partir de operaciones matemáticas susceptibles de ser llevadas a cabo por los computadores, analizan la información de la persona y emiten un resultado de acuerdo a lo que le interese analizar al "observador". Dada la gran cantidad de información disponible de la persona en las redes, más la que obtienen los sensores y cámaras, pocos aspectos de nuestra vida quedan resguardados de este rastreo que se ha impuesto respecto de las personas en la sociedad digital.

Desde el punto de vista del debido proceso legal, el perfilado presenta algunos de los riesgos más temidos de la humanidad. Mientras la doctrina y jurisprudencia se ha inclinado por mantener férreos controles de las actividades investigativas prejudiciales o judiciales que representen una potencial intrusión en la vida privada de las personas, a través de la exigencia de orden judicial como regla general, el perfilamiento generalmente se efectúa sin que las personas se enteren siquiera, adoptándose decisiones respecto de laspersonas en los más variados ámbitos de su vida.

En efecto, sin que exista la participación previa de los tribunales de justicia, el perfilamiento es invisible, incluso para la persona que se ve afectada por una decisión de un tercero a su respecto. A vía ejemplar,una solicitud de crédito podría ser otorgada antes de ser solicitada,una admisión a un lugar rechazada, o el apostamiento de un guardia de seguridad a distancia prudente de la persona mientras camina por un centro comercial, podrían ser inadvertidas por la persona. Pues bien, esta invisibilidad y las capacidades de observación se ven potenciadas por la creciente multiplicidad de dispositivos y soportes que sirven a la recogida de datos de las personas.

La virtual aceptación de la ciudadanía a estos sistemas de vigilancia se ve aún más favorecida en aquellos lugares en que los conflictos armados son parte del día a día. No es de extrañar que países como Israel o Corea del Sur sean la cuna de estas tecnologías de vigilancia masiva. Retomando al mismo autor citado al comienzo de este acápite, Armand Mattelard:

"El acopio de ficheros policiales y administrativos combina a la perfección con la preocupación de las autoridades públicas de identificar aquellos focos que potencialmente puedan tener comportamientos violentos o desviados. Se trate del joven 'movido', del paciente psiquiátrico, del terrorista o del potencial criminal, el objetivo que se busca es el de anticipar aquellos comportamientos que sean considerados peligrosos o anormales y así prevenir los posibles riesgos. Un conjunto diverso de medidas, progresivamente establecen las bases de una estructura de control renovada, a través del incremento de los ficheros y de sus interconexiones, de la mejora en la identificación de las personas –especialmente a través de la biometría– y de la experimentación de métodos automáticos de clasificación y de detección".[81]

81 MATTELART, A. y otro, *De Orwell al Cibercontrol*. Gedisa, Barcelona. 2015; p. 17.

5.5 Videovigilancia como medio para obtener pruebas a ser presentadas en juicio

Tratándose de la prueba de hechos controvertidos en materia civil, la videovigilancia se ha empleado tanto en la preconstitución de pruebas como en la producción de las mismas durante el proceso.

Un ejemplo en esta materia es la sentencia dictada por el TEDH Nº 10764/09, de 27 de mayo de 2014.[82] En este caso, instado por una persona de nacionalidad española que se vio involucrada en un accidente de tráfico, se alegó que sus derechos fundamentales habían sido vulnerados por la aceptación como prueba, por parte del tribunal, de grabaciones realizadas sin su consentimiento por detectives privados contratados por una aseguradora, quienes obtuvieron filmaciones del demandante manejando una motocicleta en circunstancias que esa persona había alegado que, como consecuencia del accidente, no estaba en condiciones de conducir un vehículo,

En este caso, el TEDH señaló en primer lugar que para ese tribunal "es de la opinión que la grabación de imágenes de video constituye igualmente una injerencia en la vida privada del individuo". Luego, respecto de la propia imagen, señaló que "la imagen de un individuo es uno de los atributos principales de su personalidad, por el hecho de revelar su originalidad y permitirle diferenciarse de sus congéneres. El derecho de la persona la a la protección de su propia imagen constituye de esta manera uno de los componentes esenciales para alcanzar la plenitud personal y presupone, principalmente, el control del individuo sobre su propia imagen. Si tal control implica en la mayoría de los casos la posibilidad para el individuo de rechazar la difusión de su imagen, comprende al mismo tiempo el derecho de éste de oponerse a la captura, conservación y la reproducción de la misma por un tercero (…)".[83]

82 TEDH, demanda Nº 10764/09, De La Flor Cabrera c. España.
83 TEDH, demanda Nº 10764/09, De La Flor Cabrera c. España. (FJ 30 y 31).

En tercer lugar, el TEDH reafirma que los Estados no solo deben abstenerse de realizar injerencias arbitrarias a través de los poderes públicos, sino que además les cabe un rol positivo inherente al respeto efectivo de la vida privada o familiar, e incluso pueden requerir "de la adopción de medidas tendentes al respeto a la vida privada, incluso en las relaciones entre los mismos individuos", debiendo al efecto establecer un justo equilibrio entre los derechos e intereses en juego.

En relación a la aplicación de estos criterios al caso en análisis, el TEDH señala "que el presente caso no trata de la difusión de imágenes relativas a la vida cotidiana del demandante, sino exclusivamente de la toma y la posterior utilización de tales imágenes como medio de prueba en el marco de un proceso civil", por tanto, la finalidad de la filmación fue la de "contribuir de manera legítima al debate judicial, con el fin de permitir al asegurador poner a disposición del juez el conjunto de los elementos pertinentes"; "las imágenes no estaban destinadas a ser publicadas", continúa la sentencia, por lo que no había riesgo de una explotación posterior "no habiendo sido realizada su toma de una manera sistemática o permanente".

Adicionalmente, el TEDH reconoce que "no se ha puesto en duda el hecho de que el demandante se encontrara en la vía pública cuando las escenas fueron grabadas y que no hubo ninguna interferencia en su comportamiento", y por último, en relación al sujeto que realiza las filmaciones, consideró que se trataba de una agencia de detectives privados debidamente habilitada para realizar esta actividad de acuerdo al derecho interno de España.

Jurisprudencia y cámaras de vigilancia

La Corte Suprema, en autos rol Nº 23.683-14, declaró nula la sentencia dictada por el Tribunal de Garantía de Valparaíso en el proceso RUC Nº 1400270322-0, que se había basado, como prueba, en el análisis de un video extraído de una cámara de vigilancia y las fotografías tomadas de las especies incautadas, por haberse incumplido la garantía del debido proceso legal

al infringirse lo previsto en los artículos 6º y 7º, además del art. 19 Nº 3 CPR Chile, en concordancia con el artículo 373 letra a del Código Procesal Penal.

Esto, por cuanto "el personal policial procedió a realizar diligencias investigativas sin orden previa y en forma autónoma interrogó al menor acerca de su participación en el hecho al momento de su detención, sin la presencia de abogado defensor, omitiendo dejar registro de la misma, transgrediendo así lo establecido en el artículo 130 letras d) y e) del Código Procesal Penal, en relación con los artículos 83, 84 y 227 del mismo texto y 31 de la ley 20084 [*ley de responsabilidad penal juvenil*]", razón por la cual se pidió la exclusión de toda esta prueba, al haber sido obtenida en contravención de las garantías fundamentales, vicios que fueron alegados por la defensa en todas las etapas del proceso, pero que fueron desatendidos por el tribunal.

El cuestionamiento a las pruebas dice relación con el hecho que fueron obtenidas por la policía sin que concurriera una hipótesis de flagrancia en los hechos que se pretendía probar a través de ellos.

La Corte estima procede aplicar al caso lo dispuesto en el inciso tercero del artículo 276 del Código Procesal Penal, que dispone que "el juez excluirá las pruebas que provienen de actuaciones o diligencias que hubieren sido declaradas nulas y aquellas que hubieren sido obtenidas con inobservancia de garantías constitucionales".

En razón de la aplicación de este artículo, la Corte sostiene que "toda la prueba y elementos obtenidos en un proceder al margen de la ley constituye prueba ilícita, misma calidad que tiene, producto de la contaminación, toda la prueba posterior que de ella se deriva [*el análisis del video de las cámaras de vigilancia*], esto es, la materializada en el juicio, consistente en las declaraciones de los funcionarios policiales sobre el contenido de las pesquisas, el video las fotografías y testimo-

nios que hayan derivado de tal indagación. En este sentido, aunque el juez de la instancia haya afirmado su convicción condenatoria en prueba producida en la audiencia, al emanar ella del mismo procedimiento viciado, no puede ser siquiera considerada, por cuanto su origen está al margen de las prescripciones a las cuales la ley somete el actuar de los auxiliares del Ministerio Público en la faena de investigación".

5.6 Procedencia de los "modernos medios de prueba" en el proceso

Según Vivares Porras (2015)[84], si el objetivo es definir la verdad de un enunciado, es necesario que se puedan usar todas las informaciones útiles para tal efecto.

Taruffo ha entendido al respecto que fenómenos como las "pruebas científicas" o "tecnológicas" escapan a cualquier tipificación normativa y que –aparte de las discusiones sobre su admisibilidad– el uso tan difundido que en la práctica se hace de las pruebas atípicas muestra cómo está destinado al fracaso cualquier intento de "cerrar" el catálogo normativo de las pruebas.

Es así como existe un relativo consenso en que ningún ordenamiento establece la omnicomprensividad de la regulación de los medios de prueba, y no es casualidad que en muchos ordenamientos –también el *civil law*– esté admitida la posibilidad de usar pruebas no expresamente previstas por la ley y "resulta evidentemente la naturaleza 'incompleta', si no residual, de las normas en materia de prueba".[85]

De ahí que se plantee la necesidad de ir sustituyendo los sistemas de prueba legal o tasada por sistemas mixtos o derechamente la libertad probatoria.

5.6.1 Relevancia, idoneidad y proporcionalidad

Si los medios de prueba que podrían eventualmente presentarse en juicio están taxativamente enumerados, habrá que constituir estándares de admisibilidad que otorguen certeza jurídico-procesal a las partes. Entre estos criterios, se han incluido los de relevancia, idoneidad y proporcionalidad.

84 VIVARES PORRAS, Luis Felipe, "El juicio de proporcionalidad como garantía del derecho a la prueba", en *Revista de la Facultad de Derecho y Ciencias Políticas,* UPB, Vol. 45 Nº 123, 2015; pp. 435-452.

85 TARUFFO, Michele, *La prueba de los hechos*. Madrid, Trotta, 2002; p. 346.

Siguiendo a Taruffo, podría definirse el **criterio de relevancia** como "un estándar lógico de acuerdo con el cual los únicos medios de prueba que deben ser admitidos y tomados en consideración por el juzgador son aquellos que mantienen una conexión lógica con los hechos en litigio, de modo que pueda sustentarse en ellos una conclusión acerca de la verdad de tales hechos".[86]

Ahora bien, la relevancia no es un concepto inamovible o fijo, sino más bien específico y contextual, en relación al caso concreto en el cual se la evalúa. En efecto, "el juicio de relevancia es marcadamente contextual. De esta manera, dependiendo del resto de la prueba dis-ponible, una misma pieza de información podrá ser calificada como relevante (no hay nada más a lo que echar mano), o irrelevante (el resto de la prueba es abundante y de excelente calidad). Debido a que la línea que separa la relevancia de la irrelevancia resulta borrosa, el juicio que al respecto se haga debe tener en cuenta valores como los costes de la litigación y la eficiencia del proceso probatorio. Así, por ejemplo, en un juicio que se cuenta con una cantidad de información *prima facie* suficiente para decidir los hechos, la incorporación de nueva prueba difuminará el efecto de lo ya disponible (el esfuerzo de recepción y de análisis de la nueva prueba hace más difícil mantener el foco de atención en el resto de la prueba)".[87]

La relevancia, por tanto, se encuentra en estrecha relación con la idoneidad y proporcionalidad. En ese sentido, se ha entendido que el principio de proporcionalidad se traduce en "una prohibición de excesos" en relación a la finalidad de la prueba, de las competencias legales de quien las solicita, ordena y produce, en relación a las reglas del debido proceso legal y debido resguardo a los derechos fundamentales de las partes. Adicionalmente, la prueba se deberá ajustar a criterios de necesidad, en el sentido de que la realización de la diligencia o presentación de las pruebas producidas *extra muros* del proceso sean aquellas que, asegurando la finalidad probatoria, sean las menos lesivas para los derechos de las personas.

