

**PROYECTO DE LEY CONTRA EL USO ABUSIVO DE DATOS  
PERSONALES Y RESGUARDAR DE LOS USUARIOS ANTE EL CORREO  
ELECTRÓNICO NO SOLICITADO**

*Andrés Herrera Troncoso*  
Abogado, Universidad de Chile  
Master en Derecho de las Telecomunicaciones y de las  
Tecnologías de la Información, Universidad Carlos III de Madrid

*Alberto Cerda Silva*  
Profesor Asistente Derecho Informático, Universidad de Chile  
Magíster en Derecho Público, Universidad de Chile

**SUMARIO:** I.- INTRODUCCIÓN.- II.- OBSERVACIONES AL TEXTO DEL PROYECTO.- 1.- GARANTÍA CONSTITUCIONAL CONCERNIDA.- 2.- MARCO CONCEPTUAL DEL PROYECTO.- A) DATO PERSONAL.- B) FUENTE ACCESIBLE A PÚBLICO.- C) DATO SENSIBLE.- 3.- TRATAMIENTO DE DATOS PERSONALES PATRIMONIALES.- 4.- SISTEMA DE PROTECCIÓN ANTI-SPAM.- III.- CONCLUSIONES.

**I.- INTRODUCCIÓN**

Mediante moción parlamentaria del H. Senador Novoa se ha presentado proyecto de ley por medio del cual se propone modificar la Ley N° 19.628, sobre Protección de la Vida Privada, con el fin evitar el uso abusivo de datos personales o de empresas y de resguardar a los usuarios de correo electrónico de la propaganda comercial no solicitada.<sup>1</sup>

El proyecto de ley en comento es precedido de un extenso texto en el cual se consignan las razones que motivan el mismo, a saber: la problemática del procesamiento computacional abusivo y anónimo, con fines de lucro, de los datos personales o nominativos de empresas y personas naturales, cuyo tratamiento supone un enfoque con perspectiva que trascienda las fronteras; y, el perjuicio ocasionado por el spam o correo electrónico masivo, abusivo y no deseado, cuyo tratamiento evidencia la insuficiencia de la autorregulación y las limitaciones del contexto de la actual normativa sobre protección al consumidor en la materia.

---

<sup>1</sup> Corresponde al Boletín 3.796-07.

Al respecto, la iniciativa consulta modificar el concepto de dato personal, contenido en la citada Ley N° 19.628, para incluir en él aquéllos concernientes a personas jurídicas; extender el concepto de dato sensible para incluir entre ellos aquéllos concernientes a direcciones de correo electrónico, nóminas de clientes, y estados financieros y patrimoniales; modificar el concepto de fuente accesible a público, a efectos de evitar ciertas imprecisiones en que incurriría el tenor actual del mismo; reemplazar las hipótesis en que la ley faculta el tratamiento de datos sin autorización de su titular; limitar las condiciones que legitiman el tratamiento de datos cuando su recopilación tiene lugar en Internet; e, incorporar todo un título nuevo para reglamentar la protección de los datos sensibles en general y las direcciones de correo electrónico en particular.

## II.- OBSERVACIONES AL TEXTO DEL PROYECTO

El proyecto en examen admite observaciones en cuanto a: la determinación de la garantía fundamental afectada; la determinación de su marco conceptual, particularmente en lo concerniente a los conceptos de titular de datos personales, fuente accesible a público y dato sensible; la precisión de las condiciones que legitiman el tratamiento de datos personales patrimoniales; y, por último, el sistema de protección anti-spam que diseña. Nos detendremos en cada uno de ellos.

### I.- GARANTÍA CONSTITUCIONAL CONCERNIDA

En una primera mirada al proyecto sometido a consideración de la Comisión, se aprecia que éste titubea en cuanto a la determinación del bien jurídico que pretende tutelar, errando en la calificación del mismo, tanto a la luz de la normativa interna como del desarrollo de la doctrina especializada en la materia, particularmente en lo concerniente a las personas jurídicas; así, por ejemplo, unas veces alude al derecho a la privacidad, otras al derecho a la intimidad, o bien a la vida privada.

