Europa y la Protección de los Datos Personales*

Ahti Saarenpää
Decano Facultad de Derecho de la Universidad de Laponia, Finlandia[1]
Profesor de Derecho Privado y Director del Instituto de Derecho Informático

1. La protección de los datos personales como un problema legal

La protección de los datos personales es un problema *social*; y es también un problema *legal*. En una palabra, es un problema con "P" mayúscula. En la sociedad de la información, el camino hacia la apropiada protección de los datos personales está lleno de obstáculos. Y podemos fracasar al percibir esto si nosotros pensamos que la cuestión está reducida a la regulación legal de los datos en un sentido técnico. Simplemente no podemos funcionar prescindiendo de los datos personales en nuestra moderna sociedad de la información.

No, no podemos manejarnos sin disponer de datos personales. Estamos acostumbrados a usar diferentes *formas de identificación,* desde nuestro nombre o una imagen hasta diversos identificadores biométricos. Usamos estas formas de *identificación* para comprobar nuestra *identidad* y permitirnos ser identificados en diferentes situaciones.[2] Así podemos hablar de

---

* Traducción desde el inglés de Alberto Cerda Silva, investigador del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile. Efectuada dentro del marco de la investigación *"Intimidad y nuevas tecnologías. Análisis de la tutela efectiva a los derechos de los titulares de datos personales en Chile"*, financiada por el Departamento de Investigación de la Universidad de Chile.

1 El autor ha participado en el anteproyecto de Ley de Datos Personales de Finlandia como miembro del Comité de Datos Personales.

2 Es importante, de hecho esencial, observar que la identidad y la identificación son cosas distintas. Una persona puede disponer de muchas identidades, tantas como sus datos personales le permitan. Éstos se utilizan en diversa manera para la identificación del individuo. Cf., por ejemplo, Saarenpää *"The Constitutional State and Digital Identity"*, II Congreso Mundial de Derecho Informático, Madrid 2002, www.ieid.org/congreso/ponencia_i.htm

sistemas de identificación; por ejemplo, el número de identificación personal usado en los países nórdicos, tendencia técnica natural. Nosotros repudiamos los códigos cerrados e identificadores biométricos únicos que son manifestaciones de tal ambición. El desarrollo tecnológico permite incrementar la precisión y seguridad de los medios de identificación.

Entonces, ¿por qué debería el tratamiento y la protección de los datos personales constituir una cuestión legal? Me parece que a lo menos por cuatro razones: las exigencias de la democracia, la sociedad red, la búsqueda de la eficiencia y el complejo curso vital de la información. Cuando mi colega y amigo el Profesor *Timo Konstari*, el principal experto finlandés en Derecho Público, describió la primera Ley de Protección de Datos Personales de Finlandia como la ley más dificultosa de su vida, él parecía perplejo, pero había dado en el clavo.[3] Las cuatro consideraciones que he citado hacen conjuntamente de la protección de los datos personales un extraordinariamente difícil problema social, y un aun más complicado problema legal.

Donde la *democracia* está concernida, la cuestión es la relación entre lo público y lo privado. En una genuina democracia, la maquinaria social existe para nosotros, los ciudadanos. Nosotros disponemos de nuestro derecho a la *autodeterminación*. Nosotros concedemos a la sociedad, a los medios de comunicación y al mercado autorización en la medida necesaria para supervisar y monitorearnos y usar nuestros datos personales. Formalmente, en la democracia burocrática, los ciudadanos existen para la máquina, los medios y la organización; aquí se nos conceden ciertas libertades, donde hay razones para ello. La diferencia entre estas dos formas de democracia es substancial. El estándar de protección de datos, como espero demostrar posteriormente, constituye un indicador de la democracia: mientras más efectivamente protegemos nuestros datos personales, más cerca nos encontramos de la idea de democracia. Y, por otro lado, podemos preguntarnos si un Estado sin legislación sobre protección de datos es una democracia realmente.[4]

La *sociedad red* está añadiendo nuevas dimensiones a nuestras vidas. Trabajamos más y más con redes de información. El *e-government* está convirtiéndose en una central y visible forma de gobierno. Observamos el surgimiento de cyber-comunidades que trabajan virtualmente sobre redes de información. Y hablamos de *apertura* o *transparencia* como parte de la democracia. En una sociedad tal, quienes quizás han progresado más en Europa han sido precisamente los países nórdicos, en los cuales el procesamiento de datos personales en las redes de información es parte de la rutina diaria.