86 TARUFFO, ídem; p. 38.
87 COLOMA C., Rodrigo, "Conceptos y razonamientos probatorios". En *Revista de Derecho* (Valdivia), Vol. 30 Nº 2, Valdivia, 2017. Disponible en línea [consulta: 19.10.2020].

En cada caso concreto habrá de establecerse y analizar si, entre un determinado elemento de juicio (fuente de prueba) y la aseveración cuya verdad debe determinarse, existe o no una "relación de relevancia" dada por la relación de inferencia entre el hecho comunicado por la fuente de prueba y el hecho afirmado por la parte del proceso. Luego, la existencia entre el hecho a probar y el hecho probatorio define la relevancia de la prueba de que se trate.[88]

Alexy[89], respecto al principio de proporcionalidad como mandato de optimización, exige que "sus tres subprincipios, es decir los subprincipios de idoneidad, necesidad y proporcionalidad en sentido estricto, se siguen lógicamente de ella, o sea son deducibles de ella en un sentido estricto. Por lo tanto, quien objeta la teoría de los principios tiene también que objetar el principio de proporcionalidad"; "los principios exigen la máxima realización posible, en relación con las posibilidades fácticas y jurídicas. La relación con las posibilidades fácticas conduce a los subprincipios de idoneidad y necesidad… en cambio, el principio de proporcionalidad en sentido estricto se origina a partir del mandato de máxima realización posible en relación con las posibilidades jurídicas, sobre todo en relación con los principios que juegan en sentido contrario".

Sobre este tema, Bernal[90], en base a la jurisprudencia alemana, sostuvo que "toda intervención en los derechos fundamentales que no observe las exigencias de estos subprincipios (del principio de proporcionalidad) es ilegítima y, por tanto debe ser declarada inconstitucional. La aplicación del principio de proporcionalidad presupone que una medida del poder público represente una intervención en un derecho fundamental, es decir, lo afecte negativamente, bien sea anulando, aboliendo, restringiendo o suprimiendo una norma o una posición que pueda ser adscrita *prima facie* a la disposición constitucional que tipifica el derecho intervenido. Si la medida de intervención supera el test de los subprincipios de proporcionalidad, tal medida será válida

88 TARUFFO, Michele, *La prueba de los hechos*. Madrid, Trotta, 2002; p. 442.
89 ALEXY, Robert, *Tres escritos sobre derechos fundamentales y la teoría de los principios*. Ed. Universidad del Externado de Colombia, 2003; pp. 101-103.
90 BERNAL, Carlos, "Racionalidad, proporcionalidad y razonabilidad en el control de constitucionalidad de las leyes". En Bernal, C., *El derecho de los derechos*. Bogotá, Universidad Externado de Colombia, 2005; pp. 67-68.

definitivamente como una restricción al derecho correspondiente. En caso contrario, la norma o la posición del derecho fundamental objeto de la intervención adquiere una validez ya no solo *prima facie*, sino también definitiva, y por ello una ley que incide negativamente en el derecho debe ser declarada inconstitucional".

Prieto[91], al analizar el principio de proporcionalidad, lo divide en cuatro elementos o subprincipios:

- **Finalidad:** frente a una medida limitadora del derecho a la prueba, habrá de verificarse si esa medida persigue un fin constitucionalmente legítimo. Si no cumple este requisito sería una limitación **inconstitucional**.
- **Adecuación:** la medida constitucionalmente admisible debe ser "conducente", "acertada", esto es, que sea apta para la consecución de su fin. Si la medida de que se trate no cumple el requisito de adecuación en relación al fin, la limitación no encuentra sustento en el derecho a la prueba y por tanto se torna **ilegítima**.
- **Necesidad**: la medida limitadora que cumple las dos condiciones anteriores debe ser la única que, obteniendo los mismos resultados, resulte menos lesiva respecto del derecho limitado.
- **Proporcionalidad en sentido estricto**: implica la exigencia de acreditar una relación de equilibrio entre los beneficios a obtener con la medida limitadora y la lesión propiciada al derecho afectado por la limitación. Tratándose de las pruebas científicas y técnicas que se implementen y empleen, estas deben además corresponderse al estándar generalmente aceptado por la disciplina de que se trate, tanto en los métodos a emplear como en la producción de resultados.

De acuerdo a Torcuato: "Dos elementos, por tanto, deben ser tenidos en consideración: la exigibilidad (*Erforderlichkeit*) y la adecuación (*Geeghtheit*)". A propósito del artículo 18 inciso segundo de la Constitución de Portugal, en que está consagrado el principio de prohibición de

91 PRIETO, Luis, "El juicio de ponderación constitucional". En M. Carbonell, *El principio de proporcionalidad en el estado Constitucional*. Bogotá, Universidad Externado de Colombia, 2007; pp. 99-146.

exceso, el autor, siguiendo a Canotilho, señala que "en el ámbito específico de las leyes restrictivas de derechos, libertades y garantías, que cualquier limitación, hecha por ley o con base en la ley, debe ser adecuada (apropiada), necesaria (exigible) y proporcional (con justa medida), en relación a los resultados obtenidos".[92]

Especial relevancia tendrá en este ámbito las afectaciones a la vida privada de las personas a través de las grabaciones y análisis de datos que puedan hacer los RPA y sus sistemas asociados, especialmente cuando las personas se encuentran en espacios privados, pero también en espacios públicos realizando actividades privadas, ajenas a los hechos que se investiguen.

5.6.2 Prohibiciones probatorias y las pruebas tecnológicas

Se entiende por prohibiciones probatorias aquellas limitaciones a la prueba en el proceso que son fruto de una contraposición de intereses, ya sean estos colectivos o individuales, los cuales primarían respecto del derecho a la prueba o a probar en juicio.[93] Esto sucede, por ejemplo, cuando la realización de la diligencia afectara indebidamente los derechos fundamentales de la persona, en tanto emanan directamente de su dignidad y libre desarrollo de su personalidad (autodeterminación).

En el ámbito de lo público, las prohibiciones probatorias podrían venir dadas por su afectación a las instituciones públicas, tales como la seguridad nacional y el interés de la nación. Es el caso de la prohibición del sobrevuelo de drones sobre edificios y predios de las Fuerzas Armadas de un país, en las zonas fronterizas y otras áreas estratégicas, por ejemplo, por albergar infraestructuras críticas.

92 TORCUATO A. Luiz F., *Provas Ilícitas. Interceptaçôes telefônicas, ambientais e gravaçôes clandestinas. Revista Dos Tribunais*. Ed. Thomson Reuters, Sao Paulo, 2015, en base a CANOTILHO, J.J. Gomes, *Direito Constitucional*. Lisboa, 1989; pp. 487-488 (traducción libre de la autora).

93 HENKEL, Heinrich, *Strafverfahrensrecht*. Stuttgart, Kohlhammer, 1968; p. 271.

Al respecto, Ambos, a la luz de la experiencia alemana, enfatiza la importancia del reconocimiento de las prohibiciones probatorias, especialmente con la eclosión de las nuevas tecnologías de la información y las comunicaciones. Si bien se refiere a la invención del "detector de mentiras" y del "narcoanálisis", su razonamiento es plenamente aplicable al caso que nos ocupa.

Sin embargo, estima que esto no implica que se contengan en el texto expreso de la legislación, "sino que más bien ello está determinado en sentido material de acuerdo con la razón de ser de la norma procesal violada y en consideración a aquellos intereses contrapuestos que obstaculizan la averiguación de los hechos. De otra manera, si se exigiese una disposición legal expresa de la prohibición de la utilización probatoria, es decir, una prohibición de utilización probatoria codificada, esto implicaría la finalización de las discusiones político-criminales y dogmático-procesales de manera más bien rápida, puesto que las regulaciones de prohibición legalmente establecidas son, además de pocas, (relativamente) inequívocas".[94]

Subijana conceptualiza la prueba prohibida como "la que surge con violación de las normas constitucionales que reconocen los derechos fundamentales de una persona". Para este autor, la prueba ilícita es la que "infringe cualquier ley que regula el modo y manera de obtener una fuente de prueba o de aportarla al juicio. Así, por ejemplo, la presencia del Secretario Judicial en las entradas y registros domiciliarios, cuya regulación se encuentra en el artículo 569 LECrim".[95]

Ambos[96] señala al respecto que la doctrina alemana dominante distingue –bajo el concepto general de "prohibiciones probatorias"– entre prohibiciones de producción de pruebas (*Beweiwehebungsverbote*), que

94 AMBOS, Kai. "Las prohibiciones de utilización de pruebas en el proceso penal alemán: fundamentación teórica y sistematización". En *Política Criminal* Vol. 4 Nº 7 (julio 2009); pp. 1-56. Disponible en línea [consulta: 12.08.2020].

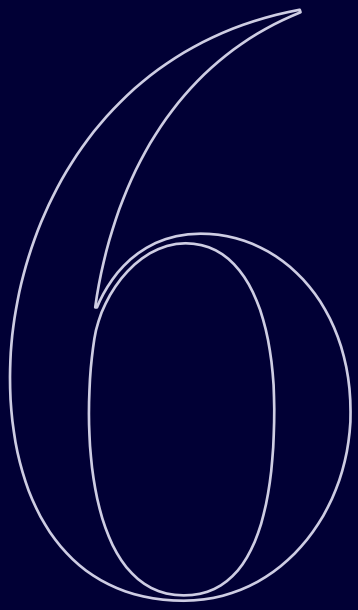
95 SUBIJANA Z., Ignacio José, "La prueba videográfica en el proceso penal". En *Videovigilancia: ámbito de aplicación y derechos fundamentales afectados, en particular la protección de los datos personales*, Etxeverría Guridi, José Francisco y otro, coordinadores. Monografías Turant Nº 726 Ed. Tirant lo Blanch, España, 2011.

96 AMBOS, Kai, "Las prohibiciones de utilización de pruebas en el proceso penal alemán: fundamentación teórica y sistematización". En *Política Criminal* Vol. 4 Nº 7 (julio 2009); pp. 1-56. Disponible en línea [consulta: 12.08.2020].

incluyen prohibiciones de temas probatorios, de medios de prueba y de métodos probatorios; y la prohibición de utilización de pruebas (*Beweiswertungsverbote*). Por tanto, responderían a la primera de estas categorías:

- La que se obtiene vulnerando determinadas garantías constitucionales tales como la intimidad personal y familiar (arts. 18.1 CE y 19 Nº 4 CPR Chile), la inviolabilidad de domicilio (18.2 CE) y la tutela del secreto de las comunicaciones (18.3 CE).
- Las que en su producción lesionan derechos constitucionales previstos para hacer efectivo el derecho de defensa (24.1 y 24.2 CE).
- Aquellas que se obtienen utilizando medios que la Constitución prohíbe. A vía ejemplar, obtener una confesión o una información empleando la tortura o cualquier trato inhumano o denigrante (15 CE).
- Las que se refieren a temas que están prohibidos, por ejemplo, la consulta de antecedentes penales que han sido borrados por una amnistía.
- Las que consisten en medios excluidos o prohibidos. Por ejemplo, la declaración de un testigo que no estando obligado a declarar, se niega a hacerlo.
- El uso de un dron en un espacio privado, sin autorización judicial y fuera de las hipótesis que los autorizan.

Como podemos apreciar, existen prohibiciones absolutas, esto es, que rigen con carácter general, y otras específicas para la situación puntual de la que, lo que deberá analizarse en cada caso concreto.