Con todo, y más allá de la confusión inicial respecto del bien jurídico tutelado, el proyecto plantea un conflicto de garantías constitucionales que serviría de fundamento a las modificaciones que se proponen y que, a su juicio, constituye el contexto en el que dicho proyecto debe analizarse. La moción plantea la pugna entre el derecho a la intimidad<sup>2</sup> –garantía constitucional de la que gozan las personas naturales– y el derecho a la información que reclama la sociedad toda, a la que se daría respuesta con la formulación de un nuevo concepto del citado derecho a la intimidad, que surgiría frente a la llamada “libertad informática”.

Sobre el particular, cabe considerar, en primer término, que el proyecto de ley que se materializó en la Ley N° 19.628, denominada sobre Protección de la Vida Privada, originada en una moción presentada ante el Senado con fecha 5 de enero de 1993, sólo tuvo por objeto aportar mecanismos que permitieran a las personas naturales una efectiva y adecuada protección al derecho de la vida privada, en el ámbito del derecho civil, ante eventuales vulneraciones o amenazas

ilegítimas de que pudieran ser víctimas.<sup>3</sup> Así, claramente, el proyecto no tuvo por finalidad central convertirse en una ley de protección de datos personales, aunque el legislador terminó abordando sólo esa temática en el contexto de una protección específica a la “vida privada” e intimidad de las personas, por lo que la denominación final de la Ley en la que éste se convirtió –“sobre Protección de la Vida Privada”– resultó, por cierto, demasiado genérica considerando la materia particular abordada en ella.<sup>4</sup>

Por su parte, y a fin de clarificar los motivos que han justificado la existencia de cuerpos normativos protectores de datos personales o nominativos, en cuanto mecanismo de amparo de las libertades y derechos fundamentales de la persona natural, podemos advertir que el acelerado desarrollo de las sociedades modernas ha traído consigo el surgimiento de una tercera generación de derechos humanos, vinculados íntimamente al empleo de los medios tecnológicos. Para algunos autores, estos derechos de tercera generación responden al fenómeno de la “contaminación de las libertades”, que haría referencia a la erosión y degradación que afecta a los derechos fundamentales ante determinados usos de la tecnología.<sup>5</sup> Así, las múltiples y complejas amenazas a las libertades y derechos fundamentales que, en esta nueva etapa histórica de las sociedades, puede suponer la utilización de la tecnología, o, en palabras de TONIATI, “la posibilidad de tratamiento informático por parte de una multitud de operadores, de una multitud de datos personales referidos a una multitud de sujetos”<sup>6</sup>, hace indispensable la adopción de un estatuto de protección de los datos

<sup>3</sup> Diario de Sesiones del Senado, Sesión 20 (anexo de documentos), pp. 3079 - 3089. La moción contemplaba disposiciones que determinaban la extensión de la vida privada, excluía las intromisiones ilegítimas a su respecto, brindaba instrumentos procesales para su protección frente a éstas y aun de compensación para el evento de haberse producido. Además, uno de sus títulos contenía disposiciones que regulaban el tema de la protección de los datos personales frente a su procesamiento informático. Vale decir, el proyecto esbozaba un sistema de protección a la vida privada en sus diversos aspectos, aun cuando sólo circunscrito al ámbito civil. Cabe consignar que ya con antelación se habían redactado dos proyectos de ley en la materia, los que ni siquiera llegaron a ser sometidos a la consideración del legislativo: uno ante la Junta Militar presentado por el entonces Ministro de Justicia (1986 - 1987), un segundo proyecto también del Ministerio de Justicia durante el gobierno de Patricio Aylwin.

<sup>4</sup> Vid. Informe Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados, Diario de Sesiones de la Cámara de Diputados, Sesión 3ª, 04.06.1996, pp. 149 y ss. Alguna opinión se había manifestado en el seno de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado al respecto, orientado a realizar una reflexión más profunda en cuanto al tratamiento de los datos personales y acusando la insuficiencia de la normativa prevista al respecto en el proyecto de ley. Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, en Diario de Sesiones del Senado, Sesión 63ª (anexos de documentos), p. 7486. Para una revisión de la historia de la ley, vid. CERDA SILVA, Alberto, “La Autoridad de Control en la Legislación sobre Protección frente al Tratamiento de Datos Personales”, Tesis para optar al grado de Magister en Derecho, facultad de Derecho de la Universidad de Chile, Santiago, Chile, 2003, Capítulo II.

