Privacidad de la información digital: autodeterminación vs. *commodity*

Francisco González Hoch [*]

I. Información digital y privacidad

1. El avance tecnológico de las computadoras, junto a la facilidad para comunicarlos, han provocado un enorme aumento en la cantidad de información disponible respecto a cualquier persona. Esto ha permitido a algunos sostener que vivimos en la era de la "información digital", la cual plantea desafíos antes desconocidos para el derecho de la privacidad.

2. En efecto, la privacidad, entendida como la esfera de reserva que protege hechos o informaciones de carácter personal y que naturalmente entendemos excluidos del conocimiento de terceros, es amenazada por el desarrollo de la tecnología, que facilita a cualquier persona adquirir información sobre otra que normalmente no podría conocer sin su autorización. Tanto es así que, intuitivamente, una de las primeras preocupaciones al pensar sobre la pérdida de privacidad de nuestra "información personal"[1] por obra de bases de datos computacionales, es averiguar el tipo de información que sobre nosotros está disponible a terceros e identificar quiénes pueden acceder a ella.

3. El derecho se ha preocupado extensamente de la protección de la privacidad desde fines del siglo pasado[2], como consecuencia del surgimiento de nuevas técnicas de obtención y difusión de información que aparecían como amenazas a la vida privada, aún cuando la precisa definición de los contornos de lo privado continúe siendo objeto de análisis y debate. Como ha dicho un autor, la batalla por la privacidad en el siglo veinte ha sido una lucha por adaptar los principios sobre privacidad a los constantes avances tecnológicos[3]. Lo que subsiste es la preocupación central por preservar el carácter privado o confidencial de la información

---

[*] Abogado, profesor de derecho de la Facultad de Derecho de la Universidad de Chile.

1. En este sentido, Raymond Wacks, *Personal Information, (Privacy and the Law)*, Oxford University Press, 1989, quien define "información personal" como "los hechos, comunicaciones u opiniones que se relacionan con el individuo y que sería razonable esperar que éste considerara como íntimos o sensibles y que, por tanto, quisiera retirar o al menos restringir su recolección, uso o circulación" (página 26). En este trabajo, la información personal relevante es la *"información digital"*, esto es, la contenida en registros o bases de datos computacionales, aunque nada obsta a que los argumentos aquí expuestos se extiendan también a información personal contenida en otros registros.

2. Por su trascendencia y vigencia actual, es común en la doctrina mencionar que la reflexión legal contemporánea sobre privacidad comenzó con el artículo de S. Warren y L. Brandeis, "The Right of Privacy", *Harvard Law Review*, 4, 1890, páginas 189 y siguientes; hay traducción al español como *El Derecho a la Intimidad*, edición preparada por Benigno Pendás y Pilar Baselga, Madrid, Civitas, 1995.

3. Robert Gellman, "Does Privacy Law Work?", en Philip E. Agre and Marc Rotenberg editors, *Technology and Privacy: The New Landscape*, Massachusetts Institute of Technology, 1997, página 203.

que nos atañe, en el sentido de retener cierto control sobre su uso y diseminación[4].

4. La batalla continúa, por lo que cualquier regulación legal de los tres aspectos que se muestran como claves en la materia, esto es, (i) definir la clase de información que puede o debe estar disponible libremente al público, (ii) identificar los derechos de las personas cuya información está en las bases de datos y (iii) definir a quién corresponde la palabra final respecto al uso de la información personal, supone optar entre justificaciones morales, filosóficas y jurídicas contrapuestas.

5. En este trabajo se postula, por una parte, que el desarrollo de tecnologías de información digital y la facilidad de su acceso han alterado inadvertida pero radicalmente la distinción entre "información pública" e "información privada", lo que obliga a repensar y regular sus límites; y, por la otra, que, por regla general, debe reconocerse a toda persona el control final de la información que le atañe, en ejercicio de un derecho de autodeterminación informativa, pues, de lo contrario, su información personal se convierte en una simple mercancía o *commodity.*

6. Pretender reflexionar sobre esta materia partiendo de cero parece absurdo. Por ello, el plan de este trabajo será, en primer lugar, examinar la legislación comparada; en segundo, analizar la acción de *Hábeas Data,* que permite acceder a información personal y corregirla, existente en diversos países americanos y europeos; en tercer lugar, esbozar el debate doctrinario sobre el fundamento y alcance de la especial protección que requiere la información personal; y, en último, formular algunos comentarios personales, con especial referencia a la situación legal en Chile.

II. Experiencia legal comparada

A. Europa

7. Tanto las legislaciones nacionales internas como los acuerdos multilaterales entre los países miembros de la actual Unión Europea han tenido un enorme desarrollo en las últimas tres décadas, cuyo examen es particularmente valioso porque muestra las adaptaciones de que han sido objeto las reglas, a medida que el avance de la tecnología planteaba nuevos retos, y mientras se acumulaba experiencia en la aplicación de las primeras regulaciones.

Estas regulaciones, desde 1970[5], nacieron fruto de la reacción de temor ciudadano frente a la amenaza de creación, por parte del gobierno,

4. El creciente interés actual por la privacidad se muestra, entre otros, en que un libro de fuerte contenido legal pero escrito en lenguaje cotidiano se haya convertido en un Best Seller: *The Right to Privacy*, Ellen Alderman & Caroline Kennedy, Vintage Books, 1997.

5. Ley de protección de datos del estado alemán de Hesse. A ella le siguieron la ley sueca de datos (1973), la ley de protección de datos del estado alemán de Rheinhald-Pfalz (1974) y la ley federal alemana sobre protección de datos (1977).

de una base de datos computacional centralizada capaz de almacenar toda la información existente sobre la vida de los particulares[6].

8. Es interesante destacar que el nombre empleado uniformemente en las regulaciones europeas, desde 1970 hasta nuestros días, para describir lo que actualmente se entiende como el derecho a controlar la información respecto a uno mismo ha sido "protección de datos"[7]. Las primeras leyes no mencionaban la palabra privacidad, ni la expresión "información personal", empleada frecuentemente en la doctrina. El uso de palabras técnicas (datos, bases de datos) antes que jurídicas (privacidad, intimidad), se justifica en que las primeras leyes dictadas en Europa sobre la materia sólo buscaban regular tecnologías[8]. Si bien esas leyes fueron luego modificadas o interpretadas a la luz de las nociones de privacidad e intimidad, según se verá, los antiguos términos técnicos fueron conservados.

9. Desarrollo generacional de la legislación europea. La legislación de los países europeos sobre privacidad de la información (o "protección de datos"), puede ser explicada históricamente como un sistema de reglas desarrollado en cuatro generaciones o etapas, marcadas por preocupaciones específicas que justificaron el dictado de nuevas normas o la modificación de las ya existentes[9].

10. La *primera* generación de leyes (entre 1970 y 1977) fue dictada como respuesta al tratamiento electrónico de datos por parte del gobierno y de grandes empresas. Las normas se centraron básicamente en regular esta nueva tecnología de "procesamiento electrónico".

De esta manera, la mayoría de las normas de la primera generación no buscaban proteger la privacidad individual sino sólo regular el rol del procesamiento de datos frente a la sociedad. La protección de datos era vista, desde esa perspectiva, como una herramienta para enfrentar el peligro que la computación representaba a través del procesamiento de información sobre individuos determinados. Las reglas buscaron fijar un "correcto uso" del procesamiento de la información, estableciendo tempranamente el procedimiento de acceso a los datos, la posibilidad de corregir la información, y los mecanismos de registro y licencia previos a la recolección de la misma[10]. Por último, el cumplimiento de las reglas no se dejó entregado a los propios individuos -a quienes no se dio acción directa- sino a una agencia o entidad especialmente creada al efecto[11].

11. La *segunda* generación, a cuya vanguardia estuvieron las legislaciones de Francia, Austria, Dinamarca y Noruega (dictadas entre

---

6. Viktor Mayer-Schönberg, "Generational Development of Data Protection in Europe", en Philip E. Agre and Marc Rotenberg editors, *Technology and Privacy: The New Landscape*, Massachusetts Institute of Technology, 1997, páginas 219-241.

7. Ya es un lugar común mencionar -siguiendo a Spiros Simitis, el primer comisionado de protección de datos del estado alemán de Hessen- que no son los "datos" los que necesitan protección, sino la persona con la cual los datos se relacionan. Véase Mayer-Schönberg, *op.cit.*, página 219.