Contratación electrónica

← Índice de contenidos

Como hemos visto, el derecho informático tiene amplios espacios para el derecho público, pero también tiene múltiples aspectos del derecho privado, particularmente derecho civil y comercial, destacando en especial el área del comercio electrónico, que aúna en sí principios y normas aplicables en los dos ámbitos señalados.

Ello porque, aparejado al desarrollo del comercio electrónico, surgen nuevas modalidades de contratación, que usualmente incorporan al proceso el uso de dispositivos y plataformas de software en las distintas fases de la celebración del contrato.

Por ejemplo, hoy es común que la oferta de productos y servicios se realice en un determinado sitio web, donde se muestra y describe el producto, pero el pago se hace a través de otras plataformas, especializadas, como las de Transbank o las de determinadas instituciones bancarias.

Antes de seguir, se hace necesario tener claro primero qué es la contratación electrónica.

6.1 Sobre el concepto de contratación electrónica

Existen muchas definiciones de lo que es un contrato electrónico, quizás tantas como autores han escrito sobre el tema, pero en este curso solo mencionaremos dos: una de ellas es la contenida en la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico de España, que dice que es todo contrato en que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos conectados en redes de comunicaciones.

La otra definición es la que nos señala Maggio[97], que presentamos aquí no porque sea la mejor, sino precisamente porque tiene un defecto que se repite en muchos otros autores: entiende el contrato electrónico como el acuerdo de voluntades cuya celebración se perfecciona sin la presencia física de las partes contratantes y a través de medios electrónicos. Pero en ese punto comete un error: es perfectamente posible que dicho contrato sea celebrado a través de medios electrónicos, que verse sobre bienes digitales y que, sin embargo, los contratantes estén frente a frente, pues han decidido que esta modalidad es la que mejor se acomoda a sus necesidades. Y no por ello deja de ser un contrato electrónico.

97 MAGGIO, Lorena, "Contratos electrónicos". En microjuris.com, MJ-DOC-14922-AR | MJD14922. Disponible en línea [consulta: 12.08.2020].

6.2 Sobre la regulación del contrato electrónico

A pesar de que el contrato electrónico, con sus requisitos, ritualidad y efectos, no está especialmente regulado en nuestra legislación, no podemos afirmar que carece de normas aplicables, pues además de las normas civiles y comerciales relativas a contratos de la legislación común, también rigen las normas especiales de la Ley Nº 19.496, sobre protección de los derechos de los consumidores, cuando se trate de relaciones de consumo, y también la Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, si se utilizara esta tecnología en el proceso de suscripción del contrato.

Así por ejemplo, la Ley Nº 19.496 señala que en los contratos electrónicos no se entiende formado el consentimiento si el consumidor no ha tenido previamente un acceso claro, comprensible e inequívoco de las condiciones generales del mismo y la posibilidad de almacenarlos o imprimirlos; a su vez, la ley sobre firma y documento electrónico establece que los contratos suscritos por medio de firma electrónica serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en papel.

Sin embargo, se debe tener presente que nos estamos refiriendo en este acápite *exclusivamente* al contrato electrónico en el entorno regulatorio nacional, por lo que no nos referimos a las particularidades de la contratación electrónica internacional, que nos llevaría a abordar los problemas de jurisdicción y ley aplicable, ni tampoco a los estándares y convenciones sobre comercio electrónico que se promueven, como la ley modelo de la CNUDMI sobre comercio electrónico, o el Acta Uniforme de Transacciones Electrónicas de los Estados Unidos.

6.3 Clasificación de los contratos electrónicos

En doctrina existen múltiples clasificaciones de los contratos electrónicos, pero la verdad es que no todas las distinciones son útiles desde el punto de vista jurídico, aunque sirven para contar con un panorama sobre las realidades posibles de encontrar cuando se nos habla de contratación electrónica.

6.3.1 Según el tipo de sujetos intervinientes

Existe el **contrato electrónico mercantil** o contrato empresa a empresa, conocido por las siglas B2B (del inglés *business-to-business*), que son aquellos celebrados por empresas o personas jurídicas en general.

Pero también existe el **contrato electrónico de consumo**, conocido como B2C (*business-to-consumer*), que son celebrados por una empresa por una parte y un consumidor por otra, ya sea este persona natural o jurídica.

La distinción tiene relevancia, pues en el segundo caso, con seguridad, es aplicable la Ley Nº 19.496, de protección de derechos de los consumidores.

Pero el mundo de la contratación electrónica no se agota en las relaciones proveedor/consumidor o en aquellas entre empresas, sino que también existen contratos que no tienen por objeto el comercio, o cuyas partes no pueden ser categorizadas como comerciantes, proveedores o consumidores, entendiéndose que en estos casos estamos ante **contratos electrónicos civiles**, como pueden ser por ejemplo los de prestación de servicios profesionales celebrados electrónicamente.

6.3.2 Según la forma en que se expresa la voluntad

Se habla de **contratos electrónicos simples** cuando se perfeccionan exclusivamente por medios electrónicos. En cambio, se habla de **contratos electrónicos mixtos** cuando una de las partes expresa su voluntad de contratar a través de medios electrónicos y la otra lo hace por medios convencionales, como la firma de un documento impreso.

6.3.3 Según la forma de aceptación del contrato

Los contratos *shrink wrap* han caído en desuso últimamente, pero tuvieron su momento de gloria en la primera década de este siglo, usualmente a propósito de la venta de licencias de software en soportes físicos, como discos compactos y DVD. Usualmente, la caja de cartón que contenía el programa informático traía impresos los términos y condiciones de uso del mismo, los cuales se entendían aceptados por el hecho de abrir el empaque, que usualmente venía envuelto en una película plástica transparente que en inglés se denomina "*shrink wrap*" (de ahí el nombre).

Sin embargo, muchas veces la totalidad del contrato no estaba expresado en la envoltura, lo que dio lugar a serios cuestionamientos sobre la validez del consentimiento ante cláusulas sorpresivas.

Un poco más cerca en el tiempo se encuentran los contratos *browse-wrap*, cuyos términos y condiciones ya no tienen una expresión física, sino que se encuentran al interior de un sitio web y se entienden aceptados por el solo hecho de navegar por el mismo, independientemente de que ninguna manifestación expresa de aceptación sea requerida.

En Chile, uno de los primeros en utilizar este tipo de contratos fue el diario *El Mercurio* en su portal web emol.com, cuestión que causó una gran polémica no solo por la forma de dar por prestado el consentimiento de los visitantes del sitio, sino también por el excesivo detalle y extensión del contrato.

Por supuesto, el cuestionamiento general a este tipo de figuras las ha hecho desaparecer de la vida jurídica, pues es muy difícil de sostener que por solo visitar un sitio web los usuarios del mismo han celebrado un contrato y contraído obligaciones que nunca tuvieron posibilidad de conocer con anterioridad.

Tal situación evolucionó hacia lo que hoy se llaman contratos *clickwrap*, que también suelen suscribirse al momento de visitar un sitio web, con la fundamental diferencia que ahora la manifestación de voluntad del usuario es expresa, pues se obtiene una manifestación externa de

la misma mediante la presión de un botón, imagen o icono que da cuenta que el usuario ha leído y aceptado los términos y condiciones que se le han presentado para su lectura.

Sin embargo, se debe tener presente que en la práctica ello suele ser una mera formalidad, pues por lo extenso y complejo de los términos y condiciones, y siendo generalmente cláusulas de adhesión, prácticamente nadie los lee. Por eso no han faltado los bromistas que han incorporado disposiciones mediante las cuales los firmantes ceden todo su patrimonio a un tercero, o prometen entregarle el alma al final de sus días, sin que normalmente nadie advierta el real contenido del texto.

6.3.4 Según el modo de adhesión

Los **contratos electrónicos de libre discusión** son una rareza, pero existen: las partes se ponen de acuerdo en su contenido y luego lo suscriben electrónicamente, si bien claramente no son la regla general.

La regla general son los **contratos electrónicos de adhesión**, en los cuales una de las partes impone a la otra el contenido del contrato y esta última solo puede aceptarlo o rechazarlo, pero no tiene el poder suficiente para proponer reformas al mismo. O dicho de otro modo, no tiene poder de negociación.

Dignos de mención en esta clasificación son los **contratos inteligentes** (o *smart contracts*), en los cuales hay un acuerdo inicial de las partes de participar del mismo, lo que da lugar a una serie de procedimientos y acciones prediseñados computacionalmente que ocurrirán en forma automática al acaecer ciertas circunstancias previamente definidas.

6.3.5 Según su ejecución

De acuerdo a la última clasificación que señalaremos, existen los **contratos electrónicos online**, que se celebran y ejecutan a través de la web y que típicamente corresponden a aquellos por los cuales se adquieren servicios electrónicos de *streaming* de música o contenido audiovisual digital, como los que se celebran con Spotify (música), Teatrix (teatro argentino) o Filmin (cine europeo).

Sin embargo, también existen los **contratos electrónicos offline**, que se celebran electrónicamente, pero cuya ejecución es física por necesidad. Es el caso, por ejemplo, de la compra electrónica de productos de supermercado, los cuales llegan al hogar del contratante en vehículos de reparto que nada tienen de virtuales.

6.4 Formación del consentimiento

Nuestro Código Civil data del siglo antepasado y, por tanto, jamás previó la existencia de la contratación electrónica.

Sabemos que es un cuerpo normativo inspirado en el Código de Napoleón, y que responde a ideas o principios de libertad, igualdad y libre determinación de la voluntad (lo que conocemos como principio de autonomía de la voluntad), por lo que tiene plena confianza en el libre albedrío de los contratantes a la hora de regular sus relaciones mutuas.

Por ende, prácticamente las únicas limitaciones que encontró a dicha autonomía están marcadas por los vicios que puede tener el consentimiento y también la protección de los incapaces.

Dicho lo anterior, y teniendo presente que el contrato electrónico no es un tipo especial de contrato sino solo una modalidad de expresión del consentimiento, lo cierto es que se aparta de la teoría clásica del contrato (la que se enseña regularmente en las escuelas de derecho) en lo que dice relación con problemas de prueba y también los derivados de determinar en qué momento y lugar se forma el consentimiento, elemento base a la hora de determinar cuál es la legislación aplicable.

Teniendo presente que el contrato electrónico no es un tipo especial de contrato sino solo una modalidad de expresión del consentimiento, lo cierto es que se aparta de la teoría clásica del contrato en lo que dice relación con problemas de prueba y también los derivados de determinar en qué momento y lugar se forma el consentimiento, elemento base a la hora de determinar cuál es la legislación aplicable.

El Código Civil chileno no se preocupó de regular en detalle la formación del consentimiento. Más adelante, el Código de Comercio de 1865 reguló la materia en sus artículos 96 y siguientes.

El Código de Comercio, en su mensaje, dice que viene a llenar un sensible vacío en nuestra legislación comercial civil. Así, concede valor a la oferta verbal; define el valor de la oferta escrita; regula la retractación y su eficacia; atribuye valor a la aceptación simple y a la aceptación incondicional, y en general, otorga certeza acerca de dónde y cuándo se perfecciona el acuerdo, esto es, en el lugar y momento de la aceptación, tal como plantea el artículo 104 del Código de Comercio al señalar que "residiendo los interesados en distintos

lugares, se entenderá celebrado el contrato, para todos sus efectos legales, en el de la residencia del que hubiere aceptado la propuesta primitiva o la propuesta modificada".

Sin perjuicio de lo anterior, el Código de Comercio no lo solucionó todo y se resiste a darle valor a ofertas a personas indeterminadas, como las contenidas en catálogos de venta: "Las ofertas indeterminadas contenidas en circulares, catálogos, notas de precios corrientes, prospectos, o en cualquiera otra especie de anuncios impresos, no son obligatorias para el que las hace". Cuestión que se vino a solucionar recién con las nuevas leyes sobre protección del consumidor.