<sup>5</sup> Sobre la polución o contaminación de las libertades, en relación con la protección de los datos personales, cf. PÉREZ LUÑO, Antonio; LOSANO, Mario y GUERRERO, María, “Libertad informática y leyes de protección de datos personales”, Centro de Estudios Constitucionales, Madrid, España, 1989, p. 144; PÉREZ-LUÑO, Antonio, “Intimidad y Protección de Datos Personales: del Habeas Corpus al Habeas Data”, en Estudios sobre el Derecho a la Intimidad, Ed. Tecnos, 1992, pp. 36 - 45; PÉREZ-LUÑO, Antonio, “Derechos humanos, Estado de derecho y constitución”, 5ª edic., Ed. Tecnos, Madrid, 1995, pp. 345 - 349. Ahora, hay doctrina que va aun más allá, esbozando derechos humanos de cuarta generación, cf. RODRÍGUEZ, Ma. Eugenia, “La Nueva Generación de Derechos Humanos. Origen y Justificación”, Universidad Carlos III de Madrid, Ed. Dykinson, 2002.

<sup>6</sup> Cit. por SÁNCHEZ BRAVO, Álvaro, “La protección del derecho a la libertad informática en la Unión Europea”, Secretariado de Publicaciones, Universidad de Sevilla, Sevilla, España, 1998, p. 35.

<sup>2</sup> En relación con el derecho a la intimidad puede verse la trascendental obra de S. D. WARREN y L. D. BRANDEIS, “The Right to Privacy”, en *Harvard Law Review* N° 5, de 1890. Obra traducida al español: S. D. Warren y L. D. Brandeis, “El Derecho a la Intimidad”, Ed. Civitas, Madrid, España, 1995.

personales, que se constituya en garantía de la libertad e igualdad de los miembros de toda comunidad.

Es menester consignar, además, que la normativa y doctrina especializada, corroborada incluso jurisprudencialmente, entiende que los derechos fundamentales a la intimidad y al honor, en atención a su contenido, no ofrecen garantías suficientes frente a las amenazas que el uso de la informática puede entrañar para la protección de las personas. Es así como, la garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excedería el ámbito propio del derecho fundamental a la intimidad, y que se traduce en un derecho de control sobre los datos relativos a la propia persona, el que se ha dado en llamar "autodeterminación informativa" en la doctrina alemana, y "libertad informativa" en las doctrinas italiana y española.<sup>8</sup>

De esta manera, se constituye un derecho autónomo y fundamental a la protección de datos, que a diferencia del derecho a la intimidad -con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar-, atribuye a su titular un cúmulo de facultades que consisten, en su mayor parte, en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos. La peculiaridad de este derecho fundamental a la protección de datos respecto del derecho fundamental tan afín como es el de la intimidad radica en su distinta función, lo que trae consigo diferencias, también, en su objeto y contenido.

En efecto, la función del derecho a la intimidad será la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, y, por su parte, el derecho a la protección de datos perseguiría garantizar a esa persona un poder de control

sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

Además, el derecho a la protección de datos tendría un objeto más amplio que el del derecho a la intimidad, ya que el primero extendería su garantía no sólo a la intimidad o privacidad, sino, también, a la "esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada", inextricablemente unidos al respeto de la dignidad personal y al pleno ejercicio de los derechos de la persona. El objeto del derecho a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su finalidad no es sólo el amparo de la intimidad individual, sino los datos de carácter personal. Por consiguiente, su ámbito de protección también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el hecho que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo.

Por su parte, este derecho fundamental a la protección de datos difiere del derecho a la intimidad en cuanto a su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido, el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que le permiten garantizar especialmente a cada persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer (como por ejemplo, el derecho a que se requiera el previo consentimiento para el tratamiento de los datos personales o el derecho a acceder, rectificar, modificar y cancelar dichos datos).

Reconociendo, entonces, la existencia de un verdadero derecho autónomo de protección de datos, con las características citadas, emanado de la denominada "libertad informática" o "autodeterminación informativa", derivada de una paulatina construcción doctrinaria y jurisprudencial "europea"<sup>9</sup>, no puede establecerse como contexto de la moción presentada la afectación pura y simple del derecho a la intimidad, en su sentido más esencial, frente a la libertad de información y al derecho de emitir opinión, dado que, si bien nuestra Ley N° 19.628 fue denominada como protectora de la vida privada, muchas de las modificaciones propuestas exceden de los límites de las

<sup>7</sup> Expresión acuñada por el Tribunal Constitucional alemán, en su sentencia de 15 de diciembre de 1983, sobre la Ley del Censo. Dicha sentencia puede encontrarse traducida al español en Boletín de Jurisprudencia Constitucional N° 33, España, 1984, pp. 126 y ss.