8. Mayer-Schönberg, *op.cit.*, página 224.

9. Mayer-Schönberg, *op.cit.*, páginas 221-235.

10. Mayer-Schönberg, *op.cit.*, página 221.

11. Nacieron así el Comisionado de Protección de Datos en Hessen (1970), el Consejo de Inspección de Datos de Suecia (1973) y el Comisionado Federal Alemán de Datos (1977), todos ellos precursores de la más contemporánea Agencia de Protección de Datos de España (1992).

1977 y 1978), surgió como respuesta a la multiplicación de registros computacionales, públicos y privados, nacidos tras la invención de los minicomputadores a mediados de los setenta.

Desaparecido el temor a un registro computacional central del gobierno, la atención se centró en la protección de las personas frente al peligro derivado de la posible recolección y procesamiento computacional indiscriminado de información personal, por el gobierno o por particulares. El punto central de esa segunda generación fue el derecho de privacidad de cada ciudadano, aplicando al campo computacional conceptos como el "derecho a ser dejado solo" (de origen angloamericano) y el derecho de cada uno a delimitar su propio espacio de intimidad. Por primera vez, la protección de datos fue vinculada explícitamente al derecho de privacidad, y éste concebido como el derecho del individuo a rechazar a la sociedad en asuntos personales[12]. En este mismo sentido, a la privacidad de la información se le dio rango constitucional en Austria, Portugal y España[13].

Esta generación agregó sustancia a mecanismos que antes fueron concebidos como meramente procedimentales, reconociendo no sólo la facultad del individuo para acceder y corregir su información personal, sino también la de decidir en ciertas ocasiones, cuál información suya podría usarse y con qué fines. De esta manera, la protección de datos, concebida originalmente sólo como un intento de regular la tecnología computacional se convirtió en una nueva forma de libertad individual[14]. Además de agregarle contenido, se reconoció a los ciudadanos un papel central al permitirles exigir el cumplimiento forzado de las nuevas leyes. Asimismo, se extendieron las facultades de las entidades encargadas de hacer cumplir las normas convirtiéndolas, algunas veces, en *ombudsman* que abogaban por los derechos del afectado, y, otras veces, en tribunales en las disputas sobre violación del derecho a privacidad en la información, al ejercer facultades de interpretación con carácter vinculante de la ley[15].

12. La *tercera* generación nació con un fallo del Tribunal Constitucional Alemán, en 1983, que al pronunciarse sobre la Ley de Censo acuñó la expresión "autodeterminación de la información"[16]. Con esta sentencia, la libertad individual, entendida como el derecho a excluir o rechazar invasiones a la información personal, noción típica de la segunda generación, fue transformada en un derecho constitucional mucho más participativo. Este derecho constitucional consiste, como señaló el Tribunal Constitucional, en la "aptitud

12. Mayer-Schönberg, *op.cit.*, página 226.

13. El artículo 18.4 de la Constitución Española de 1978 establece: "La ley *limitará* el uso de la *informática* para garantizar el honor y la *intimidad* personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos", (énfasis añadido) con lo que pone de manifiesto el carácter de amenaza con que el constituyente español concibe la informática, y la obligación que impone al legislador de "limitarla".

14. Mayer-Schönberg, *op.cit.*, página 227.

15. Es el caso especialmente de la Comisión de Protección de Datos de Austria, que puede decidir controversias entre particulares y autoridades públicas. También ocurre así con las agencias holandesa y noruega; véase Mayer-Schönberg, *op.cit.*, página 228.

16. 15 de diciembre de 1983, 1 BvR 209/83-NJW 1984, página 419; véase Mayer Schönberg, *op. cit.*, página 229.

de la persona para decidir por sí misma, de manera general, la entrega y uso de su propia información personal".

El mismo Tribunal estableció que todas las fases del procesamiento de la información, desde su recopilación hasta la transmisión de la misma estaban sujetas a limitaciones constitucionales y que, por tanto, los derechos de participación del individuo debían ser extendidos a todas esas etapas[17]. La Corte agregó que cada vez que el gobierno pidiera información personal a los ciudadanos, debía explicar por qué necesitaba esa información y las consecuencias específicas de la negativa a suministrarla.

Las leyes de la tercera generación se basaron en los fundamentos y decisión del Tribunal Constitucional ya citada[18], y se caracterizaron por el énfasis puesto en el derecho individual a la participación y la autodeterminación de la información. En palabras de un autor austríaco, ante la realidad innegable de que en la sociedad contemporánea nadie puede optar en forma seria por no participar en ella completamente, lo decisivo es que "debe darse a los individuos la oportunidad de definir la forma en que toman parte en la sociedad mediante la entrega de información personal"[19].

13. Por último, la *cuarta* generación de leyes europeas (1990-1998) ha tratado de superar las limitaciones de la anterior, estableciendo diferentes soluciones para enfrentar un problema clave: la débil posición negociadora en que generalmente se encuentran los individuos al ejercer sus derechos de privacidad. Este problema ha sido enfrentado tanto tratando de restablecer cierto equilibrio mínimo de la posición en la que se encuentra el individuo frente a las poderosas administradoras de bases de datos como fijando áreas de protección legal obligatoria[20].

El primer mecanismo -en mi opinión, de enorme trascendencia al cambiar el eje fundante de la responsabilidad civil- consistió en crear un sistema de responsabilidad estricta (objetiva), como es el caso de la reforma a la ley alemana sobre la materia[21]. El segundo mecanismo -protección de datos "sensibles"- persiguió prohibir la recopilación o manutención de ciertos tipos de datos[22]. Especialmente relevante es la Directiva sobre Protección de Datos de la Unión Europea de 1995, que prohibe el tratamiento de datos personales que revelen (i) el origen racial o étnico, (ii) las opiniones políticas, (iii) las convicciones religiosas o filosóficas, (iv) la pertenencia a sindicatos, así como el tratamiento de los datos

17. Mayer-Schönberg, *op.cit.*, página 230.

18. Se trata básicamente de reformas a leyes existentes, por ejemplo: modificación a leyes de diversos estados alemanes como consecuencia de la sentencia del Tribunal Constitucional; la modificación a la ley austríaca de protección de datos (1986); la reforma a la Ley Federal Alemana sobre protección de datos (1990); y, la adopción de una garantía constitucional específica en materia de privacidad de la información en Holanda.

19. Mayer-Schönberg, *op.cit.*, página 231.

20. Mayer-Schönberg, *op.cit.*, páginas 232-233.

21. Ley Federal de Protección de Datos de 1990, §7.

22. Así ocurre con nuevas leyes dictadas en Noruega, Finlandia, Dinamarca, Bélgica, Francia e Inglaterra, que imponen prohibiciones absolutas de procesar "información sensible".

relativos a (v) la salud o a (vi), la sexualidad, excepto en casos específicos expresamente enumerados[23].

La *cuarta* generación impulsó el dictado de normas para ciertas áreas específicas (sectoriales), atendiendo a sus características particulares. Esta tendencia fue recogida por la Directiva de la Unión Europea, mediante la idea de "códigos de conducta sectoriales", por lo que es previsible que ella será la fuente de nuevas leyes nacionales europeas[24].

La tendencia legislativa europea más reciente apunta a separar las tareas públicas de supervisión del cumplimiento de las leyes, de aquéllas relativas a la decisión de conflictos derivados de violaciones a la privacidad de la información. Subsiste, en el centro del modelo legal de protección de datos, el derecho a la participación y autodeterminación del individuo en materia de información, pero ahora apoyado y reforzado con la intervención estatal directa para dar efectividad al cumplimiento de esos derechos.

B. Estados Unidos

14. La regulación de los Estados Unidos tiene fuertes diferencias con la legislación de países europeos, como se verá al analizar la protección legal de la privacidad de la información digital en ese país, materia que será examinada en tres sedes distintas: leyes especiales sobre privacidad, principios constitucionales y acciones basadas en el *common law.*

15. Leyes especiales sobre privacidad: en forma semejante a lo ocurrido en Europa, fue el temor frente al poder que podía alcanzar el gobierno centralizando en materia computacional la información privada de los particulares la causa que motivó el dictado, en 1974, de la primera ley sobre privacidad *(Privacy Act)*[25].

Esta ley estableció reglas generales sobre recolección, manutención, uso y entrega de información personal en poder de agencias federales. Como su objetivo principal fue restringir el uso por el gobierno de tecnología computacional para invadir la privacidad[26], la primera gran limitación de esta ley es que no se aplica a las relaciones entre particulares, lo que presenta una importante diferencia con las legislaciones europeas, de aplicación indistinta al sector público y privado. La ley sobre privacidad ha sido objeto de fuertes críticas por la doctrina, reprochándosele la ausencia de una autoridad que supervise su cumplimiento y la vaguedad de sus disposiciones, muchas de las cuales se han convertido en letra muerta por carecer las agencias gubernamentales de incentivos o amenazas para cumplirlas. Se le ha criticado, asimismo, la falta de restricciones

23 Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, artículo 8º.