Debemos tener presente, tal como nos lo recuerda el profesor Mauricio Tapia, que el telégrafo, el teléfono y el fax son medios técnicos que pueden utilizarse para la formación del consentimiento a distancia y que no estaban presentes al momento de la redacción de los Códigos[98], por lo que los medios electrónicos no deberían marcar una particular diferencia.

98 TAPIA R., Mauricio, "Medios electrónicos: formación del contrato y protección de la intimidad del consumidor en Chile". En *Contratación electrónica y protección de los consumidores*, coordinado por Leonardo Pérez Gallardo. Reus, Madrid, 2017; p. 82.

6.5 La ley de protección de derechos del consumidor

En el año 1997 se dictó la Ley Nº 19.496, ley chilena de protección de los derechos de los consumidores, que en términos generales establece límites de orden público al contrato: uno de ellos es el imperativo de redacción clara, lo que implica u ordena preferir el sentido menos favorable al redactor frente a la ambigüedad de una cláusula. También implica la regla de prevalencia de la condición particular sobre las disposiciones generales.

Así, la ley de protección de los consumidores declara que el proveedor debe respetar los términos ofrecidos al consumidor en los catálogos y, además, le otorga otros derechos especiales como la facultad de retractación, que se amplía a 90 días cuando los contratos se celebran por medios electrónicos.

Pero no es conveniente engañarse al respecto, pues también concede el empresario la facultad de determinar los requisitos para ejercerlo, por lo que es perfectamente posible que el consumidor no pueda ejercer el derecho de retracto.

Asimismo, la ley del consumidor establece especiales deberes de información tratándose de contratos celebrados por medios electrónicos: el hecho de no otorgar un conocimiento claro y comprensible de las condiciones generales incluye la posibilidad de entender que no se ha formado el consentimiento.

Además se establece de forma inequívoca que la sola visita a un sitio web no puede significar en modo alguno aceptación de las condiciones del mismo, y por último declara lícita la oferta de publicidad no solicitada con oferta genérica de contratación, con la sola condición de indicar una forma en que el consumidor pueda suspender su envío.

6.6 Nuevas formas de contratación y contratos inteligentes

Uno de los aspectos más interesantes de la tecnología *blockchain* es su uso para la generación de *smart contracts* o contratos inteligentes, quizás la idea más innovadora que se ha cruzado por el campo del derecho civil y comercial en los últimos años.

Cabe recordar que la tecnología *blockchain*, esencialmente, es un sistema de registro de datos distribuido en varios nodos de una red informática, lo que hace que esos datos sean contrastables y no adulterables: es información que se conserva y actualiza entre todos los participantes.

Esta tecnología tiene tantas posibles aplicaciones que, en su momento, los profesionales de las tecnologías de la información lo presentaron como la panacea de la eficiencia: la programación a través de algoritmos de actos jurídicos complejos, lo que teóricamente permitiría prescindir de abogados, notarios y jueces, ahorrando significativamente en costos de gestión de los contratos.

No obstante, para que ello sea posible debe existir un riguroso diseño que, frente a la judicatura, haga incuestionable el contrato en cuanto acto jurídico. En la medida de que no logremos convencer a los jueces de que lo que están viendo es un contrato respetuoso de las normas civiles y comerciales de nuestro ordenamiento jurídico, estaremos en serios problemas, particularmente cuando el contrato deba reunir requisitos o condiciones especiales que no dependan de la mera voluntad de los intervinientes.

El primer elemento a considerar en el diseño algorítmico del *smart contract* es uno tan evidente que suele ser omitido y por ello, olvidado: no debe contravenir la ley. Sin embargo, tampoco debería contravenir las políticas públicas de un determinado país, pues de lo contrario la difusión de su existencia generaría una tensión y daño reputacional que, probablemente, los intervinientes no querrían para sí.

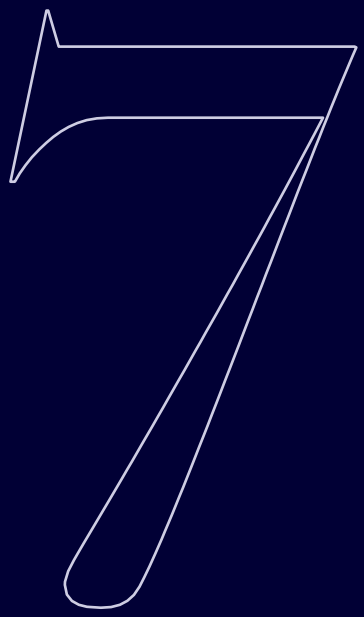
Un segundo elemento es que el contrato debe reflejar, en forma del todo evidente, el consentimiento de las partes que concurren en el mismo, pues en la medida en que un juez no vea clara dicha manifestación de voluntad, debería dejar caer el contrato.

Un tercer elemento, que también debe quedar reflejado en forma explícita en el diseño, es que en aquellos contratos abiertos a su aceptación por otros debe regularse la forma que debe revestir la aceptación, para entender inequívocamente cuándo se ha formado el contrato y evitar controversias futuras sobre si, frente a actuaciones que se reflejan en un código de programación y en la cual ninguno de los firmantes se vio la cara ni tomó un lápiz para hacer un garabato en un papel, fueron claros los términos de la oferta y todavía más el momento de su aceptación.

Hay un cuarto elemento, que requiere una ingeniería jurídica y técnica particularmente delicada, que se presentan en aquellos contratos respecto de los cuales las leyes prescriben solemnidades que requieren la intervención de terceros u otras complejidades, como por ejemplo un ministro de fe o la incorporación de un certificado. Ello supone una labor de coordinación previa, incluso de *evangelización*, para tener la certeza de que, llegado el momento, cada quien ejecutará su rol y se cumplirán los requisitos y ello será del todo evidente para quien examine el código de programación.

Finalmente, mencionaremos como quinto elemento, que no debería integrarse en el mismo contrato, aquellos actos que sean gratuitos para algunos y onerosos para otros, pues sembrarán la sospecha sobre la real naturaleza del contrato inteligente, dejándolo expuesto a una eventual declaración de nulidad. Esta podría ocurrir, por ejemplo, si alguien explora judicialmente el camino del enriquecimiento sin causa. Es decir, la claridad y precisión del flujo de las operaciones y de lo que obtiene cada quien al participar del contrato, también debe quedar prístinamente claro para el tercero imparcial que lo examine.

Los *smart contracts* tienen mucho que ofrecer, tanto que puede revolucionar el mercado de la contratación, pero sus efectivos progresos los veremos recién en años venideros.



Relaciones laborales y tecnologías

← Índice de contenidos

La masificación del uso de la informática y la convergencia de industrias tradicionalmente separadas ha llevado a repensar el esquema de trabajo y los derechos y deberes de las partes involucradas en una relación laboral.

La sociedad red ha implicado una adaptación radical de nuestra convivencia social. En particular, en la organización de los medios productivos ha significado adaptar también la nueva empresa a la nueva realidad.

La masificación del uso de la informática y la convergencia de industrias tradicionalmente separadas han llevado a repensar el esquema de trabajo y los derechos y deberes de las partes involucradas en una relación laboral.

Sin embargo, esta nueva situación, al igual que otros fenómenos a que ha dado lugar el uso de las tecnologías, no puede ser analizado como un enclave ajeno a los principios generales del derecho y a los criterios que inspiran a un Estado democrático.

Desde un enfoque de garantías fundamentales, tanto del empleador como del trabajador, es posible apreciar que las normas han debido ir ponderando los derechos y estableciendo reglas que permitan el desarrollo de la relación laboral en el nuevo contexto.

Desde la óptica del empleador, cobra relevancia el derecho de propiedad respecto de los medios materiales e inmateriales que, ordenados bajo su dirección, ha dispuesto para el logro de fines económicos, sociales, culturales o benéficos, dotándose de una individualidad legal determinada[99], que se esgrime como justificación del derecho a ejercer el poder de vigilancia sobre sus empleados utilizando, incluso, medios tecnológicos.

Respecto de los medios que se ponen a disposición del trabajador, revisten cada día una mayor relevancia los de índole tecnológica, como computadores, redes, software e incluso la conectividad, especialmente en tiempos en que el teletrabajo ha comenzado a masificarse también. El empleador costea estos medios y los pone a

99 Artículo 3º Código del Trabajo.

disposición de sus trabajadores para el desarrollo de las actividades productivas y, a cambio, tiene la pretensión de controlar el uso que de ellos haga el trabajador.

Otro elemento, que cambia radicalmente la visión de la regulación del trabajo, es la modificación de la matriz productiva resultante del impacto de las tecnologías, lo que nos acerca más a una sociedad de servicios, pudiendo incluso estar deslocalizados. Ello impone un desafío desde la óptica de la protección de los derechos de los trabajadores.

Ahora bien, en lo que al trabajador respecta, los derechos que la legislación le otorga deben ser interpelados frente al cambio tecnológico. Es así como el derecho a la protección de la vida privada, la dignidad y demás derechos que se engloban dentro de lo que se ha dado en llamar "ciudadanía laboral", se ven estresados por las potencialidades de las tecnologías como método de vigilancia y control empresarial.

El derecho al descanso, en sus diversas modalidades, también se ha visto debilitado frente a la hiperconectividad que proporcionan las tecnologías de la información y las comunicaciones. Adicionalmente, el teletrabajo ha puesto en jaque además a las normas de seguridad e higiene en el trabajo, que ahora se desempeña en los domicilios de los trabajadores.

En las siguientes páginas nos referiremos a estos aspectos.

7.1 Poder de vigilancia del empleador

El artículo 7º del Código del Trabajo, cuando define el contrato de trabajo, dispone que será tal la convención por la cual el empleador y el trabajador se obligan recíprocamente, este a prestar servicios personales bajo dependencia y subordinación del primero, y aquel a pagar por estos servicios una remuneración determinada.

Una de las manifestaciones de la subordinación o dependencia[100] es la vigilancia, que puede ser ejercida por el empleador respecto del desempeño del trabajador. Sin el propósito de entrar en el análisis del contrato de trabajo, nos referiremos a los elementos que han debido ser objeto de estudio ante la irrupción de las tecnologías en la empresa.

El artículo 5 del Código del Trabajo dispone lo siguiente:

> "Art. 5º. 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".

Si bien este artículo menciona especialmente la intimidad, la vida privada y la honra de las personas, entendemos que no solo estas garantías deben ser respetadas por el empleador, sino que es el conjunto de derechos y garantías que se le reconocen al trabajador, quien no las pierde ni ve disminuidas por el hecho de estar vinculado por un contrato de trabajo con su empleador.

100 Sobre el concepto de subordinación, ver, entre otros manuales, ALONSO OLEA, M. y CASAS BAAMONDE, M. E., *Derecho del trabajo, 18ª edición revisada*. Civitas, Madrid, 2001; pp. 47 y 59; ALBIOL MONTESINOS, I., CAMPS RUIZ, L.M., LÓPEZ GANDÍA, J. y SALA FRANCO, T., *Derecho del trabajo. Contrato individual*, 3ª edición (actualizada hasta septiembre de 2001). Tirant lo Blanch, Valencia, 2001; p. 21.

Es así como se han aprovechado las tecnologías para implementar sistemas de videovigilancia, entendida como "la actividad de vigilancia y protección de las personas y bienes ejercida a través de un sistema de seguridad electrónico que combina la captación y grabación de imágenes y/o sonidos".[101]

En este caso, el objetivo dice relación con el derecho del empleador de garantizar la seguridad del entorno de trabajo y de paso, monitorear las actividades de las personas que laboran en él. Ciertamente, su uso estará modelado por los derechos fundamentales que concluyen en dicha relación y así, por ejemplo, se ha resuelto que solo podrán instalarse estos sistemas en espacios "laborales", no en áreas de descanso o esparcimiento de los trabajadores, ni en zonas donde desarrollen actividades privadas. Asimismo, no podrán programarse para seguir un objetivo específico, sino que deberán grabar planos generales.

Ciertamente, su uso estará modelado por los derechos fundamentales que concluyen en dicha relación y así, por ejemplo, se ha resuelto que solo podrán instalarse estos sistemas en espacios "laborales", no en áreas de descanso o esparcimiento de los trabajadores, ni en zonas donde desarrollen actividades privadas.