<sup>8</sup> La extensión que se confiere a la *privacy* en Estados Unidos rebasa -gracias a su desarrollo jurisprudencial- con creces el marco que se le atribuye en la experiencia continental, aun cuando los problemas en que se aprecia su concurrencia suelen vincularse a cuestiones sobre procreación, matrimonio, vida familiar y sexual. Cf. ORTIZ VALLEJO, Antonio, "Derecho a la intimidad e informática", Ed. Comares, España, 1994, pp. 35 y ss. La amplitud conferida a la *privacy* entre los norteamericanos explica por qué la protección de los datos queda circunscrita en ella. En cambio, para la doctrina continental es discutible si las prerrogativas que se confieren al titular de datos personales por las leyes protectoras de datos son expresión del derecho a la intimidad, o bien es necesario construir un nuevo derecho que brinde tal amparo, que se ha dado en llamar "autodeterminación informativa" en la jurisprudencia alemana y "libertad informática" en el desarrollo de la doctrina italiana y española. Cf. FROSSINI, Vittorio, "Los derechos humanos en la sociedad tecnológica", Anuario de Derechos Humanos, núm. 2, 1983, pp. 101 - 115; PÉREZ-LUNO, Antonio, "Los Derechos Humanos en la Sociedad Tecnológica", en Cuadernos y Debates, Centro de Estudios Constitucionales, Madrid, 1989, núm. 21, pp. 133 - 213; MURILLO DE LA CUEVA, Pablo Lucas, "El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales frente a la Informática", Ed. Tecnos, Madrid, 1990, *passim*. Por su parte, entre nosotros, es de la opinión que el enfoque de la autodeterminación informativa es complementario a la configuración del derecho al respeto de la vida privada. NOGUERA ALCALÁ, Humberto, "El derecho a la libertad de opinión e información y sus límites". Lexis-Nexis, Chile, 2002, pp.152 - 153. Por la autodeterminación informativa, *vid.* CERDA SILVA, Alberto, "Autodeterminación Informativa y Leyes sobre Protección de Datos", en *Revista Chilena de Derecho Informático*, núm. 3, 2003, pp. 47 - 75.

<sup>9</sup> Sobre el particular, cabe referirse especialmente a la sentencia 292/2000 del Tribunal Constitucional español, que acogiendo un recurso de inconstitucionalidad deducido por el Defensor del Pueblo en contra Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, reconoció un derecho constitucional autónomo que se contendría en el artículo 18.4 de la Constitución Española, que no sería otro que el derecho fundamental a la protección de datos personales. Dicha interpretación ha sido recogida, además, en el artículo 8° de la Carta de Derechos Fundamentales de la Unión Europea, Niza, 2000.

garantías que aseguran proteger. Así, sin perjuicio de que, al tenor de este nuevo concepto del derecho de protección de datos, se requieran de modificaciones substanciales a dicho estatuto legal que respondan a dicha noción, la reforma propuesta en cuya virtud se incorporan las personas jurídicas al ámbito de protección de la ley afecta seriamente el espíritu y los principios informadores de ésta, pues la tutela jurídica que le otorga es la misma que a las personas naturales, sin efectuar distinción alguna en su tratamiento, llegando incluso a plantear la incorporación como "dato sensible" la dirección de correo electrónico, tanto respecto de las personas naturales como de las personas jurídicas, en aras de la protección de la intimidad y la vida privada, de la cual carecen, en su sentido más puro, éstas. Para efectuar la modificación que pretende el proyecto, se requeriría no sólo plantear un nuevo enfoque al bien jurídico que se desea proteger, al amparo del citado "derecho a la protección de datos", sino que, una vez establecido lo anterior, plasmar en el nuevo cuerpo legal las necesarias diferencias en el tratamiento normativo entre las personas naturales – originarias beneficiarias de la protección que se brinda a los datos personales – y los intereses de las personas jurídicas.

Sobre esta materia, cabe indicar que la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, establece, por una parte, una protección a los derechos y libertades fundamentales de las personas naturales, entre ellos el derecho a la intimidad, y por otra, una protección a los "intereses legítimos de las personas jurídicas".