24. Un ejemplo es la ley de Finlandia, que regula el uso de bases de datos para investigación científica, estadísticas, investigación de mercado, marketing directo y reportes de crédito; véase Mayer-Schönberg, *op.cit.*, página 241, nota 65.

25. 5 U.S.C. §552a (1994).

26. Gellman, *op.cit.*, página 195.

efectivas a la difusión externa de información privada fuera del ámbito o propósito para el cual esa información fue recolectada[27].

16. Con respecto a las bases de datos privadas, la ley más importante que regula los derechos de los consumidores y las responsabilidades de los titulares de las bases de datos, es la ley sobre Corrección al Emitir Reportes de Crédito *(Fair Credit Reporting Act*, de 1970 y modificada por última vez en 1996 [28]). Esta ley incluye normas sobre acceso y corrección de datos; límites a la recopilación, uso y divulgación de información; acciones judiciales y mecanismos administrativos de cumplimiento, entre otras.

17. Principios constitucionales: si bien el texto de la Constitución de los Estados Unidos no menciona la palabra "privacidad", ello no ha impedido que existan amplios debates constitucionales en su nombre, los que han abarcado desde el derecho a la reproducción (aborto), hasta la prohibición de ser objeto de arrestos o registros ilegales. Sin embargo, en materia de *privacidad de la información* no existen pronunciamientos claros de la Corte Suprema[29].

Uno de los fallos frecuentemente citados es *Katz v. United States*[30] en el que la Corte Suprema de 1967, cambiando un precedente sentado en 1928, decidió que la intercepción de líneas telefónicas constituía un tipo de "cateo o registro", cubierto por la norma constitucional que protege a los ciudadanos contra registros y arrestos no razonables. Con todo, la Corte sostuvo que la Cuarta Enmienda sólo protege la privacidad individual contra ciertos tipos de intrusión gubernamental, pero no establece un derecho constitucional general de privacidad. Por último, la Corte declaró que la protección del derecho general de una persona a su privacidad "está entregado principalmente -así como la protección de su propiedad y de su vida misma- a la ley de los estados individuales [y no a la Constitución]". De esta manera, la importancia del fallo radica más en aquello que niega (protección constitucional generalizada a invasiones a la privacidad) que en aquello que afirma (exclusión de pruebas obtenidas ilícitamente -mediante intercepciones telefónicas-, área del derecho constitucional y procesal penal bastante desarrollada).

Diez años más tarde, la Corte Suprema examinó la posibilidad de que existiera un derecho constitucional de privacidad de la información en *Whalen v. Roe*[31], caso en que se discutía la constitucionalidad de una ley estatal que ordenaba reportar al estado de Nueva York, y guardar en una base de datos computacional, los nombres y direcciones de todas las personas que obtuvieran ciertas drogas. Si bien la Corte falló que la exigencia de divulgar información al estado no era inconstitucional, un autor sostiene que ello se debió en gran parte a los fuertes resguardos contra usos no autorizados de la información que contemplaba la misma ley. La Corte no se pronunció derechamente sobre la existencia de un

27. Gellman, *op.cit.*, página 201.
28. 15 U.S.C. 1681-1688t (1994).
29. Gellman, *op.cit.*, página 201.
30. 389 U.S. 347, 1967.
31. 429 U.S. 589, 1977.

derecho constitucional de privacidad de la información, aún cuando insinuó que el deber del estado de evitar divulgaciones impropias de la información "podría argumentarse que tiene sus raíces en la Constitución".

Finalmente, la Corte Suprema ha reiterado que no existe protección constitucional respecto al acceso a bases de datos computacionales mantenidas por terceros. Así, en *United States v. Miller* [32], un fallo de 1976 aún vigente, la Corte decidió que una persona no tenía expectativas de privacidad en registros de cuentas mantenidos por un banco. Según el fallo, el titular de la cuenta bancaria no tenía derecho a saber u oponerse cuando el gobierno pidió al banco información sobre su cuenta.

18. Acciones basadas en el *common law:* Estas acciones se fundan en la amenaza de que particulares usen bases de datos computacionales en forma impropia, violando la privacidad de las personas cuya información está contenida en esas bases de datos.

En un influyente artículo de 1960[33], William Prosser, autor también de uno de los más renombrados tratados sobre responsabilidad civil extracontractual *(Torts)*, clasificó en cuatro grupos los ilícitos de violación de privacidad reconocidas en el common law: (a) Intrusión: irrupción (física o de cualquier otro modo) en la soledad de otro de una manera altamente ofensiva; (b) Revelación pública de hechos privados: publicar información privada de otro altamente ofensiva, que no es de interés legítimo para el público; (c) Falsedad: publicar una opinión altamente ofensiva y falsa sobre otro; y, (d) Apropiación: usar el nombre o la apariencia de otro, sin su consentimiento, para obtener una ganancia[34].

El problema, como lo destaca un autor, es que la protección que pueden otorgar las acciones nacidas de los ilícitos por violación de privacidad del common law es por completo insuficiente[35]. A ello se suma que las características propias de la información digital -como su utilización al interior de una organización sin manifestación externa y sin que el afectado siquiera lo sepa- hacen difícil sino imposible configurar los supuestos de hecho propios de las acciones clásicas fundadas en intrusión física, divulgación pública o falsas luces. Por último, debe destacarse que la doctrina sostiene que en el estado actual del derecho no puede haber responsabilidad por el uso de información contenida en un registro público[36].

---

32. 425 U.S. 435, 1976.

33. William Prosser, "Privacy", *California Law Review*, 48, 1960, páginas 383-423.

34. Los cuatro grupos descritos por Prosser fueron recogidos en el *Restatement (Second) of Torts*, §§652A-E (1977); para una explicación en español véase José Martínez de Pisón, *El Derecho a la Intimidad en la Jurisprudencia Constitucional*, "Civitas", 1997, páginas 32-33.

35. Gellman sostiene que los ilícitos clásicos de privacidad probablemente no podrán "inducir o forzar al titular de la base de datos a publicar descripciones de los sistemas de registro, a limitar sus prácticas de recopilación de información, a cumplir con estándares de calidad de la información, a permitir acceso y corrección individual, o a restringir usos internos de la información", *op.cit.*, página 210.

36. Gellman, *op.cit.*, página 210.

C. Comparación Europa - Estados Unidos

19. Resulta sorprendente constatar que, a pesar de haber surgido como respuesta a un temor inicial común -la creación de una base de datos centralizada por el gobierno- las reglas y principios sobre protección de la información personal de los países de Europa y Estados Unidos mantienen fuertes diferencias al menos en tres áreas claves: existencia de una agencia encargada de hacer cumplir las normas, aplicación general de las normas a bases de datos públicas y privadas, y, protección constitucional clara a la privacidad de la información.

La explicación para las diferencias entre el modelo europeo y el americano se encuentra, en palabras del profesor italiano Vittorio Frosini, en que: "en la legislación federal de los Estados Unidos, se afirmó en la práctica el principio según el cual 'todo está permitido, salvo lo que está prohibido' por una interdicción expresa y motivada de la ley"; en el otro extremo, la ley federal de la República Alemana parece basada, al contrario, en la regla según la cual cualquier actividad relativa al procesamiento de datos personales 'está siempre prohibida, salvo cuando está permitida' por una autorización expresa del poder público"[37].

III. Acción de *Hábeas Data*

20. En la legislación comparada se han establecido diferentes mecanismos para prevenir violaciones a la privacidad de la información personal que puedan derivarse del tratamiento computacional de datos. Si bien la extensión de la protección y los instrumentos legales específicos varían de un país a otro, pueden reconocerse en todos ellos características comunes que manifiestan la preocupación por el peligro que el uso de información digital puede significar para la intimidad.

Los mecanismos legales consisten básicamente en (i) resguardos para el procesamiento computacional de información, y, (ii) la *acción de hábeas data*, que permite a una persona conocer, corregir, actualizar o cancelar información personal que le afecta, mecanismos que se examinan a continuación.

21. Resguardos para el procesamiento computacional de información digital: Estos pueden examinarse, ejemplarmente, a la luz de las normas españolas, en especial la Ley Orgánica 5/1992, sobre regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), que dio cumplimiento al mandato constitucional de "limitar el uso de la informática para garantizar el honor y la intimidad personal de los ciudadanos" (artículo 18.4).