101 ORDEÑAÑA G. Ixusko, "La videovigilancia en el ámbito laboral. Especial incidencia en su utilización como prueba en el proceso laboral". En *Videovigilancia*, Monografías Tirant Nº 726. Coordinadores Etxeverría Guridi, José Francisco y otro. Ed. Tirant Lo Blanch, Valencia, 2011; p. 46.

Adicionalmente, se ha proscrito la videovigilancia encubierta. En el caso español, así ha sido previsto en la normativa laboral[102] y en la de protección de datos personales.[103] En sentencia de 10 de julio de 2000, el Tribunal Constitucional de ese país se pronunció respecto a la videovigilancia encubierta en sentencia 186/2000, al sostener que estos sistemas debían cumplir los siguientes requisitos para considerarse aceptable:

a. **Juicio de idoneidad**, según el cual la medida debe ser capaz de conseguir el objetivo propuesto.

b. **Juicio de necesidad**, según el cual la medida es necesaria para lograr el objetivo perseguido; tratándose de videovigilancia en el trabajo, que al menos existan razonables sospechas respecto de los hechos que se busca indagar, por parte de quien emplea la medida.

102 Al respecto, véase el Estatuto de los Trabajadores de España, Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, que en su art. 20 bis dispone: "Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.

Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales".

103 Al respecto, la ley orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales, en su artículo 89 dispone lo siguiente: "Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley".

c. **Juicio de proporcionalidad**, para determinar si se había llegado a un equilibrio justo entre interferir en un derecho fundamental y la importancia del fin legítimo buscado; este equilibrio se cumpliría al limitar la medida a los espacios y por el tiempo estrictamente necesario para cumplir con el objetivo propuesto.

Ahora bien, estos criterios también han sido objeto de análisis en derecho comparado. Es el caso de las videocámaras debidamente informadas a los trabajadores, tal y como se ha resuelto en sentencia 39/2016, del Tribunal Constitucional Español.[104]

Desde la entrada en vigor de las leyes de protección de datos, la sentencia 29/2013, de 11 de febrero de ese año, agregó además que la instalación permanente de cámaras de videovigilancia por motivos de seguridad requería que los representantes sindicales y empleados recibiesen una notificación previa, y que la falta de este requisito constituiría una violación a lo previsto en el artículo 18.4 de la Constitución española (CE).

La nueva ley de protección de datos personales, aprobada en 2018, regula en su artículo 89 el tratamiento de datos obtenidos por el empleador a través de cámaras o de videocámaras. Al respecto, dispone lo siguiente:

> "1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y con-

104 En lo pertinente, en su fundamento jurídico número 5, la sentencia 39/2016 del Tribunal Constitucional, de 3 de marzo de 2016, consideró que "...el uso de cámaras de seguridad fue justificado (ya que existía una sospecha razonable que algunos de los empleados robaban efectivo de la caja), apropiado (para verificar si estas irregularidades estaban siendo cometidas por algunos de los empleados, y en tal caso, adoptar las medidas disciplinares apropiadas), necesario (la videovigilancia se utilizaría como prueba de dichas irregularidades) y proporcional (la grabación se limitó a la zona donde se encontraba la caja)".

cisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3.La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley".

En una perspectiva similar, en relación al uso de cámaras bajo la pretensión de seguridad y vigilancia en el ámbito del control de los procesos de trabajo y cumplimiento de obligaciones laborales, se ha recurrido a las tecnologías visuales bajo la pretensión de la necesidad de medir la productividad humana desde mucho antes de la eclosión de las tecnologías digitales.

Un caso que se cita al respecto es el de Frank B. Gilbert (1868-1925), quien se autodenominó experto en eficiencia industrial y en ciencias de la administración, dedicándose a la observación y seguimiento tanto de obreros como profesionales, quienes voluntariamente se sometían a sus observaciones. Para ello, "recurrió a las tecnologías visuales y, en especial, a la cámara cinematográfica, a la cual anexionaba un cronómetro, de forma que las transformaba en un ciclógrafo, un cronociclógrafo, según loa casos. Argumentaba que, contrariamente a la *watch-box*, la cámara

no podía equivocarse, ya que la cámara no representa la realidad: ella es la realidad. El experto en eficiencia industrial pone la cuestión del control en el orden del día de la era visual".[105]

De nuestra parte, entendemos que para comprender adecuadamente los límites del poder de vigilancia del empleador debemos recordar que, en todo caso, "las facultades empresariales se encuentran limitadas por los derechos fundamentales de los trabajadores, entre los cuales se encuentran la protección de su vida privada, de sus datos personales, y del derecho a la información respecto del empleo de estos medios intrusivos de vigilancia laboral".[106]

A esta misma conclusión ha arribado la autoridad administrativa, en Chile, con ocasión de lo dispuesto en el artículo 5º del Código del Trabajo.[107] Es el caso del Ord. Nº 2875/72, de 22 de julio de 2003. Nos detendremos en este caso porque, de acuerdo a la descripción de los hechos, el empleador había instalado "16 cámaras fijas en el exterior de las instalaciones (patios) y 16 en su interior (solo en el área de producción), activándose la grabación, según lo declarado por el empleador, al detectarse problemas, tales como congestionamiento vehicular en las áreas de carga, situaciones de riesgo provocadas por los trabajadores, personas laborando sin sus implementos de protección personal, etc."; "asimismo, se pudo constatar que existen dos tipos de cámaras: aquellas dirigidas directamente a los procesos productivos o áreas específicas, y las cámaras domos, las cuales tienen un radio mayor de captación de imagen, por ejemplo toda

105 EWEN, S., "The bride of Frankenstein", en *Journal of Communication*, Vol. 29 Nº 4, otoño 1979; pp. 13-19. Citado por Mattelart y otro, op. cit.

106 Véase por ejemplo las SSTC 98/2000, de 10 de abril, fundamento jurídico 7; SSTV 308/2000, de 18 de diciembre, FJ 430 de noviembre (fj.18).

107 En el caso de Chile, el art. 5º DFL 1 de 2002 (versión de 28.11.2018), dispone lo siguiente:

"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.

Los derechos establecidos por las leyes laborales son irrenunciables, mientras subsista el contrato de trabajo.

Los contratos individuales y los instrumentos colectivos de trabajo podrán ser modificados, por mutuo consentimiento, en aquellas materias en que las partes hayan podido convenir libremente".

una nave de producción". En este caso, la descripción del sistema se complementa con la cantidad de cuadros que el sistema es capaz de procesar y con la existencia de dos operadores.

Lo anterior es importante por cuanto la empresa declaró que la finalidad del sistema de videovigilancia era mantener un nivel de seguridad que permitiera evitar atentados desde el exterior de la empresa y al proceso productivo mismo, así como asegurar la producción y su manipulación. Estos objetivos se habrían logrado, de acuerdo a las declaraciones de la propia empresa. Pues bien, el organismo fiscalización consideró que, a la luz del artículo 5º del Código del Trabajo, ya citado, "lleva necesariamente a concluir que la utilización de mecanismos de control audiovisual (grabaciones por videocámaras)…, solo resulta lícita cuando ellos objetivamente se justifican por requerimientos o exigencias técnicas de los procesos productivos o por razones de seguridad…, debiendo ser el control de la actividad del trabajador solo un resultado secundario o accidental del mismo", nunca como la intención primaria del empleador.

Ahora bien, en cuanto al alcance de la seguridad como justificación del sistema, este organismo consideró que se limita a la seguridad de las personas, de las instalaciones o cuando el proceso productivo así lo exija, desde el punto de vista técnico.

Entendemos que estas consideraciones se condicen con el llamado "contenido ético jurídico del contrato de trabajo" de la aplicación del principio de buena fe contractual que rige en la materia, y del necesario resguardo de la dignidad de los trabajadores. De hecho, el ente fiscalizador sostiene en este caso que una forma de control empresarial permanente y continuada "provoca en el trabajador, inexorablemente, un estado de tensión o presión incompatible con la dignidad humana. El trabajador, al verse expuesto de forma ininterrumpida al ojo acusador de la cámara, será objeto de una forma intolerable de hostigamiento y acoso por parte de su empleador".

"Este control sujeta a los trabajadores a una exasperante e irritante presión. Tales controles continuados importarían en el trabajador un verdadero temor reverencial frente a su empleador, haciendo inexistente toda esfera de libertad y dignidad".

De hecho, este tipo de sistemas vulneraría la esencia misma de la libertad y autodeterminación del ser humano, impidiéndole en los hechos la más mínima licencia de comportamiento.

A juicio de esta autoridad, el principio de proporcionalidad "se traduce en un examen de admisibilidad –ponderación– de la restricción que se pretende adoptar basado en la valoración del medio empleado –constricción del derecho fundamental– y el fin deseado –ejercicio del propio derecho".

Como corolario a los antecedentes antes analizados, podemos sostener que las grabaciones obtenidas como ocasión del empleo de sistemas de videovigilancia solo serán eficaces como prueba en juicio cuando cumplan las condiciones que hemos señalado en este apartado.

7.2 Teletrabajo

Como se ha dicho, las nuevas tecnologías de la información han afectado a casi todos los ámbitos de la vida personal y social. La organización del trabajo no ha escapado a estos efectos y de esta forma, hoy ya no resulta extraño hablar de "teletrabajadores", incluso los ordenamientos nacionales e internacionales han asumido el desafío de analizar jurídicamente este tema, para efectos de adecuar la normativa vigente al cambio tecnológico.

A diferencia de otros fenómenos a los que ha dado lugar la red internet, no es esta el factor que hizo nacer el concepto. En efecto, fue la crisis del petróleo, unida a la conciencia de la contaminación ambiental, la que provocó hacia los años 70 al físico Jack Nilles a plantear la necesidad de considerar la posibilidad de "llevar el trabajo a la casa y no al trabajador al trabajo, evitando de esta forma los desplazamientos y consecuentes gastos de energía y aumento de contaminación".[108]

Sin embargo la red de redes sí es la que potencia el fenómeno del teletrabajo, al punto que hoy en día es posible apreciar cifras considerables a nivel internacional en tal sentido. En la Comunicación de la Comisión de las Comunicaciones Europeas al Consejo y al Parlamento Europeo, de 13 de marzo de 2001[109], se sostiene que a esa fecha un 5,6 % de los europeos desarrolla alguna actividad de teletrabajo, si bien se reconoce que hay diferencias significativas entre los distintos estados miembros.

Así por ejemplo, en Dinamarca esta cifra se eleva a un 17,6 % de teletrabajadores permanentes y ocasionales, situación que se justificaría por un entorno social y legal más favorable y la existencia de incentivos fiscales. Con todo, aun en este entorno se reconoce que

108 Al respecto véase "El teletrabajo nació de otra crisis".
109 Unión Europea, *eEurope 2002, Impacto y prioridades*, COM(2001)0140 final. Bruselas, 13 de marzo de 2001. Disponible en línea [consulta: 12.08.2020].

persisten desigualdades, entre las cuales cabe mencionar una mayor posibilidad de teletrabajar para los hombres y mayor presencia de esta modalidad laboral entre los ejecutivos.

La búsqueda de un concepto del teletrabajo no ha sido pacífica. Se han realizado varios intentos, de los cuales cabe destacar sus elementos comunes, como son el trabajo por cuenta ajena, realizado a distancia y sirviéndose de redes de telecomunicaciones.

El teletrabajo es, primero y antes que nada, trabajo por cuenta ajena, entendido como el desarrollo de una actividad laboral costeada y remunerada por un tercero por su cuenta y riesgo.

En segundo lugar, se trata de un trabajo desarrollado en un lugar distinto al de las dependencias de "la persona natural o jurídica que utiliza los servicios intelectuales o materiales de una o más personas"[110], esto es, de la persona del empleador. Como podemos apreciar, si bien el lugar en el cual se presten los servicios constituye un elemento integrante del concepto, lo es solo en cuanto a la necesidad de que el trabajo se desarrolle en un lugar distinto al de la empresa, no así respecto de que se desarrolle en un lugar determinado, como podría ser el domicilio del trabajador u otro que se haya definido.