## 2.- MARCO CONCEPTUAL DEL PROYECTO

Las modificaciones comprendidas en el proyecto que se informa presentan, también, serios inconvenientes asociados a las definiciones contempladas actualmente en la Ley N° 19.628, relativas a "dato personal", "fuente accesible a público" y "dato sensible", según lo que se considera seguidamente.

### a) Dato personal (Artículo 1°, número 1, del proyecto)<sup>10</sup>

El proyecto aboga por la ampliación del ámbito de protección de la ley, al incluir entre sus beneficiarios a las personas jurídicas, de forma de prevenir diversas prácticas mediante las cuales se realiza un tratamiento indebido de los datos que les conciernen, bajo la excusa de no serles aplicable actualmente la ley sobre protección de datos. Sin embargo, si bien parece adecuado que se disponga algún grado de protección jurídica a los datos de las personas jurídicas, debe repararse en que los términos y propuestas de la moción, creemos, no resultan convenientes.

En efecto, aun cuando la citada moción conceptúa como datos personales tanto aquéllos concernientes a personas naturales como jurídicas, en algunas de sus disposiciones limita el alcance de las mismas tan sólo a las personas naturales y a las empresas, dejando fuera del alcance de las normas a toda aquella persona jurídica que no revista el carácter de tal. Así acontece, por ejemplo,

<sup>10</sup> El artículo 2°, letra f), de la Ley N° 19.628, define a los datos de carácter personal o datos personales como aquellos "relativos a cualquier información concerniente a personas naturales, identificadas o identificables".

en el artículo 1°, número 4, del proyecto, al referirse a la recopilación de datos desde Internet, ocasión en que injustificadamente se cife a las empresas y personas naturales. Tal error se observa ya en el propio mensaje que precede a la propuesta normativa del proyecto, e inclusive en el título de éste.

Los términos de la moción, al ampliar el concepto de datos personales a aquellos referidos a las personas jurídicas, suponen una completa alteración a la coherencia normativa y de principios de la Ley N° 19.628. Fuera de lo dicho anteriormente respecto de los principios que informan dicho cuerpo legal y de la extensión artificial de su ámbito de aplicación sin responder a ellos, en el proyecto no se abordan materias tales como quién debería autorizar el tratamiento de datos en el caso de una persona jurídica, quién puede requerir información de los datos de una persona jurídica, qué datos, y quién puede ejercer, en tal caso, los derechos de modificación, cancelación y bloqueo.

Por otro lado, el proyecto, así como el texto que le precede, insinúa una relación de propiedad entre el titular de los datos personales y éstos; así sucede, por ejemplo, a la hora de conceptuar las fuentes accesibles a público. Tal propuesta, lejos de contribuir a solucionar los problemas que suscita la aplicación de la Ley N° 19.628 los agravará: ¿quién puede ser calificado como dueño de los datos concernientes a falta de credibilidad financiera de una persona?, ¿la persona concernida, la persona responsable del tratamiento de los datos, o la entidad financiera o bancaria atinente? En este sentido, el proyecto prescinde de la experiencia habida en el derecho comparado, así todos los Estados miembros de la Unión Europea, y de las Recomendaciones formuladas por Naciones Unidas y la OCDE<sup>11</sup> en la materia, en todas las cuales no se establece una relación de dominio entre el titular y los datos que le conciernen, confiriéndole derechos a su respecto por la sola circunstancia de referirse a su persona.

### b) Fuente accesible a público (Artículo 1°, número 3, del proyecto)<sup>12</sup>

El proyecto acertadamente observa los inconvenientes que suscita el concepto de fuente accesible a público, cuya importancia radica en autorizar el tratamiento de los datos personales incluidos en ella con prescindencia del consentimiento del titular de los mismos.

En este sentido, resulta interesante la intención que inspira al proyecto, en cuanto a tratar que el régimen de los datos contenidos en dichas fuentes constituya la excepción y no la regla general. Los amplios términos en la definición actual contenida en el artículo 2° letra i) de la Ley N° 19.628, traen consigo que el régimen normal y común tenga un ámbito de aplicación reducido.

<sup>11</sup> "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data", Recomendación del Consejo de la OCDE, de 23 de septiembre de 1980, y su anexo "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data"; y, "Principios rectores para la reglamentación de los ficheros computarizados de datos personales", adoptados por la Asamblea General de las Naciones Unidas en su resolución 45/95, de 14 de diciembre de 1990.