Esta ley contiene principios generales que rigen la recolección de información, destinados a garantizar tanto la veracidad de la información personal como la "congruencia y racionalidad" del uso de los datos, esto es, que ellos no sean utilizados sino para la finalidad con que fueron obtenidos[38].

---

37. Vittorio Frosini, *Informática y Derecho*, Editorial Temis, Bogotá, 1988, página 120.

38. Francisco Fernández, "El Régimen Jurídico del Tratamiento Automatizado de los Datos de Carácter Personal en España", en *Ius et Praxis*, Universidad de Talca, 1997, año 3, Nº1, páginas 33-69. La exposición de los principios sigue básicamente esta obra, páginas 57 - 63.

La doctrina española ha distinguido seis grupos de principios orientadores de la protección a la información personal: consentimiento del afectado, tratamiento de datos sensibles, calidad de los datos, medidas de seguridad, deber de secreto y cesión de datos[39].

El principio básico en esa ley es exigir la obtención del *consentimiento del afectado* para el tratamiento computacional de sus datos, salvo en casos exceptuados: (a) recolección de datos de fuentes accesibles al público, (b) recolección para ejercer funciones propias de la administración pública, o, (c) recolección de datos cuando éstos se refieran a "personas vinculadas por una relación de negocios, una relación laboral, una relación administrativa o un contrato y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato" (Ley, artículo 6º).

El principio del consentimiento se ve especialmente reforzado a propósito de la *información sensible*, pues en algunos casos (ideología, creencias religiosas) se exige el consentimiento expreso y por escrito del afectado, y, en otros (raza, salud, vida sexual) que exista una autorización legal expresa, pero en ambos casos se prohibe n las bases de datos con ese solo objeto.

El principio de la *calidad de los datos* es el más amplio, pues comprende varios otros principios. El más importante, en mi opinión, es la exigencia de congruencia entre la finalidad perseguida y la información recabada (artículos 4.1, 4.2). Además, la exigencia de que los datos sean verídicos, exactos y actuales (artículos 4.3, 4.4), la prohibición de la recolección por medios fraudulentos, desleales o ilícitos (artículo 42), la orden de que los datos sean almacenados de forma de poder acceder a ellos el interesado (artículo 4.6) y, por último, el derecho a que los datos desaparezcan después del plazo establecido en la ley o en las relaciones contractuales entre el administrador de la base de datos y el afectado (artículo 15.5).

En resguardo del principio de *seguridad de los datos*, la ley obliga a adoptar medidas para evitar la pérdida, alteración, tratamiento o acceso no autorizado (artículo 9). La ley impone el *deber de secreto profesional* al responsable de la base de datos y a quienes intervengan en el tratamiento de datos de carácter personal (artículo 10).

Por último, la ley española reconoce expresamente que al cruzar información contenida en diversas bases de datos puede lograrse un perfil personal de un individuo, violando así su privacidad[40].

22. Acción de Hábeas Data: Probablemente el mecanismo más importante para la protección de la información personal mediante el control de su uso es

39. Fernández, *op.cit.,* páginas 57-63.

40. Así, la Exposición de Motivos de la Ley Orgánica 5/1992 (LORTAD) señala: "El progresivo desarrollo de las técnicas de recolección y procesamiento de datos y de acceso a los mismos ha expuesto la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: aquella es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo- *la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado"*.

la *acción de hábeas data*, que permite típicamente a un individuo conocer, rectificar y cancelar los datos que se refieren a él[41].

El término *acción de hábeas data* ha sido empleado principalmente por ordenamientos constitucionales y legales de España y de diversos países latinoamericanos, si bien su contenido da cuenta de derechos semejantes a aquellos reconocidos a las personas en las leyes de protección de información personal de Europa y Estados Unidos examinadas en el capítulo II *(supra*, párrafos 7-18).

23. Fue Brasil, en 1988, el primer país que usó en su Constitución la expresión *Hábeas Data* (artículo 5 inciso 72[42]), bajo la influencia de la Constitución de Portugal, de 1976, que establece limitaciones al uso de la computación por la autoridad pública[43]. Es interesante destacar que las nuevas constituciones que se dictaron en Brasil y Portugal fueron consecuencia de la instauración de la democracia luego del derrocamiento de dictaduras militares, y una de sus objetivos fue permitir conocer la información almacenada por las antiguas policías políticas en sus bases de datos. Una situación semejante ocurrió en Paraguay, en 1992[44].

24. Una de las características generales más destacadas de la acción de hábeas data es que, en atención a los objetivos que busca cautelar (protección de la información personal), se establecen mecanismos especialmente rápidos de solución de conflicto, en muchos casos mediante acciones judiciales de carácter constitucional, sea dentro del régimen general de las acciones de amparo o tutela (Colombia, por ejemplo), sea con acciones específicas de protección de datos informáticos (como en Perú y Argentina)[45].

25. La extensión de los derechos que otorga la acción de hábeas data varía según los ordenamientos legales. Si bien el elemento común de toda

---

41. Así, la doctrina argentina ha definido la acción de hábeas data señalando que ésta es "un instrumento para controlar la calidad de ellos, corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su posible transmisión"; véase Miguel Ángel Ekmekdijian y Calogero Pizzolo (h.), *Hábeas Data. El derecho a la intimidad frente a la revolución informática*, Depalma, Buenos Aires, 1996, página 23.

42. Constitución de Brasil (1988), artículo 5 inciso 72: "Se concederá Hábeas data: primero, para asegurar el conocimiento de informaciones relativas a la persona del solicitante, que conste en registros o bancos de datos de entidades gubernamentales o de carácter público. Segundo, para la rectificación de datos, cuando el interesado no prefiera hacerlo por proceso sigiloso, judicial o administrativo".

43. Dalmo de Abreu Dallari, "El Hábeas Data en Brasil", en *Ius et Praxis*, Universidad de Talca, 1997, año 3, Nº1, páginas 71-80.

44. El artículo 135 de la Constitución de Paraguay dispone: "Toda persona puede acceder a la información y a los datos que sobre sí misma o sobre sus bienes obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y su finalidad. Podrá solicitar ante el magistrado competente la actualización, rectificación o destrucción de aquellos, si fuesen erróneos o afectaren ilegítimamente sus derechos"; véase Luis María Benítez, "La acción de Hábeas Data en el Derecho Paraguayo", en *Ius et Praxis*, Universidad de Talca, 1997, año 3, Nº1, páginas 107-118.

45. El artículo 43 párrafo tercero de la Constitución de Argentina, de 1993, dispone: "Toda persona podrá impetrar esta acción (se refiere al amparo) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

acción de esta clase es conocer, rectificar y -a veces- cancelar información, hay sistemas jurídicos, como el peruano por ejemplo[46], en cuya Constitución de 1993 se permite, además, actualizar la información, excluir datos sensibles y asegurar la confidencialidad de datos de carácter reservado (secreto bancario, tributario o médico).

Esto ha permitido a la doctrina clasificar la acción del *hábeas data*, en atención a sus objetivos, en cinco grupos: (1) *Hábeas data informativo:* procura recabar información en bases de datos, y contempla tres subgrupos: (i) exhibitorio: para que se exhiban los datos, ejerciendo el derecho de acceso; (ii) finalista: para conocer con qué finalidad se registró la información; y, (iii) autoral: para saber quién obtuvo los datos (y quién los ha accedido); (2) *Hábeas data* aditivo: tiene por finalidad agregar algo a la información existente en la base de datos (ej.: actualizar la información o incorporar nuevos datos, aclarando que una deuda se ha pagado); (3) *Hábeas data corrector:* su objetivo es modificar la información que no sea verdadera; (4) *Hábeas data reservador:* persigue asegurar la reserva o confidencialidad de la información, evitando que trascienda a terceros; y, (5) *Hábeas data cancelatorio*: su propósito es eliminar información "sensible", que puede dar lugar a discriminación, tal como la relativa a ideas políticas o religiosas, orientación sexual, raza y enfermedades[47].

26. De esta manera, la acción del hábeas data se manifiesta como un instrumento especialmente eficaz para proteger y delimitar la información contenida en bases de datos. Es indicativo, en cuanto a la importancia que se le atribuye al tema, resaltar que al menos siete países iberoamericanos tienen disposiciones de rango constitucional que se refieren directamente a la protección de la información personal contenida en bases de datos computacionales[48], a los cuales deben sumarse también las constituciones de Holanda (1983), de Suecia (1990) y de Hungría (1993).