> Antes de salir con rumbo a Chile, hice algunas búsquedas usando Google por mi nombre, lo cual me retornó 334 documentos en los cuales él figuraba en una forma que el motor de búsqueda logró identificar. Esta figuración no ha sido muy alta y el

[3] El Profesor Konstari fue el primer finlandés que trabajó en la protección de los datos personales y, actualmente es Vice Director de la Agencia de Protección de Datos de Finlandia. La Agencia es una autoridad que se ocupa de las cuestiones que implican los principios de la protección de los datos y de ciertas materias referentes a derogaciones.

[4] Aquí nos encontramos en el límite del relativismo cultural. En el debate sobre los derechos humanos, el relativismo cultural se refiere a las clases de desviaciones aceptables respecto de los estándares de los derechos humanos que se permiten desde un punto de vista cultural. Vid. PERRY, *"The Idea of Human Rights"*, p. 57.

> número de aciertos registra pérdidas por las diferentes formas en que declina mi nombre en finlandés. Pero, aun así es bastante, si consideran que he procurado evitar la publicidad. Cuando realizo búsquedas sobre mi conocido colega y amigo noruego *Jon Bing*, quien ha estado más en la mirada pública, el resultado fue alrededor de 3600 documentos. Él está realmente en la red. Pero inclusive un ciudadano ordinario puede aparecer en ella. En mi ciudad natal, Rovaniemi, recientemente hemos tenido un caso donde un hospital local puso el nombre de una persona admitida por cuidados de salud mental en una red abierta. El hospital consideró que era su obligación poner los documentos que contenían tales decisiones en una red como ésta.

La tercera razón que he mencionado, asociada a los problemas sociales y legales relativos a la protección de los datos personales, fue la búsqueda de la *eficiencia*. Y este es un verdadero problema. Ahora, estamos entrando en la era de los sistemas documentales, pero sólo se trata de los primeros pasos. Una proporción significativa de la producción de documentos por las diferentes organizaciones es realizada electrónicamente, pero mediante convencional –diría "natural"– procesamiento de textos. En tal proceso, los datos personales han sido y continúan siendo datos tal y como cualquier otro. Extraer los datos del documento una vez concluido supone ciertas consideraciones financieras, y cuando los intereses de un individuo singular son pesados por contraposición a las finanzas públicas, es usual que el individuo sea quien pierda. Desdichadamente.

Ha sido y continúa siendo difícil obtener que las organizaciones que producen documentos en la sociedad de la información planifiquen desde un comienzo tal proceso respetando al ser humano y sus datos personales. En otras palabras, los datos personales deben ser tratados desde el principio como información que se procesa de una forma diferente. Esto es costoso, pero sus costes son menores que remover los datos personales incluidos en los documentos después de concluidos. Disponer del código correcto en el momento y lugar adecuados es una cosa increíblemente importante. Si esto es descuidado posteriormente, la protección de los datos personales llega a ser –o al menos esto sucede en Europa– una propuesta muy costosa.

Y el cuarto problema legal –y por sobre todo *legal*– que les he mencionado era el complejo curso vital de la información. El derecho en democracia es y debe ser una cuestión simple. De otra manera no podemos hablar de democracia, porque en ella *los ciudadanos deben conocer qué es el derecho*. Esta es una idea central del *Estado constitucional*. Los ciudadanos deben conocer la ley.

Pero, ¿cómo podemos legislar sobre el tratamiento de la información? La información no es estática. La regulación tradicional de los documentos en soporte de papel –por mencionar un ejemplo– es suficientemente clara al respecto. Hablamos de documentos públicos o documentos que deben mantenerse confidencialmente. Pero cuando comenzamos a hablar del curso vital de la información –cuán largo es el camino que la información puede tomar– nos encontramos con una situación fundamentalmente distinta. Esta es la razón por la cual la *Directiva Europea sobre Datos Personales*[5] se refiere al tratamiento de datos personales. Estos

[5] Directiva 95/46/CE del Parlamento Europeo y el Consejo de 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.

pueden tomar múltiples formas y su regulación es extremadamente dificultosa. La forma y ubicación de la información, así como el modo en que es procesada pueden cambiar totalmente con rapidez. El legislador debe ser capaz de regular un fenómeno dinámico. Y esto no es sencillo de lograr. La historia y el estado actual de la regulación de los datos personales en Europa nos suministra un ejemplo de ello.