Finalmente, se trata de un trabajo realizado con apoyo de sistemas y redes de telecomunicaciones para la transmisión del flujo comunicaciones a que da lugar la relación laboral, tanto desde como hacia el trabajador o al empleador, o incluso entre los integrantes de un determinado equipo de trabajo.

Asimismo, por su naturaleza, normalmente involucra a los sistemas de tratamiento de la información como herramientas de trabajo cotidiano. No se trata de un trabajador que eventualmente se conecta a un punto de red para efectos de enviar un correo electrónico, aunque este correo contenga datos que emanan de su trabajo, sino de

110 Artículo 3º letra a del Código del Trabajo, DFL 1 Ministerio del Trabajo, año 1994.

La OIT ha definido el teletrabajo como "cualquier trabajo efectuado en un lugar donde, lejos de las oficinas o los talleres centrales, el trabajador no mantiene un contacto personal con sus colegas, pero puede comunicarse con ellos a través de las nuevas tecnologías".

trabajadores que se mantienen conectados, realizando sus labores en una comunicación permanente, o por lo menos sostenida, con su empleador.

En el entorno internacional, la OIT ha definido el teletrabajo como "cualquier trabajo efectuado en un lugar donde, lejos de las oficinas o los talleres centrales, el trabajador no mantiene un contacto personal con sus colegas, pero puede comunicarse con ellos a través de las nuevas tecnologías".[111]

De su parte, en la doctrina, según Eduardo de No-Louis y Caballero pueden ser catalogadas como propias del teletrabajo "todas aquellas actividades profesionales desarrolladas a través de un equipo informático, que hacen uso de las técnicas de teletratamiento y telecomunicación para enviar información en tiempo real al centro de trabajo, producción o servicios y que genera un valor añadido a sus usuarios".[112]

En este punto, deberemos considerar además que conforme a nuestra legislación y "para los efectos de la legislación laboral y de seguridad social, 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".[113]

En consecuencia, se trata de un trabajo intelectual, desarrollado por cuenta ajena y "a distancia". Respecto de este último punto, deberemos señalar que no se trata necesariamente de un trabajador que presta sus servicios desde su domicilio, sino más bien que esta característica alude a que los servicios se prestan en un lugar distinto de aquel en el que será evaluado el desempeño del trabajador, y del cual emanan las instrucciones específicas en atención a las cuales debe desarrollar sus labores.

111 JURI SABAG, Víctor Ricardo, "La flexibilidad laboral a través del teletrabajo". En *Revista Laboral Chilena*, febrero-marzo (2000).

112 DE NO-LOUIS Y CABALLERO, Eduardo, "El working-house informático o tele-trabajo". En *Revista Iberoamericana de Informática y Derecho* Nº 4, 1994; pp. 593-604. Disponible en línea [consulta: 12.08.20].

113 Artículo 3º inciso final del Código del Trabajo, DFL 1 Ministerio del Trabajo, 1994.

Es así como hoy se considera que, en realidad, el teletrabajo es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional sin la presencia física del trabajador de la empresa durante una parte importante de su horario laboral. Engloba una amplia gama de actividades y puede realizarse a tiempo completo o parcial.

La actividad profesional en el teletrabajo implica el uso frecuente de métodos de procesamiento electrónico de información y el uso permanente de algún medio de telecomunicación para el contacto entre el teletrabajador y la empresa.

7.2.1 El lugar físico en que se ha previsto la prestación de servicios

La primera alternativa en el tiempo fue considerar que era factible que una persona desarrollara su trabajo desde su domicilio. Esto dio lugar a tres figuras básicas. En primer lugar, la que más nos interesa es aquella que se refiere a los **teletrabajadores empleados**, en la cual, en virtud de una estipulación del contrato de trabajo, se establece que el lugar de prestación de servicios será el domicilio del trabajador. En segundo lugar, una figura bastante común en nuestros tiempos es la del **autoempleado** o **trabajador "*freelance*"**, esto es, que ofrece sus servicios desde su domicilio y sin sujeción a contrato de trabajo.

Finalmente, hoy han cobrado importancia los **teletrabajadores "empresarios"**, que son aquellos emprendedores que inician una empresa gestionada desde su propia casa.

Al margen de las implicancias legales del trabajo domiciliario, psicológicamente se ha estimado que esta no es la mejor opción, especialmente en lo que se refiere a los necesarios resguardos del régimen de descanso de los trabajadores. En efecto, se ha dicho que el teletrabajo domiciliario provoca una transgresión en los espacios de recreación y de convivencia familiar, que obstaculizarían o aun impedirían el adecuado descanso de los trabajadores.

Así también, el teletrabajo domiciliario podría producir un deterioro en las habilidades sociales del trabajador, al no tener contacto con sus compañeros de labores. Aún más, provocaría niveles de estrés laboral superiores a los del trabajador tradicional, al no existir instancias en las que pueda compartir sus experiencias laborales.

En todo caso, el deterioro psicológico del trabajador no es el único elemento negativo del teletrabajo domiciliario, pues los riesgos derivados de las condiciones de higiene y seguridad es otro elemento que se ha cuestionado, abriéndose el debate respecto de quién debe solventar los gastos de adecuación del hogar a las necesidades del trabajo.

Finalmente, en el aspecto patrimonial, se ha dicho que la única forma aceptable de financiar los gastos de funcionamiento, tales como luz, agua, teléfono, instalaciones y mobiliario que esta tipología de teletrabajo requiere, es aquella en la cual el empleador asume este costo; sin embargo, esto conlleva la dificultad de aislar dichos costos de aquellos que se producen de ordinario en el domicilio del trabajador.

En atención a lo que hemos analizado, existen diversas formas de teletrabajar, dependiendo del lugar en que se prestan los servicios, algunos de los cuales se revisan en los próximos acápites.

7.2.1.1 Centros de recursos compartidos

Se trata de una instalación física dotada de tecnologías de la información y comunicaciones. Aglutina en un solo edificio una serie de prácticas relacionadas con el teletrabajo y con ello se busca organizar los recursos humanos de la empresa de la que se trate, para obtener una mayor efectividad y una mayor flexibilidad. Está dotado de un gran equipamiento informático y de telecomunicaciones.

7.2.1.2 Telecentros

Son centros compartidos por varias empresas, fundamentalmente pequeñas y medianas, dotados de tecnologías de la información y comunicaciones y puestos de trabajos conectados a una red, donde normalmente los trabajadores se agrupan atendiendo a un criterio geográfico.

Estos telecentros han de tener el equipamiento suficiente para realizar las funciones que con ellos se pretende. Pueden ser propiedad de empresas o de asociaciones de empresas que comparten costos, empresas de telecomunicaciones y o de empresas informáticas, que los crean con la intención de incentivar el uso tanto de equipos como de líneas de comunicaciones.

El teletrabajador puede trabajar en casa y acudir a este centro en determinados momentos en los que tenga que hacer una transmisión especial y no cuente en casa con los recursos adecuados.

7.2.1.3 Oficinas satélite

Son lugares de trabajo pertenecientes a la misma empresa, pero independientes de la sede corporativa. En ellos, el elemento predominante no es la organización funcional, sino la geográfica. Se abren para que acudan los trabajadores que viven más cerca, con independencia del puesto de trabajo que ocupen o de las tareas que desempeñen. Se diferencian de las oficinas tradicionales solo en el hecho de que reúnen empleados de la empresa que viven en sus cercanías.

7.2.1.4 Televillage o telecottages

Son centros de teleservicios asociados generalmente a instalaciones en granjas, pueblos pequeños, locales de escuelas públicas, etcétera, en zonas rurales.

Obedecen a una combinación de negocio, en cuanto a empresas que realizan sus propias actividades por su intermedio, política estatal de empleo y altruismo (ya que en este tipo de centro se suele dar todo tipo de información relacionada con las nuevas tecnologías a los habitantes de estas zonas rurales).

Con este tipo de teletrabajo se trata de retener a la población propia de una determinada región o zona geográfica, y atraer incluso a la población más preparada, que suele vivir en los grandes centros urbanos. También son activos en teleenseñanza, facilitando el estudio y la formación básica o permanente a los habitantes de la zona.

7.2.2 El teletrabajo en la legislación nacional

En nuestro ordenamiento jurídico laboral, la Ley Nº 19.759, publicada en el Diario Oficial de 5 de octubre de 2001, introdujo una modificación al Código del Trabajo a propósito de los trabajadores excluidos de la limitación de la jornada de trabajo:

> "Asimismo, quedan excluidos de la limitación de jornada, los trabajadores contratados para que presten sus servicios preferentemente fuera del lugar o sitio de funcionamiento de la empresa, mediante la utilización de medios informáticos o de telecomunicaciones".

Sin embargo, en general, la alternativa del trabajo domiciliario conlleva el inconveniente para el trabajador relativo a la inversión de la carga de la prueba en cuanto a la existencia del contrato de trabajo. En efecto, deberemos tener especial cuidado respecto del trabajador que realiza sus labores en su domicilio, por cuanto nuestro Código del Trabajo, en su artículo 8º inciso cuarto, dispone:

> "No hacen presumir la existencia de contrato de trabajo los servicios prestados en forma habitual en el propio hogar de las personas que los realizan o en un lugar libremente elegido por ellas, sin vigilancia, ni dirección inmediata del que los contrata".

Frente a la insuficiencia de esta norma, la Ley Nº 21.220, promulgada el 24 de marzo de 2020 y publicada dos días después, modificó el Código del Trabajo (CT) en materia de trabajo a distancia, introduciendo las siguientes normas:

- **Exclusión de la limitación de jornada de trabajo**: "los trabajadores contratados para que presten sus servicios preferentemente fuera del lugar o sitio de funcionamiento de la empresa, mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones".
- **Introducción de un Capítulo IX en el Título II del Libro I,** con las siguientes nuevas normas:

a. **Define teletrabajo** como aquella modalidad de trabajo a distancia en la que los servicios "son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante estos medios" (art. 152 quáter G, CT).

   En este ámbito, cobra relevancia el que no se considerará teletrabajo "si el trabajador presta servicios en lugares designados y habilitados por el empleador, aun cuando se encuentren ubicados fuera de las dependencias de la empresa" (art. 152 quáter H, CT).

   Asimismo, en este aspecto, se prevé que "la modalidad de teletrabajo podrá abarcar todo o parte de la jornada laboral, combinando tiempos de trabajo en forma presencial en establecimientos, instalaciones o faenas de la empresa, con tiempos de trabajo fuera de ella" (art. 152 quáter J, CT).

   Al respecto, conforme al artículo 3º letra b del DFL 1 del Ministerio del Trabajo, de 1994, es trabajador toda persona natural que preste servicios personales intelectuales o materiales, bajo dependencia o subordinación, y en virtud de un contrato de trabajo, en el caso del teletrabajo se tratará más bien de servicios intelectuales.

b. **Regula el pacto de teletrabajo.** En caso de que el teletrabajo se pacte en el contrato de trabajo, el contrato de trabajo de los teletrabajadores, además de las estipulaciones previstas en el artículo 10, debe contener lo siguiente:

   1. Indicación expresa de que las partes han acordado la modalidad de trabajo a distancia o teletrabajo, especificando si será de forma total o parcial y, en este último caso, la fórmula de combinación entre trabajo presencial y trabajo a distancia o teletrabajo.

2. El lugar o los lugares donde se prestarán los servicios, salvo que las partes hayan acordado que el trabajador elegirá libremente dónde ejercerá sus funciones, en conformidad a lo prescrito en el inciso primero del artículo 152 quáter H, lo que deberá expresarse.

3. El periodo de duración del acuerdo de trabajo a distancia o teletrabajo, el cual podrá ser indefinido o por un tiempo determinado, sin perjuicio de lo establecido en el artículo 152 quáter I.