IV. Fundamento y alcance de la protección legal a la información digital

27. En los capítulos anteriores se han expuesto las reglas y mecanismos existentes en el derecho comparado respecto al tratamiento de la protección de la privacidad de datos personales mantenidos en bases de datos computacionales.

En el debate doctrinario sobre el fundamento y alcance que debe darse a ese tratamiento, compiten justificaciones morales y jurídicas contrapuestas, entre aquellos que postulan la liberalización completa en el uso masivo de las bases de datos, fundados en consideraciones de bienestar general, y, quienes están en favor de que la recopilación y divulgación de la información digital

46. Francisco J. Eguiguren, "El Hábeas Data y su Desarrollo en el Perú", en *Ius et Praxis*, Universidad de Talca, 1997, año 3, Nº1, páginas 119-135.

47. Néstor Pedro Sagües, "El Hábeas Data en Argentina (Orden Nacional)", en *Ius et Praxis*, Universidad de Talca, 1997, año 3, Nº1, páginas 107-118.

48. Como se vio, estos países son Portugal (1976), España (1978), Brasil (1988), Colombia (1991) , Paraguay (1992), Perú (1993) y Argentina (1994).

dependa de la voluntad de cada persona. Estas concepciones serán examinadas brevemente a continuación.

28. Liberalización en el uso de información digital: Desde una perspectiva de análisis económico del derecho, se parte de la base que *el mercado* funciona más eficientemente mientras mayor sea la información de que dispongan sus agentes. Por ello, si se permite que la información sea puesta a la libre disposición de quien la necesite, disminuirán los costos de transacción para obtenerla y podrán tomarse decisiones menos arriesgadas, lo que traerá consigo una maximización del bienestar social por la disminución del costo del crédito.

En caso contrario, si la información no estuviese fácilmente disponible, habría que incurrir en mayores costos para obtenerla, los créditos se otorgarían en condiciones más riesgosas, aumentarían los costos de recuperación de préstamos, y, en definitiva, se produciría una disminución del bienestar social, porque el sistema financiero sería más ineficiente, los créditos más caros y su otorgamiento más engorroso.

Para lograr que los actores del mercado puedan decidir con la mayor cantidad de información posible, además de los mecanismos tradicionales para conocer la historia de morosidad o solvencia de una persona, se propone que también los datos laborales y penales sean de libre acceso público, para que eventuales empleadores y otras contrapartes puedan consultarlos antes de tomar sus decisiones. Este argumento ha sido planteado usando un concepto amplio de mercado, no limitado sólo a relaciones comerciales sino que incluye casi cualquier tipo de interacción personal, afectiva, laboral, etc.

Muchas veces este argumento se presenta con una analogía entre relaciones personales y la compraventa de cosas, señalando que así como no hay razones para permitir el fraude en la venta de mercaderías (si se oculta información acerca de sus defectos), tampoco hay buenas razones económicas para permitir a las personas tener derechos de propiedad sobre información que las desacredita frente a terceros[49].

29. Argumentos en contra del uso indiscriminado de la información digital: Aun cuando, en principio, puede parecer un objetivo social eficiente y equitativo el tratar de lograr la masificación del crédito y la disminución de su costo, el primer problema que éste presenta es la dificultad para valorar la pérdida de espacios de reserva producidos con ese uso indiscriminado, para poder comparar pérdida y beneficio y obtener una conclusión en términos utilitaristas.

Pero independiente del problema de valoración utilitarista, se postula que la liberalización en el uso de información digital conlleva inevitablemente la pérdida de espacios de intimidad o reserva que nos permiten desarrollarnos como persona y gobernar nuestras relaciones de amistad, afecto, familia, etc.

Por ello, la tesis que postula una amplia difusión de la información personal puede ser rebatida desde diversos ángulos, sea desde la perspectiva tradicional de la protección de la privacidad, sea desde el punto de vista de la protección especial que requiere la información personal digitalizada mediante el derecho a la autodeterminación informativa.

---

49. Richard A. Posner, "The Right of Privacy", 12, *Ga. Law Review*, 393, 1978.

30. Restricciones al uso indiscriminado de la información digital basadas en la privacidad: Entre quienes abogan por una protección amplia de la privacidad se sostiene que es falsa la analogía entre el ocultamiento de información en la venta de mercaderías y la información personal respecto a individuos, uno de los argumentos esgrimidos para abogar por una mayor divulgación de la información que desacredita a una persona, como se recordará, y que esta diferencia entre mercaderías y personas justifica un tratamiento legal diferente, fundándose en diversas razones, según se examina brevemente[50]:

(a) Se ha sostenido por algunos que la privacidad radica en que el control sobre la información personal es de importancia crítica para preservar la *autonomía* del individuo frente a otros actores del medio social. Se persigue cautelar la dignidad personal y la individualidad. Por eso, sin la posibilidad de ocultar sus pensamientos e inclinaciones del escrutinio de otros, la persona se fusionaría con la masa, dejando de ser individuo[51].

(b)Charles Fried argumentó que la necesidad de la privacidad se basa en que el "control de la información respecto a uno mismo" es una condición necesaria para desarrollar relaciones de intimidad con otros, en especial relaciones de amor, amistad y confianza[52]. Si bien diez años más tarde modificó su posición respecto a que el *control de la información sobre uno mismo* fuese "la condición necesaria" para el desarrollo de relaciones de amor, amistad y confianza, mantuvo que las relaciones personales "dependen de un sentido seguro de sí mismo, un sentido de que al menos moralmente uno es de uno mismo y no de propiedad de otros, o incluso de la comunidad como un todo"[53]. En esta misma línea, se ha argumentado que la "privacidad de la información" está dada por una expectativa razonable de que, bajo circunstancias normales, la mayoría de la información respecto a uno mismo no está disponible públicamente[54].

(c) Diversos autores han destacado que existe una estrecha relación entre la posibilidad de retener u ocultar alguna información y la habilidad para desempeñar efectivamente *roles* sociales diferenciados[55]. Por ello, sólo cuando una persona tiene control sobre la información sobre sí misma pueden mantenerse el desempeño creíble de los roles sociales[56].

---

50. Sigo aquí, en parte, la exposición de Kim Scheppele en: *Legal Secrets, Equality and Efficiency in the Common Law,* The University of Chicago Press, Chicago, 1988, páginas 181-184.

51. Edward. J. Bloustein, "Privacy is Dear at Any Price: A Response to Professor Poner's Economic Theory", 12, *Ga. Law Review*, 393, 1978, páginas 429-453; el origen está en un artículo más antiguo, Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", 39, *NYU Law Review*, 962, 1964.

52. Fried, Charles, "Privacy", *Yale Law Journal,* 77, 1968, página 482; también citado por Scheppele, *op.cit.*, página 182.

53. Fried, Charles, "Privacy: Economics and Ethics, A Comment on Posner", 12, *Ga. Law Review,* 423, 1978.

54. Judith Wagner DeCew, *In Pursuit of Privacy, (Law, ethics and the rise of technology)*, Cornell University Press, Ithaca, 1997, página 75.

55. Véase, entre otros, Enrique Barros, "Honra, Privacidad e Información: un crucial conflicto de bienes jurídicos", en *Revista de Derecho*, Universidad Católica del Norte, Sede Coquimbo, 1998, páginas 45-58 (especialmente 50 y 51).

56. Scheppele, *op.cit.*, página 183.

(d) Por último, otros autores han argumentado en favor de un derecho de privacidad especialmente fuerte en contextos que involucran entrega de información por particulares al gobierno o a grandes corporaciones, fundados en el desequilibrio en los recursos y el poder entre una persona y esos actores[57] .

31. Restricciones al uso indiscriminado de la información personal basadas en la protección especial que merece la información digital (derecho de autodeterminación informativa): las objeciones que pueden formularse al uso indiscriminado de la información personal desde la perspectiva de la privacidad entendida como secreto, confidencialidad, reserva o esfera de intimidad, no son las únicas.

En efecto, el concepto de "información personal" es más amplio que el de privacidad, pues el primer concepto abarca, en general, toda la información que identifica, atañe o se refiere a un individuo, aún cuando no sea "secreta", "confidencial" o "reservada", facetas típicas de la privacidad en una concepción estricta.

Lo que ocurre, sin embargo, es que los datos que identifican a una persona pueden ser aisladamente considerados inofensivos o aparentemente triviales, pero su agregación altera los convierte en una amenaza para la reserva o identidad de una persona.