De este modo, he esbozado el problema. A continuación, deseo proseguir con la revisión del desarrollo del marco legislativo de la protección de los datos personales en Europa y los inconvenientes relacionados con él. En lo que sigue, procuraré tener en cuenta los problemas básicos que les he descrito.

2. CINCO GENERACIONES DE PROTECCIÓN DE DATOS EN EUROPA

Hay muchas maneras de comenzar a contarles la historia de la protección legal de los datos personales –protección de datos–. Cuando hablamos de privacidad, algunos retroceden hasta Adán y Eva. Cubrir parte del cuerpo con una hoja de higuera era el primer paso en la preservación de nuestra privacidad respecto de otros. Hacia fines de los 70, nuestra privacidad, y frecuentemente nuestros datos personales también, eran protegidos en diferentes países aunque mediante una extensa variedad de disposiciones legales y prácticas normativas. Aún no se hablaba de "protección de datos" por entonces; no constituía una institución autónoma. En aquella época nadie hablaba de privacidad en Europa, pero le brindábamos protección a través de diversos medios.[6] Este largo, extremadamente extenso período puede ser calificado como la primera generación de protección de datos.

La segunda generación puede ubicarse entre 1960 y 1970. El signo de los tiempos consistía en que la protección de los datos personales era por primera vez vista como un objeto de regulación en sentido propio. En otras palabras, se transformó en una *institución legal*. El Estado de Hessen en Alemania y poco más tarde Suecia, quienes promulgaron leyes de aplicación en sus respectivos territorios, tienen el honor de ser los pioneros de la era de las leyes sobre protección de datos. Estas leyes generalmente son aludidas como la primera generación de leyes sobre protección de datos. Como leyes estas son las primeras en serlo, pero, como he sugerido, estábamos en una segunda generación de la protección de los datos. La Ley de Suecia de 1973 reflejaba el sentimiento de preocupación de la época sobre el uso de sistemas de información. ¡Debía ser obtenida una autorización de las autoridades para registrar datos personales que habían sido mantenidos usando tratamiento automatizado de datos!

Entre los años 1980 y 1990 tiene lugar lo que podríamos denominar el período de la tercera generación de protección de datos en Europa. La base del trabajo desarrollado durante tal período se encuentra en el Convenio sobre Datos Personales del Consejo de Europa, de

[6] En sólo unos años la privacidad se ha convertido en un término común en Europa, tanto en las ciencias del derecho como en la legislación. Con anterioridad, la expresión "vida privada" era usada, pero privacidad constituye un concepto más extenso. La vida privada y la protección de los datos personales son componentes de ella. Ésta es la manera como se han considerado estos elementos, por ejemplo, en la Ley sobre Protección de Datos de Finlandia. La Directiva Europea sobre Datos Personales también considera la privacidad un concepto elemental; la legislación sobre datos personales es usada precisamente para protegerle.

1980.[7] El Convenio buscaba generar una legislación relativamente uniforme en toda Europa. Algunos legislativos pudieron apreciar el sustrato y varios países de Europa adoptaron legislación sobre tales términos. La década estuvo marcada por el comienzo de la legislación. Y, de acuerdo con los objetivos centrales del Consejo de Europa, la protección de datos era ya considerada como un derecho fundamental.[8] La primera ley de datos personales de Finlandia –la Ley de Registros de Datos Personales aprobada en 1987– en gran parte adhirió al Convenio.[9]

Aunque en retrospectiva el Convenio del Consejo de Europa suministró una sólida fundamentación para la protección de los datos en Europa, la nueva generación se nos vino rápidamente encima. La principal razón de tal desarrollo fue que no todos los miembros del Consejo de Europa consideraron que el Convenio les obligaba. La uniformidad que se había pretendido no fue obtenida. Esto fue luego que la Unión Europea –UE–, la cual inicialmente se había contentado con lo realizado por el Consejo de Europa, hizo de la protección de los datos un foco de atención de sus esfuerzos legislativos. Formalmente, lo que incitó tal acción –que a primera vista parecía distante de la misión de la Comunidad– era la realización del libre movimiento de personas y bienes en la UE, lo que suponía el libre movimiento de los datos personales también.