<sup>12</sup> El artículo 2°, letra i), de la Ley N° 19.628, define a las fuentes accesibles al público como "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes".

En todo caso, la propuesta incurre en errores manifiestos, partiendo porque utiliza una nueva denominación sin cambiar la anterior<sup>13</sup>, y además porque produce el efecto contrario al deseado, dado que enumera sólo a título ilustrativo las fuentes en comentario.<sup>14</sup>

También produce un efecto equívoco que en la modificación planteada por el proyecto en el N° 4 de su artículo 1° se incluya la expresión “no requieren autorización del titular respectivo, *únicamente y de manera excepcional*, las operaciones de tratamiento de datos personales provenientes de las fuentes accesibles al público...” cuando en la definición de fuentes accesibles al público se deja abierta la puerta a aquéllas que reúnan los genéricos requisitos que ella contempla.

Asimismo, conviene anotar que los datos personales que constan normalmente en las fuentes accesibles al público son aquellos denominados “datos públicos de mera identificación”, que, a diferencia, de los datos de protección ordinaria y los datos sensibles, tienen menor resguardo normativo y, por ende, menos limitaciones en cuanto a su conocimiento y tratamiento por terceros (principalmente, no necesitan consentimiento del titular para tal efecto). Entre dichos datos, según el proyecto y la propia Ley Orgánica 15/1999 española, se encontrarían los contenidos en repertorios telefónicos y en las listas de profesionales. En ambos casos se halla el domicilio o residencia de una persona. Luego, cabe preguntarse, considerando el símil que puede establecerse entre el domicilio o lugar físico de su residencia y la dirección de correo electrónico (“domicilio en las redes electrónicas”) y su naturaleza de dato de “mera identificación” ¿cuál es el fundamento por el cual debe elevarse a la categoría de dato sensible la dirección de correo electrónico? La verdad es que no se divisa ninguna.

Incluso lo que pretende el autor del proyecto no sólo es eliminar de las fuentes accesibles al público el dato consistente en la dirección de correo electrónico y tras pasarlo al régimen ordinario contenido en la ley (como “cualquier información concerniente a personas naturales”), sino que, yendo mucho más allá, transformarlo en un “dato sensible”, de protección especialísima, aun respecto de las personas jurídicas, según lo que se verá.

De tal suerte, el proyecto lejos de contribuir a ahuyentar los inconvenientes que pretende conjurar, los acrecentará, ya que la enumeración de ejemplos que formula para explicarse es equívoca, sin que indique el elemento en común que permite, en último término, calificar a todos ellos como “fuentes accesibles al público”.

Más aún, pese a sus anunciados propósitos, el proyecto obvia definir si la determinación de una fuente de información cualquiera como de “accesible al público” es resultado de las condiciones materiales de la misma, o bien de una calificación jurídica previa; en otros términos, el proyecto soslaya establecer si para que exista una fuente accesible al público es necesario disponer de una norma que la declare tal, o bien basta atenerse al hecho de estar disponible para su consulta por cualquier persona.

c) **Dato sensible** (Artículo 1, números 2 y 7, del proyecto)<sup>15-16</sup>

El proyecto propone modificar el concepto de dato sensible, a efectos de que el mismo resulte aplicable a las personas jurídicas, y, a la vez, incluir en él las direcciones de correo electrónico, las nóminas de clientes, y los estados financieros y patrimoniales de las personas. Al respecto pueden hacerse las siguientes observaciones:

- i) El actual concepto de dato sensible previsto en la normativa nacional se ajusta sustancialmente al previsto en el derecho comparado, así en el Convenio N° 108 del Consejo de Europa, la Directiva 95/46/CE de la Unión Europea y la legislación de sus Estados partes, en las Recomendaciones de Naciones Unidas y la OCDE, e inclusive en los textos discutidos en el marco de APEC.  
Sucede que bajo el concepto de dato sensible existe un grado de acuerdo sustantivo a nivel de derecho comparado, lo cual garantiza la equivalencia normativa de las soluciones adoptadas a su respecto; alterar el concepto de dato sensible, aparte de injustificado, resultaría ineficaz de cara al flujo transfronterizo de datos personales y el carácter global de Internet.
- ii) La propuesta del proyecto introduce nuevos elementos de confusión, cuando no de error jurídico, al atribuir a personas naturales y jurídicas titularidad sobre unos mismos datos sensibles, tales como opciones ideológicas y religiosas, así como vida sexual, entre otros.
- iii) La propuesta es errática al atribuir al dato personal “dirección de correo electrónico” la calificación de dato sensible, en razón de: primero, carecer tal dato de una calidad intrínseca a los datos sensibles, según lo establecido en el derecho comparado, a saber el riesgo de menoscabar la intimidad de una persona o exponerle a actos de discriminación arbitraria; segundo, carecer de referente alguno en el derecho comparado que asegure la equivalencia normativa de la solución propuesta, así baste con acudir a las observaciones formuladas por