De esta manera, queda en claro que el bien jurídico tutelado mediante las técnicas de protección de datos no sólo es el derecho a la vida privada. Como señala un autor chileno, "queda claro, de la sentencia del Tribunal Constitucional alemán, que basta con la presencia de datos absolutamente aislados, que no digan relación alguna con la intimidad, para que la lesión al derecho de autodeterminación informativa pueda producirse a consecuencia de la vinculación de estos datos y de la construcción de un perfil del individuo que no corresponde a su personalidad"[58] .

Por ello, la protección de aquella información personal que no está directamente cubierta por el concepto de privacidad significa, de alguna manera, establecer una protección ex-ante de datos personales que, de ser agregados, ponen en peligro la intimidad de una persona.

En esta perspectiva, se ha postulado que en las sociedades informatizadas, el derecho a la intimidad, entendido tradicionalmente como una "libertad negativa" que permite cautelar la reserva y soledad de una persona, se trasmuta o deviene en una libertad positiva llamada *libertad informática*, que posibilita el control sobre la información personal[59] .

El concepto de libertad informática es homologable a lo que la doctrina alemana conoce como derecho a la *autodeterminación informativa*, y tiene por objeto reconocer que compete al individuo el control final respecto a la información que le concierne, por lo que ésta sólo puede ser usada con su

---

57. Scheppele, *op.cit.*

58. Christian Suárez, "Informática, Vida Privada y los Proyectos Chilenos sobre Protección de Datos", en *Ius et Praxis*, Universidad de Talca, 1997, año 3, Nº1, páginas 321-359, cita en página 354.

59 Pérez Luño, Antonio-Enrique, *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 1986, páginas 317-357; hay también una ordenada exposición en Zúñiga, Francisco, "El Derecho a la Intimidad y sus paradigmas", en *Ius et Praxis*, Universidad de Talca, 1997, año 3, Nº1, páginas 285-313 (en especial 300 y 301).

consentimiento. Así, la doctrina española ha señalado que este derecho pretende satisfacer la necesidad sentida actualmente por las personas de "preservar su identidad controlando la revelación y el uso de los datos que les conciernen y protegiéndose frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos propia de la informática y de los peligros que esto supone"[60].

V. Comentarios con referencia a la situación legal en Chile

32. Existen dos problemas centrales, en mi opinión, respecto a los cambios y peligros para la vida privada que está produciendo el desarrollo no regulado de tecnologías de la información.

33. El primer problema dice relación con nuestros entendimientos implícitos de reserva de la información al participar en algunas actividades públicas. Así por ejemplo, cuando yo proporciono información personal como condición para inscribirme en los registros electorales y poder votar en las elecciones, lo hago en la creencia de que esa información será usada únicamente con el fin para el cual fue entregada y que sólo podrá ser conocida por los encargados del Registro Electoral. En otras palabras, si para ejercer el derecho a voto es requisito inscribirse, la información (nombre, edad, domicilio, RUT, etc.) es dada bajo el entendimiento, implícito o explícito, de que se contribuye así a lograr un objetivo público concreto y específico: que haya elecciones limpias.

Surge así que existe o debería existir una diferencia clara de tratamiento entre (i) la información dada a una autoridad pública y (ii) la información de libre disponibilidad pública. Ocurre, sin embargo, que el desarrollo de tecnologías de información digital ha alterado inadvertida pero radicalmente la distinción entre lo público y lo privado, lo que obliga a repensar y regular sus límites. Además, esta alteración radical entre lo público y lo privado produce como segunda consecuencia la necesidad de utilizar en la protección de la intimidad un concepto amplio de privacidad o vida privada, que incluya prácticamente toda la "información personal" de un sujeto, excluyendo únicamente aquella información imprescindible para que las relaciones comerciales puedan desenvolverse.

En muchos casos se identifica inadvertidamente "información dada a la autoridad pública" con "información pública" y, al hacer ambas sinónimas se da por entendido que toda la información contenida en registros públicos puede ser accedida libremente por terceros, sin restricciones. Cabe analizar por separado los registros cuya función propia es dar publicidad a ciertos actos, de aquellos que simplemente están a cargo de autoridades públicas, para percibir que ambos generan amenazas a la reserva de la información personal.

34. (1) Es indudable que hay registros públicos que cumplen funciones puras de publicidad, de manera tal que cualquiera pueda enterarse de su contenido, hacer valer sus derechos, etc. La digitalización y el avance de las comunicaciones permiten que toda la información contenida en estos registros esté disponible para cualquiera al alcance de la mano, con sólo apretar un

60. Pablo Lucas Murillo, *El Derecho a la Autodeterminación Informativa*, Tecnos, Madrid, 1990.

botón de su computadora personal en su escritorio, lo que parece el sueño ideal del registro público de acceso universal. En este caso, sin embargo, la tecnología actual permite (a) cruzar bases de datos, (b) agregar información parcial antes dispersa y (c) buscar por elementos comunes de identificación (carnet de identidad, por ejemplo), con lo que pueden obtenerse resultados impensados al momento de crear esos registros públicos. En otras palabras, es posible obtener un verdadero "perfil" de una persona, con la más variada información respecto a ella que consta en los registros públicos, tales como quienes son los miembros de su familia, dónde vive, qué propiedades posee, qué automóvil tiene, y muchas otras.

Así, el carácter agregativo de la información digital inherente a la tecnología computacional, puede convertir la recopilación y divulgación de los datos más inocentes o triviales en amenazas reales para la privacidad de una persona, tanto (i) porque la agregación permite construir una imagen o descripción detallada de una persona a partir de sus datos parciales como (ii) porque cada dato separado, por irrelevante que parezca, puede ser usado como elemento de cruce o búsqueda en otras bases, en un interminable puzzle de bits que se unen en la construcción de la identidad digital de una persona, puesta a disposición de cualquier tercero.

35. (2) Por otra parte, en las bases de datos que mantienen autoridades públicas sin que tengan funciones de publicidad puras, la situación causada por el avance indiscriminado de la computación es aún más grave, porque (i) no sólo se repite el problema de la agregación de la información que permite prácticamente conocer a una persona sino que (ii) se desvirtúa por completo la finalidad para la cual la información fue proporcionada, al permitir que cualquier tercero la conozca -como ocurre en Chile con la información del Servicio Electoral, que éste vende y que una administradora de bases de datos comerciales (DICOM) pone a disposición del público por una tarifa-, y (iii) como consecuencia, se pierde por completo la seguridad y las expectativas respecto a qué es lo público y qué lo privado.

Puede imaginarse un caso de probable ocurrencia en un futuro no muy lejano, para mostrar la forma en que la tecnología altera imperceptiblemente nuestras percepciones y expectativas implícitas de intimidad o reserva. Este es el caso de las escrituras públicas llevadas por las Notarías, pudiendo argumentarse que éstas otorgan actualmente grados de reserva y confidencialidad relativos, porque si bien cualquiera puede inspeccionar los registros, no existen medidas de publicidad que permitan a un tercero conocer su contenido, al menos no sin incurrir en altísimos y por lo tanto impracticables costos de búsqueda (entre otras cosas, porque tendría que revisar todas las Notarías). Por esa precisa razón, en casos especiales el legislador exige que se cumplan formalidades adicionales de publicidad, como la publicación de un extracto en el Diario Oficial, para dar la posibilidad de conocimiento a terceros. Si en el futuro todas las escrituras públicas de Chile se digitalizaran y guardaran en una base de datos central, permitiéndose libre acceso por terceros con sólo apretar un botón en su computadora y pudiendo conocer así el detalle de todas las transacciones en que ha participado una persona, ¿no sería evidente que la reserva implícita con que actuaba esa persona habría desaparecido, por mucho que esas transacciones hayan constado en "escrituras públicas"? ¿No

sería obvio que en estas nuevas circunstancias sería aconsejable repensar el objetivo y funciones que cumplen las escrituras públicas, para que el avance tecnológico no los altere ni cambie las expectativas implícitas de reserva relativa con que participamos en los actos celebrados ante los Notarios? [61]

36. El segundo problema dice relación con el tipo y cantidad de información respecto a actos comerciales que estamos de acuerdo esté disponible libremente para ser conocidos por terceros.

Así, en principio desde una perspectiva del derecho civil tradicional, la deuda que yo mantenga con un banco es una relación jurídica que vincula y afecta únicamente a las dos partes del contrato, el banco como acreedor y yo como deudor, sin que los terceros tengan injerencia alguna. Ocurre, sin embargo, que el no pago de las deudas puede interesar también a terceros, para quienes la solvencia, historia comercial o capacidad patrimonial del deudor son factores decisivos para otorgar créditos. Por esta razón, desde hace muchos años- en Chile, particularmente, desde 1928[62] - el no pago de ciertos tipos de documentos mercantiles (cheques y letras de cambio, por ejemplo) dejó de ser un hecho exclusivo de las partes, al permitirse publicar tales incumplimientos para conocimiento de terceros.