El primer anteproyecto de la Directiva estaba completo en 1992. Sin embargo, el Parlamento Europeo rechazó la propuesta normativa y la regresó para enmiendas, con numerosos comentarios críticos. Sobre un ciento de comentarios fueron incorporados, un extenso número, dado que al final la Directiva hoy en día cuenta con sólo 34 artículos. La Directiva –la Directiva sobre tratamiento de datos personales– fue finalmente adoptada en octubre de 1995, señalando el comienzo de la cuarta generación de protección de datos en Europa. La UE se había convertido en el impulsor de la protección de datos, obligando a sus Estados miembros a implementar la Directiva y conduciendo a terceros países a adoptar los mismos principios, primordialmente con el fin de promover el comercio electrónico.

La Directiva ha debido ser *implementada* en todos los Estados miembros dentro de los tres años siguientes a su adopción, esto es, en octubre de 1998. Ello no sucedió. Incluso en Finlandia nos hemos demorado medio año más, aun cuando Finlandia se ha ganado la reputación de cumplir escrupulosamente con las fechas estipuladas. En los hechos, la Comisión inició procesos ante la Corte Europea de Justicia contra cinco países –entre estos Francia y Alemania– debido a su retraso en la transposición de la Directiva. En este momento, virtualmente todos los Estados miembros han implementado la Directiva, cuando menos la mayor

[7] Convenio de 28 de enero de 1981, del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos personales.

[8] Artículo 1. Objeto y fin.

El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física, sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos").

[9] En aquel entonces Finlandia no era miembro del Consejo de Europa ni parte de su Convención de Derechos Humanos. Esta fue la razón de por qué la importancia de la Convención no fue enfatizada cuando la legislación era aún un proyecto. Sin embargo, tal instrumento y la legislación sueca sirvieron de modelos para nuestra Ley de Registro de Datos Personales.

parte. El país más reciente en cumplir con ello ha sido Irlanda, cuya nueva legislación entró en vigencia a comienzos de julio del año en curso. Sólo un país aún no ha cumplido con la transposición de la Directiva, este es Francia.

Es difícil encontrar razones consistentes para explicar por qué la transposición ha tenido lugar a diferentes tiempos en los distintos países. Italia ha sido el primer Estado en completar la implementación, precisamente porque estaba iniciando la transición para disponer de una ley de protección de datos. No había necesidad de derogar o modificar la legislación preexistente. En Finlandia, el trabajo tomó más tiempo del esperado, porque deseábamos enmendar la primera ley sobre protección de datos y, a la vez, reformar la legislación sobre el derecho público de acceso a documentación.[10] Había, por lo tanto, mucho más que abordar que la sola implementación de la Directiva.

A pesar de las varias razones para el retraso en los distintos países, me atrevo a considerar que él parece explicarse por varias razones. Entre ellas, (1) el explosivo incremento en el uso de las redes de información abierta, (2) la lenta realización que el impacto de la Directiva había de tener en el procesamiento de datos cotidiano, y (3) las dificultades para encontrar una técnica legislativa apropiada. Actualmente, en Finlandia hemos invertido numerosos meses simplemente ponderando cómo debíamos redactar la legislación.

Ahora que la implementación de la Directiva está esencialmente completa, a lo menos en sus aspectos formales, uno podría pensar que disponemos de un período relativamente tranquilo en el cual la protección de los datos personales se encuentra asentada. Sin embargo, todavía no es el caso. Nuevamente estamos entrando o nos estamos dirigiendo hacia una nueva etapa. Con el riesgo de exagerar la nota, me referiría a ésta como la etapa de la *fragmentación de la protección de los datos*. Aquello que la Directiva ha logrado con algún esfuerzo –una concepción compartida de los principios de la protección de los datos personales– está en riesgo. La dificultad de la protección de los datos en las esferas social y legal supone, una vez más, estar alertas.[11]

Otra vez, el desarrollo no es resultado de un solo factor; un cierto número de impactos simultáneos pueden ser identificados como tales. La principal razón de ello nos es tan cercana que impide siquiera visualizarla. Se trata del incremento en la cantidad de legislación especial que regula la protección de los datos personales y de leyes con disposiciones relativas a la materia. Este es el resultado natural de la propia Directiva. Es difícil controlar la regulación en el alcance requerido con tan solo una ley de carácter general. Necesitamos legislación especial y necesitamos disposiciones adicionales especiales. Sin embargo, debido a la naturaleza de tal regulación, tales instrumentos frecuentemente son influenciados por criterios disímiles y, de

[10] La nueva Ley sobre Transparencia de las Actividades Gubernamentales entró en vigencia a fines de 1999, algo después de la Ley de Datos Personales. La Ley de Transparencia reguló sobre todo la publicidad y el secreto de documentos en posesión de las autoridades.