<sup>13</sup> Se refiere a las “fuentes públicas de información”.

<sup>14</sup> Las fuentes accesibles al público enumeradas en la nueva definición contenida en el artículo 1°, número 3°, del proyecto son muy similares a las señaladas en el artículo 3°, letra j) de la española Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aunque esta última, junto con conceptualizar dichas fuentes, procede a determinarlas taxativamente, manteniendo su carácter especial frente a los datos personales ordinarios. En efecto, el artículo 3°, letra j), de la Ley 15/1999 dispone que son fuentes accesibles al público “aquellas ficheros cuya consulta puede ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes accesibles al público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes accesibles al público, los Diarios y Boletines oficiales y los medios de comunicación.”

<sup>15</sup> El artículo 2°, letra g), de la Ley N° 19.628, define a los datos sensibles como “aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.”

<sup>16</sup> Según SUNE LLINAS, los datos sensibles son aquellos datos necesitados de mayor protección que la ordinaria y “que han de estar regidos por el principio general de prohibición de tratamiento –lógicamente con excepciones-, al tratarse de datos en los que la vulneración de la intimidad atenta contra el núcleo duro sobre el que se construye la inviolabilidad de la persona. Los datos sensibles han de ser datos legislativamente tasados, del tipo de origen étnico, tendencias políticas, creencias religiosas y datos sanitarios, entre otros.”. En separata *Derecho a la autodeterminación informativa y protección de datos personales*. SUNE LLINAS, Emilio, Madrid, España, 2003.

Naciones Unidas al respecto, con lo cual la propuesta evidencia no reparar en el carácter transfronterizo del fenómeno que pretende regular.

- iv) La propuesta es aun más desacertada al extender la calificación de dato sensible a los correspondientes a nóminas de clientes, así como a datos de connotación patrimonial, según lo que se dirá enseguida.

### 3.- TRATAMIENTO DE DATOS PERSONALES PATRIMONIALES

El proyecto pretende atribuir a los datos relativos a estados financieros y patrimoniales de una persona el carácter de datos sensibles, con lo cual restringiría su tratamiento sólo a los casos en que ha mediado autorización de la persona a quien se refieren o disposición legal habilitante.

El preámbulo del proyecto no consigna las razones que mueven la propuesta al respecto; sin embargo, se repara en que atribuir a tales datos el carácter de sensible carece de referente en el derecho comparado, lo cual obsta a la eficacia de la regulación, junto con constituirse en un serio obstáculo para el funcionamiento de sistemas de información crediticia actualmente administrados por entidades financieras, bancarias y otras.

Por lo que toca a calificar de sensible los datos correspondientes a nóminas de clientes, se observa que la ley sobre protección de la vida privada establece el régimen de resguardo de las personas concernidas por los datos, siendo materia de otros cuerpos legales el sistema de protección al responsable del banco datos personales ante terceros por el acceso no autorizado a los mismos, así, por ejemplo, en las normas sobre delitos informáticos, propiedad intelectual, secreto comercial u otras.

### 4.- SISTEMA DE PROTECCIÓN ANTI-SPAM

El proyecto estructura un sistema de protección especial respecto del dato personal dirección de correo electrónico, ya que no sólo se permite calificarlo erróneamente de sensible, según se ha señalado, sino que establece mecanismos para poner término a su empleo no autorizado, si bien, como se apreciará, con menoscabo de derechos fundamentales, tales como el derecho a la información, la inviolabilidad de las comunicaciones y el debido proceso legal.