Mi intuición es que permitir la publicación de información sobre incumplimientos comerciales es correcto -tanto por la mayor eficiencia debida a menores costos de transacción en buscar información, como porque todo contrato, directamente o por la forma en que se cumpla, puede afectar a terceros, en especial si éstos son acreedores actuales o potenciales del deudor- pero la experiencia, al menos en Chile, enseña que por esta vía la extensión de la información que se pone a disposición de terceros puede ampliarse a límites insospechados (hoy incluye además quiebras, multas administrativas, juicios, bienes raíces, obligaciones laborales y previsionales, entre otros), poniendo en grave peligro la privacidad de nuestra información personal, según se examinará a continuación.

37. Desarrollo de las bases de datos computacionales en Chile: este país es un caso típico de desarrollo de bases de datos computacionales en un sistema jurídico anómico, en que no existen normas específicas que regulen la recopilación, almacenamiento y difusión de información digital a terceros.

La ausencia de reglas ha permitido que empresas administradoras de bases de datos comerciales recopilen y vendan a terceros la más variada cantidad de información sobre cualquier persona, incluyendo, información relativa a: nombre, domicilios en los últimos 5 años, fecha de nacimiento, RUT, morosidades, protestos de letras y cheques, actividad económica, multas,

---

61. Un argumento similar, aunque más complejo, puede hacerse respecto al uso de otros bienes públicos, como las calles. Basado en que las calles son públicas o de uso público, ¿podrían instalarse cámaras de televisión y almacenarse la información respecto a quienes y a qué hora transitan por las calles (de ser posible identificarlos, como automóviles, por ejemplo)? ¿Y podría existir una base de datos de libre acceso que permita saber quién (y cuándo) usó los "bienes públicos" constituidos por las calles? En mi opinión, no se podría sin una pérdida grave de la privacidad en la vida diaria, por mucho que las calles sean "públicas".

62. Me refiero al Decreto Supremo Nº950, de Hacienda, de 1928, que reglamentó las publicaciones de protestos de letras de cambio y cheques en el Boletín de Informaciones Comerciales de la Cámara de Comercio de Santiago.

bienes raíces y avalúos, juicios tributarios, fecha de última declaración de impuestos, teléfono, estado civil y nombre del cónyuge, características de la casa-habitación, sociedades, y muchas otras. Además, existen bases de datos "restringidas", en que información sobre deudores financieros, de consumo y por *leasing*, junto a un registro "histórico" es suministrada sólo a ciertas personas con un contrato especial.

En el sistema bancario, por otra parte, se ha establecido un mecanismo de "información consolidada de deudas", que permite a cada banco e institución financiera tomar conocimiento de las deudas mantenidas por una persona con el sistema financiero en su conjunto. Además, esta información debe ser suministrada a la Superintendencia de Bancos, entidad que resguarda que no se produzca una concentración excesiva de los créditos en grupos de personas, situación que contribuyó en el pasado a la crisis bancaria y financiera de 1982.

Por último, en la administración pública existen también las más variadas bases de datos, cuyas características generales son la dificultad o imposibilidad para cualquier particular de conocer la información que le atañe contenida en esas bases, y que muchas veces esta información sea puesta indiscriminadamente a disposición de las administradoras de bases comerciales, quienes las cruzan con otras bases y permiten su libre acceso por terceros.

38. Régimen constitucional y legal chileno sobre protección de privacidad de información digital: la Constitución chilena no establece normas especiales de protección de privacidad en la información personal. El tema está incorporado en una garantía más amplia, "el respeto y protección a la vida privada y pública y a la honra de la persona y de su familia" (Constitución Política de 1980, artículo 19, Nº4).

El mecanismo más eficaz de amparo de los derechos constitucionales es una acción especial llamada "Recurso de Protección". Este recurso, cuya ventaja principal es su rápida tramitación y fallo al ser conocido en primera instancia directamente por la Corte de Apelaciones, ha cumplido en ciertos casos funciones semejantes a una rudimentaria acción de *Hábeas Data*, pero en general de alcance muy limitado, como se verá brevemente a continuación:

39. Jurisprudencia constitucional chilena sobre protección de datos personales:

(a) Un problema discutido con frecuencia ha sido la cancelación, por antigüedad, de la información computacional. Las reglas que rigen la publicación de protestos de cheques y pagarés establecen que los Bancos y financieras no pueden rechazar un crédito basados en información comercial superior a 5 años, pero en la práctica existe una base de datos "histórica" (con información que sobrepasa ese plazo). Diversos recursos de protección han tratando de poner fin a esta anómala situación ejerciendo el "*derecho al olvido*", pero en general la Corte, con una argumentación carente de sentido de la realidad práctica, ha señalado que la circunstancia que la administradora de bases de datos comerciales "mantenga, en forma íntegra y según su historia cronológica, información recogida de una publicación oficial, reconocida por la ley, y la proporcione a sus usuarios,

no constituye un acto ilegal o arbitrario" [63], por lo que ha rechazado los recursos basados en esta causal[64].

Creo que éste es un caso paradigmático de los peligros que conlleva el no entender que el avance tecnológico ha cambiado la forma de obtención de la información por terceros.

El derecho al olvido consiste en que después de pasado cierto tiempo, ciertos actos (incumplimientos, moras, condenas) sean dejados atrás y no se les considere al evaluar a una persona determinada. Por eso, lo que importa aquí no es si los registros electrónicos son transcripción de una publicación "oficial", como argumenta la Corte, sino simplemente que después del plazo establecido esos registros electrónicos deben borrarse. La defensa empleada por las administradoras de bases de datos de que borrar la información digital antigua "no produce el efecto de borrar lo que está escrito, impreso, publicado y distribuido" desconoce que al borrar el dato electrónico se elimina el principal medio por el cual los terceros acceden a esta información, pues es muy costoso y engorroso desplazarse físicamente a las bibliotecas a consultar la información impresa hace más de cinco años. Por ello, eliminar la información computacional antigua es el único medio efectivo de que el "derecho al olvido" sea una realidad concreta y no una mera ilusión.

(b) En otros casos se ha pedido la *eliminación* de antecedentes errados, basándose en que la protección de la vida íntima de las personas cubre también su buen nombre comercial[65]. En este tipo de fallos ha influido, sin duda, que en Chile la protección constitucional de la intimidad (vida privada) y de la honra están estrechamente vinculadas, al punto de confundirse en algunas oportunidades.

(c) Por la vía del recurso de protección también se ha planteado la *corrección* de errores cometidos por falta de cuidado y diligencia de la administradora de bases de datos comerciales al transcribir la información desde los boletines comerciales al medio computacional. Así ha sucedido en el caso de publicaciones de protestos de cheque con un número de RUT (correspondiente al girador de los cheques) que no coincidía con el nombre de la persona que aparecía como incumplidora de la obligación, quien nada debía y que presentó el recurso para que se ordenara hacer la corrección pertinente[66].

---

63. Corte Suprema, 23 de junio de 1994, publicado en Fallos del Mes Nº427, página 309; Cámara de Apelaciones de Santiago, 16 de octubre de 1996, confirmado por la Corte Suprema el 17 de marzo de 1997 (Of. Coordinadora, Nº68/97) y Cámara de Apelaciones de Santiago, 15 de junio de 1997, confirmado por la Corte Suprema el 19 de Agosto de 1997.

64. Al respecto, véase Alonso Calvo Thiele, *Tribunal Privado. Chile, una larga y angosta sábana de datos público-privados*, Editorial Norma, Santiago, 1997, con una fuerte crítica a las "bases de datos históricas".

65. Así se desprende del fallo de la Corte de Apelaciones de Valdivia, de 7 de noviembre de 1996, confirmado por la Corte Suprema el 31 de diciembre de 1996 (Of. Coordinadora, Nº60/97), que rechazó la distinción planteada en la defensa de la administradora de base de datos entre "hechos de la vida privada comercial" (no sujetos a tutela constitucional) y "hechos íntimos de la vida de una persona, cuya difusión puede ser desdorosa" (objeto de protección).

66. Cámara de Apelaciones de Concepción, 12 de noviembre de 1993, confirmado por la Corte Suprema el 3 de diciembre de 1993, en Fallos del Mes Nº421, página 1075.