4. Los mecanismos de supervisión o control que utilizará el empleador respecto de los servicios convenidos con el trabajador.

5. La circunstancia de haberse acordado que el trabajador a distancia podrá distribuir su jornada en el horario que mejor se adapte a sus necesidades o que el teletrabajador se encuentra excluido de la limitación de jornada de trabajo.

6. El tiempo de desconexión.

En todo caso, se reconoce la posibilidad de que en cualquier tiempo se pacte la modalidad de trabajo a distancia o teletrabajo, a través de un anexo al contrato de trabajo donde debe establecerse el lugar en que se prestarán los servicios o si el trabajador podrá elegir libremente el lugar en que se prestarán (art. 152 quáter H CT).

En este último caso, el empleador deberá registrar el pacto en que se acuerda la modalidad de trabajo a distancia o teletrabajo "de manera electrónica en la Dirección del Trabajo. A su vez, la Dirección del Trabajo remitirá copia de dicho registro a la Superintendencia de Seguridad Social y al organismo administrador del seguro de la Ley N° 16.744 al que se encuentre adherido la entidad empleadora".

c. **Da certeza jurídica** en relación a los derechos de los teletrabajadores, en tanto prevé que los trabajadores a distancia o teletrabajadores "gozarán de todos los derechos individuales y colectivos

contenidos en este Código, cuyas normas les serán aplicables en tanto no sean incompatibles con las contenidas en el presente Capítulo" (art. 152 quáter G CT).

d. En relación a la **duración de la modalidad de trabajo**, establece que si la modalidad de trabajo a distancia o teletrabajo "se acuerda con posterioridad al inicio de la relación laboral, cualquiera de las partes podrá unilateralmente volver a las condiciones originalmente pactadas en el contrato de trabajo, previo aviso por escrito a la otra, con una anticipación mínima de treinta días" (art. 152 quáter I CT).

e. En cuanto al **control de cumplimiento de la jornada**, en caso que proceda se prevé que "será de cargo del empleador implementar, a su costo, un mecanismo fidedigno de registro de cumplimiento de jornada de trabajo a distancia, conforme a lo prescrito en el artículo 33" (art. 152 quáter J CT).

   En todo caso, si bien se puede pactar que el trabajador distribuya libremente su jornada en los horarios que mejor se adapten a sus necesidades, deberá siempre respetarse los límites máximos de la jornada diaria y semanal. Entendemos que esto aplica cuando el trabajador está sujeto a jornada y no en aquellos casos en los que se ha eximido de esta condición.

   Uno de los riesgos del teletrabajo es que en definitiva no se respeten los tiempos de descanso del trabajador. Es por esto que este artículo de la ley prevé que "se presumirá que el trabajador está afecto a la jornada ordinaria cuando el empleador ejerciere una supervisión o control funcional sobre la forma y oportunidad en que se desarrollen las labores" (art. 152 quáter H CT).

f. **Establece el derecho a la desconexión**, respecto de los trabajadores a distancia o teletrabajadores que distribuyan libremente su horario o de teletrabajadores excluidos de la limitación de jornada de trabajo. En estos casos, el empleador deberá garantizar el tiempo en el cual el trabajador no estará obligado a responder sus comunicaciones, órdenes u otros requerimientos. "El tiempo

de desconexión deberá ser, de al menos, doce horas continuas en un periodo de veinticuatro horas. Igualmente, en ningún caso el empleador podrá establecer comunicaciones ni formular órdenes u otros requerimientos en días de descanso, permisos o feriado anual de los trabajadores" (art. 152 quáter J CT).

g. **Derecho de acceso a la empresa.** Uno de los aspectos en que se critica el teletrabajo dice relación con la falta de identificación o pertenencia del trabajador respecto de la empresa, algo que es recogido en la ley, previéndose que el trabajador a distancia o teletrabajador "siempre podrá acceder a las instalaciones de la empresa y, en cualquier caso, el empleador deberá garantizar que pueda participar en las actividades colectivas que se realicen, siendo de cargo del empleador los gastos de traslado de los trabajadores" (art. 152 quáter Ñ CT).

h. **Regula los elementos básicos de la seguridad e higiene en el trabajo y deber de información de riesgos laborales.** Si bien entrega la regulación detallada de estos aspectos a un reglamento, prevé que "en aquellos casos en que las partes estipulen que los servicios se prestarán desde el domicilio del trabajador u otro lugar previamente determinado, el empleador comunicará al trabajador las condiciones de seguridad y salud que el puesto de trabajo debe cumplir de acuerdo al inciso anterior, debiendo, en todo caso, velar por el cumplimiento de dichas condiciones, conforme al deber de protección consagrado en el artículo 184".

Aunque el empleador no queda facultado para acceder al domicilio del trabajador, podrá requerir al respectivo organismo administrador del seguro de la Ley Nº 16.744 que, previa autorización del trabajador, acceda al domicilio de este e informe acerca de si el puesto de trabajo cumple las condiciones de seguridad y salud reguladas en el reglamento, sin perjuicio de las facultades de fiscalización de la Dirección del Trabajo (art. 152 quáter M CT).

Además, el artículo 152 quáter N establece el deber del empleador de cumplir con el deber de protección, previendo las siguientes obligaciones:

1. **Informar de los riesgos que entrañan sus labores**. El empleador deberá informarlo por escrito al trabajador a distancia o teletrabajador, señalando tanto los riesgos como las medidas preventivas y los medios de trabajo correctos según cada caso en particular, de conformidad a la normativa vigente.

2. Efectuar una **capacitación al trabajador** acerca de las principales medidas de seguridad y salud que debe tener presente para desempeñar dicha labor, en forma previa al inicio de las labores a distancia o teletrabajo, a través de medios propios del empleador o a través del organismo administrador del seguro de la Ley N° 16.744.

3. Informar de la **existencia de sindicatos**. El empleador deberá informar "por escrito al trabajador de la existencia o no de sindicatos legalmente constituidos en la empresa en el momento del inicio de las labores. Asimismo, en caso de que se constituya un sindicato con posterioridad al inicio de las labores, el empleador deberá informar este hecho a los trabajadores sometidos a este contrato dentro de los diez días siguientes de recibida la comunicación establecida en el artículo 225".

7.3 El documento y firma electrónicaen los documentos laborales

Otro ámbito en que el derecho laboral se ha visto impactado por las tecnologías de la información y las comunicaciones, dice relación con el cumplimiento de la obligación del trabajador de mantener al día la documentación laboral y las posibilidades de implementar estos registros a través de documento electrónico.

Es así como el artículo 9º del Código del Trabajo dispone textualmente: "El contrato de trabajo es consensual; deberá constar por escrito en el plazo a que se refiere el inciso siguiente, y firmarse por ambas partes en dos ejemplares, quedando uno en poder de cada contratante".

7.3.1 Firma del contrato de trabajo a través de firma electrónica

Al respecto, la Dirección del Trabajo, mediante dictamen Nº 3161/064 de 29 de julio de 2008, ya señaló que es jurídicamente procedente la suscripción de contratos de trabajo haciendo uso de los medios de firma electrónica establecidos en la Ley Nº 19.799, y que tratándose de un instrumento privado no requiere de FEA sino que basta la firma electrónica simple, sin perjuicio de que será válido el contrato firmado con FEA.

Este criterio ha sido mantenido en el tiempo a través de múltiples dictámenes, entre los cuales mencionaremos solo algunos de los más recientes:

- Ord. Nº 4475 de 25 de septiembre de 2017
- Ord. Nº 4416 de 21 de septiembre de 2017
- Ord. Nº 2242 de 24 de mayo de 2017
- Ord. Nº 475 de 27 de enero de 2017.

7.3.2 Registro de asistencia

Tratándose de los registros de asistencia computacionales, consideraremos lo previsto en el Ord. Nº 1140/27 de la Dirección del Trabajo, de 24 de febrero de 2016[115], a través del cual se actualiza la doctrina institucional que había sido fijada por dictamen Nº 696/27, de 24 de enero de 1996.

Respecto de las características que deben cumplir estos sistemas, se debe destacar las siguientes:

- La marcación de asistencia debe ser un **acto voluntario** de parte del trabajador, aunque se emplee un medio electrónico.
- Sobre los **registros que debe realizar el sistema**: de manera automática se debe registrar "el nombre completo del trabajador y el número de su cédula nacional de identidad, indicando fecha, hora y minuto en que se inicia o termina la jornada de trabajo y, además, los datos del empleador. La misma información contendrán los registros de las demás marcaciones que, opcionalmente, desee incorporar el empleador, como salida o regreso de colación. Además, automáticamente luego de cada registro el sistema deberá registrar un 'Checksum1' o 'Hash2' de los datos de cada operación.

  Si existiere algún inconveniente al realizar la marcación, el sistema deberá generar una alerta señalando día, hora y lugar de la operación fallida, emitiendo, además, un código de la operación y un mensaje de error, los que serán almacenados en el sistema y entregados al trabajador, sea en formato de papel o mediante su envío de manera electrónica.

  Finalmente, cabe señalar que todas las marcaciones deberán ser transferidas en línea a una base de datos central, sin importar si se trata de equipos fijos o móviles. Ello, sin perjuicio de los respaldos que puedan contemplarse opcionalmente". Esto implica que debe quedar registro de la operación de marcaje de asistencia.

114 Ord. Nº 1140/27 de la Dirección del Trabajo, de 24 de febrero de 2016. Disponible en línea [consulta: 21.02.2021].

— Sobre los **mecanismos de identificación**: podrá emplearse cualquier mecanismo de identificación, pudiendo este "considerar parámetros biométricos, tarjetas con banda magnética u otros documentos de identificación, claves o password, token, etc., en la medida que la alternativa escogida permita dar certeza respecto de la identidad de la persona que efectúa la respectiva marca, la fecha del evento y –si corresponde– su ubicación y, al mismo tiempo, sea asimilable al concepto de firma electrónica simple que contiene el artículo 2º, letra f), de la Ley Nº 19.799, sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Dicha Firma.

Asimismo, se deberá tener presente que el mecanismo de identificación no deberá vulnerar los derechos fundamentales de los dependientes.

La identificación de los dependientes por parte del sistema, podrá realizarse de manera presencial o mediante login remoto, por ejemplo, utilizando equipos portátiles –celulares u otros– o computadores ubicados fuera del establecimiento del empleador.

Si el respectivo sistema de control utilizare como medio de identificación tarjetas con banda magnética, se les deberá asociar, en forma permanente, el número de la cédula nacional de identidad del trabajador. Además, la tarjeta deberá llevar impreso dicho número en su parte anterior junto al nombre completo del dependiente.

Cuando los sistemas de registro de asistencia contemplen el uso de dispositivos móviles –smartphone por ejemplo–, siempre deberán ser portados por el trabajador o, si ello no es posible por el tipo de mecanismo, el equipo siempre debe encontrarse disponible para realizar marcaciones, no pudiendo quedar nunca la determinación de la hora del registro al mero arbitrio del empleador. En el caso de los sistemas de registro que utilizaren para la identificación de los trabajadores claves o password, se deberá contemplar la posibilidad de que el dependiente las modifique a su elección las veces que estime necesario, sin más restricciones que los parámetros mínimos de seguridad, por ejemplo, cantidad de números, letras o uso de mayúsculas.

Atendido que este Servicio, como resultado de su labor fiscalizadora, ha verificado que existen personas que pueden presentar problemas frente a un registro biométrico y que también existen labores que afectan el debido reconocimiento, el sistema deberá contemplar una fórmula alternativa de registro –tarjetas de aproximación o claves, por ejemplo–".