En efecto, según la propuesta, la persona titular del dato personal dirección de correo electrónico podrá requerir al prestador de servicio de Internet que preste servicios de mantención y operación de casilla(s) electrónica(s) del emisor o receptor de los correos, o a quien opere como mero transportador, el bloqueo de la dirección del emisor que le envíe un correo no solicitado previamente; tal bloqueo procederá por el solo hecho de la solicitud, notificación y/o reclamo de cinco usuarios. Más aun, el prestador de servicio deberá implementar un procedimiento claro y expedito, y elaborar y publicar una lista de todas aquellas direcciones a cuyo respecto le sea solicitado bloquear la dirección del emisor, de manera que pueda ser consultada por los sistemas o servidores de correo de otros proveedores.

Pese a reconocer la necesidad de adoptar medidas técnicas y legislativas contra el spam, es necesario considerar la afectación de derechos fundamentales que ellas pueden representar. En el caso de la propuesta "notice and take down" esbozada por el proyecto, representa serios riesgos para los derechos fundamentales de quienes se comunican a través de plataformas electrónicas:

- i) Primero, porque cercena el derecho de información, consagrado en el artículo 19° número 12 de la Constitución, en su faz derecho a informar, al condicionar su pervivencia al simple requerimiento de particulares ante el prestador de servicios, al punto de constituirse en un sistema de censura previa privada.
- ii) Segundo, porque menoscaba el derecho a la inviolabilidad de las comunicaciones, al obligar a tal prestador a interceptar y/o interrumpir las comunicaciones del emisor en su caso, contrariando lo dispuesto en el artículo 19° número 5 de la Constitución, así como los ilícitos penales de los artículos 36° B de la Ley N° 18.168, General de Telecomunicaciones; 161° A del Código Penal y la propuesta de artículo 146° para el Código Penal contenida en el proyecto presidencial de ley sobre delitos informáticos en actual tramitación en el Congreso (Boletín 2.974-19).
- iii) Tercero, porque impone al presunto infractor una sanción infamante, cual es la inclusión en listados de emisores de spam, con la consiguiente merma de derechos, sin que medie resolución judicial al respecto, esto es, con infracción al debido proceso legal previsto en el artículo 19° número 3 de la Constitución y al principio de plenitud de la jurisdicción contemplado en el artículo 73° de la misma Carta Fundamental.

### III.- CONCLUSIONES

En síntesis, aun cuando el proyecto de ley parte de un análisis parcialmente acertado, en cuanto a la insuficiencia de nuestro marco normativo para hacer frente al tratamiento indebido de datos personales, las soluciones que diseña lejos de contribuir a resolver los inconvenientes actuales acentúa los mismos, generando además nuevos problemas, tales como ambigüedades conceptuales –tanto en términos operativos, como doctrinarios–, afectación de derechos fundamentales, menoscabo a los sistemas de información crediticia, y deficiencias en la equivalencia internacional de las normas.

En cuanto a la preocupación central del proyecto relativa a las medidas para evitar los envíos de correos electrónicos, cabe consignar que constituye una materia que debe abordarse en el contexto de la amplia temática de las amenazas y vulneraciones a los datos personales, a la intimidad y a la vida privada de las personas que surgen en la red de Internet en su conjunto, que ha venido a facilitar la provisión de todo tipo de comunicaciones electrónicas. Ello ha traído nuevas posibilidades, pero también nuevas amenazas y riesgos a dichos derechos y libertades fundamentales.

Por lo precedentemente expuesto, no se justifica impulsar una reforma que sólo trate parcialmente y no de manera integral, como sería deseable, los eventuales atentados a tales derechos en el mundo de las comunicaciones electrónicas. Basados en iguales motivaciones y principios habría que proponer, entonces, una adecuada protección de los datos personales relati-

vos al tráfico y localización de las comunicaciones y equipos que utilice el suscriptor (por ejemplo, computador, teléfono móvil, fax, etc.); a la identificación de las líneas telefónicas en una comunicación de esa naturaleza; a los datos de facturación de servicios de telecomunicaciones; a la adopción de medidas de seguridad y confidencialidad de la información y de las comunicaciones.

Con todo, se debe valorar la preocupación evidenciada por el proyecto en comento en procura de hacerse cargo de los numerosos reparos de que es actualmente objeto nuestra ley sobre tratamiento de datos personales, desde que se trata de un marco jurídico que requiere adecuaciones necesarias para permitir al país gozar de niveles de seguridad acordes a las exigencias de una Sociedad de la Información. Sin embargo, con el mismo énfasis en que valora la intención legislativa, se debe manifestar los serios reparos en cuanto a las soluciones esbozadas en tal proyecto.