(d) La Corte se pronunció en una ocasión sobre el *concepto de vida privada* (la denominación empleada por la Constitución para referirse a privacidad), entendiendo por tal "aquella zona que el titular del derecho no quiere que sea conocida por terceros sin su consentimiento"[67].

40. Proyectos de ley en Chile que se refieren al tratamiento de datos digitales:

Se han presentado al menos dos proyectos de ley importantes en los últimos años que tratan de la regulación legal de la información personal de carácter digital, cuyo análisis permite mostrar la forma en que se ha razonado y argumentado respecto a este tema en Chile.

El primer caso corresponde a la última modificación a la Ley General de Bancos[68]. Durante la tramitación de esta ley, se planteó por el Ejecutivo la conveniencia de crear un registro consolidado de deudas, agregando al sistema consolidado de información sobre deudas bancarias las deudas mantenidas por personas naturales con casas comerciales (ventas a crédito), que agregadamente superaran cierto monto. Se hicieron fuertes críticas a esta idea desde dos frentes: (i) las casas comerciales alegaron que, al obligarséles a suministrar la información de sus bases de datos, se les privaría del derecho de propiedad sobre esas bases, garantizado por la Constitución (artículo 19, Nº24); y, (ii) la entrega forzada de información sobre deudores de casas comerciales constituiría, asimismo, una violación al derecho de privacidad de tales deudores. Si bien finalmente la ley fue promulgada sin el capítulo relativo a la consolidación de información comercial y bancaria, es interesante constatar que gran parte de la discusión legislativa -y la disputa por conquistar a la opinión pública en los diarios- se centró más en el derecho de propiedad que en la privacidad. Por lo demás, sorprende que se hable sin más del derecho de propiedad sobre las bases de datos computacionales de las casas comerciales, en circunstancias que los datos corresponden a los clientes, quienes deberían poder exigir al término de la relación contractual que sus datos sean eliminados. De ser así, más que "propietarios" de bases de datos, las casas comerciales serían en verdad detentadores, con autorización temporal, de bases que contienen información esencialmente ajena.

El segundo caso corresponde a un proyecto de ley presentado en 1992 para la "protección civil de la vida privada", que todavía está en trámite legislativo. El proyecto planteaba originalmente establecer reglas legales para cautelar en detalle las garantías del artículo 19, Nº 4 de la Constitución, siguiendo el modelo de las legislaciones españolas (LORTAD), alemana, noruega y francesa, pero durante su tramitación fue fuertemente modificado y convertido en un proyecto de objeto más acotado, la "protección de datos de carácter personal". Esta iniciativa legal establece, en esencia, regular la obtención de información contenida en bases de datos públicas (algo semejante a lo regulado en Estados Unidos con la Ley de Libertad de Información) y, establecer normas sobre el tratamiento informático de datos, y en especial los derechos que se conceden a las personas

67. Cámara de Apelaciones de Santiago, 31 de mayo de 1993 (caso *Martorell*), confirmada por la Corte Suprema el 15 de junio de 1993, Fallos del Mes Nº415, página 347.

68. Ley Nº19.258, publicada en el Diario Oficial del 4 de noviembre de 1997.

respecto a su información personal, estableciendo por primera vez una acción de Hábeas Data en el sistema legal chileno.

Valgan sólo dos observaciones respecto a este proyecto, para mostrar que compiten en él las justificaciones contrapuestas examinadas en este trabajo (liberalización o uso indiscriminado de la información versus protección general de la liberad personal):

(A) Durante su discusión en el Congreso, la mayor administradora de bases de datos computacionales del país (DICOM), planteó la necesidad de distinguir entre: (i) aspectos relativos a la esfera íntima de las personas, entre los cuales se cuentan principios religiosos y filosóficos, antecedentes étnicos, filiación natural o ilegítima enfermedades u operaciones y, "en general, aquellos antecedentes cuya divulgación cause dolor, aflicción o vergüenza"[69]; y, (b) antecedentes de carácter comercial que terceros pueden estar en condiciones de conocer para mejor relacionarse social y económicamente. Obviamente, la administradora planteaba que sólo debían ser objeto de protección la "información íntima" (cuya divulgación cause dolor, aflicción o vergüenza), dejando desprotegida por completo todo el resto de la información personal.

(B) No está claro cuál es el principio inspirador del proyecto de ley. En efecto, si bien en el proyecto de ley se establece que "se reconoce a toda persona el derecho a recolectar, procesar, custodiar y transferir datos", se agrega luego que se reconoce este derecho a fin de "proteger a las personas por el uso que terceros puedan hacer de sus datos personales". Por eso se ha criticado que la ley se centre en la "recolección" de los datos, y se postula que "se debe partir de la base del derecho a la libertad informática de los individuos y no del derecho general a recolectar y difundir información" [70].

41. Conclusiones: información digital, ¿autodeterminación o *commodity*?

(1) La experiencia del derecho comparado muestra que la evolución de la tecnología computacional presenta amenazas constantes para nuestra percepción del ámbito de privacidad y formación de nuestra identidad en que nos desenvolvemos con expectativas razonables de reserva. El peligro de no estar consciente respecto a esta amenaza lleva a que se produzca lo que un autor lúcidamente ha llamado "la silenciosa habilidad de la tecnología para erosionar nuestras expectativas de privacidad"[71].

De igual manera, la tecnología diluye las barreras de lo público y lo privado, en desmedro de lo privado, pues se pone en conocimiento de terceros información proporcionada con fines públicos específicos y determinados. Finalmente, datos que aparentemente eran inofensivos o triviales, al ser agregados continuamente con otros también nos afectan, por lo que pasan a ser merecedores de protección, aún cuando no estén incluidos en el concepto tradicional de "privacidad" o "vida privada". Esto obliga a entender la protección

69. Presentación del fiscal de Dicom, don Jaime Guerrero, en el seminario organizado por la Universidad de Talca, publicado en *Ius et Praxis*, Universidad de Talca, 1997, año 3, Nº1, páginas 209-218.

70. Suárez, *op. cit.*, en nota 58, página 357.

71. Paul Schwartz, "Privacy and participation: Personal information and public sector regulation in the United States", *Iowa Law Review*, 80, 1995, página 553-563, citado por Gellman, *op. cit.*, en nota 3, página 211.

de la información personal digitalizada en forma más amplia que la privacidad.

(2) El peligro que crea la tecnología de la información ya no es el de poder central que conozca todos nuestros actos -a la manera de la pesadilla orwelliana de "1984", que dio lugar a la primera generación de leyes europeas- sino más bien el que se cree una sociedad digitalizada, en que la pérdida de nuestra intimidad, de nuestra vida personal y hasta de nuestra identidad esté dada porque todos conozcan todo sobre todos.

En otras palabras, la pesadilla orwelliana ha devenido en la amenaza de la creación de una especie de "conventillo informático" en el que, a semejanza de la vida en los pequeños pasajes o cités urbanos de principios de siglo, mantener espacios de reserva e intimidad sea por completo imposible, pues nuestra información personal se entiende que pertenece también al grupo social.

(3) Si bien es cierto que el mercado requiere de información para funcionar, la entrega de la información debe estar basada en el principio de autodeterminación informativa, esto es, que sea la propia persona involucrada la que tenga la decisión final respecto al destino de su información. Por ello, la entrega de información puede ser incentivada mediante mecanismos que beneficien al que participe suministrando la información (menores tasas o comisiones, etc.), pero no puede hacerse por defecto, sin consentimiento del afectado. El único límite está en el incumplimiento de obligaciones comerciales, porque ya hay asentadas prácticas y tradiciones a este respecto.

Si no se reconoce el principio de autodeterminación informativa, la información personal de un individuo se convierte en una simple mercadería o commodity, al menos en dos sentidos distintos: (a) la información personal que atañe a un individuo es objeto de compra y venta por los administradores de las bases de datos, quienes reclaman sobre esa información "derechos de propiedad". Así, información que atañe a una persona se transa en el mercado sin su consentimiento; y, (b) se produce el absurdo que la privacidad se transforma de un derecho subjetivo (a que terceros no me conozcan) en una simple cualidad u opción agregada respecto a un producto (como el color, duración, etc.), por el cual además hay que pagar, a fin de no ser molestados por terceros (así, por ejemplo, en el caso de servicios telefónicos en que debe pagarse para no aparecer en la guía, para no tener identificación cuando se hacen llamadas, etc.)[72].

72. En este sentido, Simon G. Davies, "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity", en Philip E. Asgre and Marc Rotenberg editors, *Technology and Privacy: The New Landscape*, Massachusetts Institute of Technology, 1997, página 160.