- **Comprobantes de marcación:** los sistemas computacionales de control de asistencia deberán entregar de manera automática al trabajador un comprobante de cada operación realizada, aunque se trate de un error de identificación o falla en la marca. Al respecto, el dictamen dice que este requisito puede cumplirse de dos maneras: a) a través de impresoras u otro elemento similar conectado y próximo al sistema de control de asistencia, debiendo entregar el comprobante de inmediato, y b) mediante despacho de correo electrónico al trabajador en un formato imprimible, enviada al correo personal del trabajador o al institucional si el trabajador no contare con un correo personal. A estos efectos, el trabajador de manera voluntaria informará al empleador la casilla de correo en que desea recibir la información, dejándose constancia en el contrato de trabajo o en un anexo al mismo.
- **Contenido del comprobante**: "Trabajador: La fecha de la marcación con el formato dd/mm/aa.

  Trabajador: La hora de la marcación con el formato hh/mm/ss.

  Trabajador: El número de la cédula nacional de identidad del trabajador con puntos, guion y digito verificador.

  Empleador: Rut con puntos y guion; o número de la cédula nacional de identidad con puntos, guion y digito verificador si el empleador fuera persona natural.

  Empleador: razón social de las personas jurídicas o nombre completo si fuera persona natural.

  Empleador: Domicilio, indicando calle, número, piso, oficina, comuna, ciudad y región.

En caso de utilizar equipos portátiles o móviles dotados de sistemas de posicionamiento global –GPS–, u otros mecanismos que permitan identificar la ubicación física del trabajador, tales como teléfonos celulares, el comprobante deberá, además de los datos indicados previamente, señalar el lugar en que se realiza la marcación, con la mayor precisión posible.

En caso de utilizar conexiones remotas a sistemas o plataformas de propiedad del empleador, y que estas les permitan almacenar fecha, hora y lugar desde donde se realizan tales conexiones, podrán ser utilizadas como registro de asistencia del trabajador que realiza la conexión. En este caso será obligatoria la definición de un identificador único para cada trabajador y que la contraseña o seña sea sólo conocida por él".

— **Disponibilidad del servicio:** el empleador será siempre responsable de su operación y mantención, por lo que la dirección formula las siguientes condiciones de seguridad para los sistemas:

a. **Sistema alojado en más de un servidor o data center**, de forma que el trabajador no pierda la posibilidad de realizar los registros asociados a su cumplimiento de jornada.

b. **Base de datos replicada y respaldada** en dispositivos de almacenamiento externos, de forma tal que frente a un incidente de seguridad pueda rescatarse la información histórica.

c. **Seguridad de accesos:** las bases de datos deben tener sistemas de seguridad que impidan el acceso a personal no autorizado y prevengan adulteraciones de la información que consta en ella.

d. **Seguridad en los respaldos:** los respaldos deben tener mecanismos de seguridad que impidan que se vea afectada su integridad.

e. **Verificación:** esto es, que terceros independientes que se dediquen a la certificación revisen los sistemas de manera íntegra y en forma previa a su primera comercialización, considerando los siguientes aspectos:

"**Seguridad:** la plataforma tecnológica completa deberá incorporar las medidas necesarias para impedir la alteración de la información o intrusiones no autorizadas. Tales como controles de acceso restringido, cifrado de información confidencial, etc. En particular, el sistema deberá considerar un control de acceso que asegure la autenticación y autorización correcta para cada perfil de usuario que utilice la plataforma. La plataforma deberá asegurar el registro de cada actividad realizada, de forma tal que puedan determinarse los riesgos o incidentes de seguridad.

Confidencialidad: la plataforma deberá considerar componentes y desarrollos tecnológicos que aseguren la visualización de información de acuerdo a perfiles de seguridad pertinentes y apropiados para cada función (empleador, trabajador, fiscalizador, etc.). La definición de cada perfil, así como la respectiva asignación de personas a los mismos, deberá quedar registrada en un sistema de auditoría de la plataforma. Este registro deberá ser automático y sólo deberá ser accesible mediante perfiles de administración.

Disponibilidad: la plataforma deberá considerar componentes y desarrollos tecnológicos que aseguren la permanente disponibilidad de la información que se mantenga almacenada, para su consulta vía Web".

- **GPS (sistemas de Geoposicionamiento Global):** los equipos deberán ser posteriores a 2013, contar con wifi, plan de datos y GPS encendido. "La verificación deberá considerar que en un máximo de 3 minutos la aplicación debe ser capaz de lograr una ubicación con un margen de error inferior a un radio de 30 metros (diámetro de 60 metros) para, al menos, el 95% de las marcaciones. Atendida la finalidad de este mecanismo, las pruebas no deben ser realizadas en recintos cerrados"
- **Requisitos funcionales:** el tercero que realice la verificación debe emitir un informe detallado de las pruebas realizadas, indicando expresamente el cumplimiento de todos los requisitos exigidos para la validación del sistema de que se trate.

— **Acceso para fiscalización:** "El empleador será responsable de mantener disponible la plataforma con la información actualizada y, además, deberá asegurar el acceso de los fiscalizadores a los reportes para llevar a cabo la función inspectiva de este Servicio. El acceso señalado podrá ser presencial (en las mismas dependencias del empleador) o bien remoto (desde equipos de la Dirección del Trabajo). Estos accesos deberán considerar una comunicación segura (HTTPS), utilizando puertos estándares del protocolo habilitado y mecanismos de seguridad del tipo TLS 1.0 o superior. Los sistemas deberán adaptarse a las exigencias técnicas de esta Dirección para obtener la siguiente certificación que les corresponda".

— **Compatibilidad con otros sistemas:** "La utilización de un sistema de registro de asistencia que se ajuste a las condiciones expuestas en el presente informe, no obsta a la existencia de otro sistema especial para el mismo empleador, como puede ocurrir, entre los dependientes que presten servicios fuera del establecimiento del empleador y el personal administrativo de la misma compañía. En estos casos, cada sistema podrá operar válidamente respecto de los trabajadores que corresponda, en la medida que su imple- mentación se realice de acuerdo a las normas legales y administrativas vigentes sobre la materia.

Una vez acreditado ante este Servicio el cumplimiento de todos los requisitos señalados en el presente informe, los sistemas podrán ser comercializados e instalados sin que posteriormente cada empleador usuario deba solicitar nuevamente autorización para uso. Lo anterior, no excluye la posibilidad de que el empleador usuario del sistema sea fiscalizado por esta Dirección y sancionado, si se detectaren infracciones mediante inspecciones en terreno".

7.3.3 Libro y comprobante de remuneraciones

En este caso, entre otros, el Ord. Nº 6183[116], de 29 de diciembre de 2016, resolvió que no existe inconveniente en que se cumpla la obligación de llevar un libro auxiliar de remuneraciones y la de entregar al trabajador un comprobante de la remuneración pagada, la forma como se determinó y las deducciones efectuadas (arts. 54 y 62 CT) a través de medios electrónicos, en la medida que se cumplan los siguientes requisitos:

> "1. Los trabajadores deben consentir expresamente que los comprobantes de remuneraciones en que incide la consulta, sea confeccionada, procesada y remitida de manera electrónica.
>
> Es decir, los destinatarios de la comunicación electrónica deben consentir en tal medida, toda vez que la mantención de una casilla electrónica o mail no es un requisito impuesto por el legislador para recibir sus comprobantes de pago de remuneraciones. Por tanto, si el trabajador no acordare esta modalidad de envío, sus liquidaciones y anexos de remuneraciones deberán ser entregados en soporte de papel.
>
> 2. Una vez finalizada su confección o estampada la última firma, si corresponde, el sistema debe enviar inmediatamente el documento por correo electrónico a la casilla particular que previamente el trabajador haya indicado a su empleador.
>
> No es razonable su envío a casillas institucionales, pues ante su desvinculación de la empresa, los dependientes quedarían impedidos de acceder a sus cuentas de correo corporativo y a su documentación laboral electrónica allí almacenada.
>
> Finalmente, debe tenerse especialmente presente lo consignado en el Ordinario Nº 0155/004, citado precedentemente, que detalla las dos formas de transición de una plataforma documental de papel a otra electrónica, esto es, digitalizando la documentación,

115 Ord. Nº 6183, de 29 de diciembre de 2016. Disponible en línea [consulta: 21.02.2021].

y la otra alternativa, reemplazando la documentación en soporte de papel por una nueva en formato electrónico".

7.3.4 Finiquito laboral

En este caso, por mencionar algunos de los dictámenes de la Dirección del Trabajo, a través de Ord. N° 1012/20[117], de 27 de febrero de 2015, esta resolvió que un finiquito laboral puede ser suscrito mediante firma electrónica, de acuerdo a un esquema compatible con la normativa laboral y los **autos acordados relativos a los notarios**. Adicionalmente, este dictamen valida el siguiente procedimiento de suscripción del finiquito:

"i. El empleador o su representante suscribe electrónicamente el finiquito mediante huella digital, previa verificación de su identidad por medio de la misma huella dactilar, a través de un lector biométrico instalado en la oficina de la empresa.

ii. Una vez suscrito el documento por el empleador, éste es enviado al correo electrónico personal del trabajador y al del notario público, respectivamente, junto con la información necesaria para que el trabajador acuda a la Notaría Pública correspondiente, a suscribir el documento (dirección, hora de atención, funcionario a cargo).

iii. Se envían electrónicamente al ministro de fe los documentos necesarios, esto es, cédula nacional de identidad de los comparecientes, proyecto de finiquito, liquidación de remuneración del mes anterior del trabajador, copia del contrato de trabajo, planillas de cotizaciones previsionales pagadas del trabajador y su cartola previsional actualizada.

iv.El trabajador concurre a la notaría pública y ante el ministro de fe ratifica y firma electrónicamente el finiquito mediante huella digital, previa verificación de su identidad por medio de su misma

116 Ord. N° 1012/20, de 27 de febrero de 2015. Disponible en línea [consulta: 21.02.2021].

huella dactilar a través de un lector biométrico instalado en el oficio del notario.

v. Una vez que el finiquito se encuentra firmado por las partes en la forma señalada y ratificado por el trabajador, el notario público procede a suscribir el documento también mediante firma electrónica.

vi. Por último, se envía el documento electrónico al correo electrónico del trabajador y al de la empresa".

7.4 Requisitos comunes

Conforme ha previsto la Dirección del Trabajo en múltiples dictámenes, los sistemas de documentos electrónicos laborales deben cumplir las siguientes condiciones o requisitos:

> "a) Permitir al fiscalizador una consulta directa de la información vía internet desde la página Web de la empresa en que se implemente el sistema de registro y almacenamiento electrónico de la documentación laboral propuesto, desde cualquier computador de la Dirección del Trabajo conectado a Internet, a partir del RUT del empleador.
>
> b) Contemplar una medida de seguridad a establecer conjuntamente con el respectivo empleador, con el objeto de garantizar que las labores de fiscalización de la documentación electrónica se puedan realizar sin impedimento o restricción, ya sea en razón de fecha, volumen, tipo de documento, o cualquier otra causa que impida o limite su práctica.
>
> c) El sistema debe permitir igual consulta y forma de acceso señalada previamente desde computadores del empleador fiscalizado, en el lugar de trabajo.
>
> d) Permitir la impresión de la documentación laboral, y su certificación a través de firma electrónica simple o avanzada, si corresponde, dependiendo de la naturaleza jurídica del documento y de los efectos que éste deba producir.
>
> e) Permitir directamente ante el empleador fiscalizado y con la sola identificación del fiscalizador, la ratificación de los antecedentes laborales mediante firma electrónica simple o avanzada, dependiendo de la naturaleza o los efectos jurídicos que el documento deba producir" (Ord. Nº 0789/15, DT).

Como se ha podido ver, todas las normas, instrucciones, circulares y dictámenes citados son el resultado de la aplicación directa de la Ley Nº 19.799, pues tanto respecto de los instrumentos públicos como de los privados ella establece que la firma electrónica avanzada hace **plena fe** respecto de la identidad de los firmantes, además del hecho de haber participado de manera personal en el acto de firma y, contándose con sistema de fechado electrónico, de la fecha de la suscripción del documento de que se trate.

ACADEMIA JUDICIAL CHILE

SERIE DE DOCUMENTOS MATERIALES DOCENTES