[11] Sin embargo, debe indicarse que la mayor parte de la cuestión ya ha sido regulada, aunque la armonización mediante la Directiva casi inevitablemente acarreó desarmonías. Diversos países desean enmendar su legislación anterior en base a sus experiencias. Esto es posible porque las Directivas no especifican cómo las reformas deben ser realizadas. Así en la transposición de la Directiva, las leyes sobre datos personales de los países nórdicos actualmente terminan diferenciándose más de lo que ellas habían. Las características principales de esta legislación se describen en BLUME (ed). *"Nordic Data Protección"*.

tal modo, otras leyes pueden prescindir de los fundamentos de la legislación aplicable a los datos personales. Ello puede generar graves consecuencias. Las interpretaciones de tales disposiciones no se encuentran necesariamente en línea con las aspiraciones de la Directiva.

Un segundo grupo de razones que pueden ser citadas para debilitar la protección de los datos está en algunas modalidades más tradicionales de los mismos. Ellos se relacionan con el control y la vigilancia. Los esfuerzos realizados para usar sistemas de información tan detallados como sea posible en nombre de la eficiencia administrativa, el orden y seguridad públicas, y los datos personales se han transformado en una herramienta esencial para la identificación y fines de control. Tales objetivos son fácilmente vendidos al legislador, pero la importancia de la protección de los datos personales como un medio de proteger al individuo y su privacidad es fácilmente ignorada en el proceso. Y, con todo, en el preámbulo de la Directiva de Datos Personales –consideración 34– el costo rendimiento es mencionado sólo como un factor que en ciertos casos autoriza a los Estados miembros, justificado por fundamentos de interés público relevante, para fijar excepciones a la prohibición relativa al procesamiento de la categoría de datos sensibles, cuando razones de interés público lo justifican en áreas tales como salud pública y protección social.

Un imprevisto, una sorprendente amenaza para la protección de los datos personales se materializa el 11 de septiembre del 2001. Los sucesos de tal día en Nueva York se han reflejado como restricciones a nuestras libertades, una consecuencia será que nos encontraremos retornando a la sociedad desnuda *(naked society),* donde las autoridades recopilan una ascendente cantidad de datos sobre nosotros, nacional e internacionalmente. Paradójicamente, sin embargo, tales acciones incrementan los riesgos de una eficaz y destructiva información de guerra. La proliferación de registros de datos personales y las telecomunicaciones asociadas a ellos ofrece la impresión –deseable– de constituir objetivos en tal conflicto. Esto es como si no hubiésemos aprendido nada de la Segunda Guerra Mundial, la cual tuvo un impacto importante sobre el desarrollo de la protección de los datos en relación directa con los derechos humanos. Del mismo modo, nos parece haber olvidado la advertencia formulada por la Corte Europea de Derechos Humanos unos pocos años atrás, sobre los peligros de restringir las libertades ciudadanas bajo la desproporcionada invocación de consideraciones de seguridad.[12] La configuración de la democracia en Europa parece estar cambiando.

No necesitamos exagerar los problemas asociados a la quinta generación de leyes sobre protección de datos, sin embargo. Ellos deben ser reconocidos, pero, al mismo tiempo, hemos admitido que, por un tiempo, al menos, el positivo impacto de la Directiva Europea de Datos Personales es manifiesto. La protección de los datos personales mediante la legislación se ha transformado en ***una institución legal permanente.*** La relación del individuo con la sociedad y otras organizaciones se enmarca en un ambiente de operaciones que incluye el derecho a la protección de los datos. Y este derecho es un ***derecho fundamental.*** Y como tal es comprendido por la Directiva; éste ha sido descrito como tal en la Carta de Derechos Fundamentales de la Unión Europea; y ha sido expresamente consagrado como tal en la Constitución Finlandesa, por

[12] En su pronunciamiento del 6 septiembre de 1978, Series A no. 28, en el caso *Klass and Others v. Germany*, la Corte Europea de Derechos Humanos decidió que los Estados no deben, "en el nombre de la lucha contra el espionaje y el terrorismo, adoptar cualquier medida que estimen apropiada."

ejemplo.[13] En el transcurso de la cuarta generación, la protección de los datos personales en Europa perfeccionó el punto tocante al estatus de un derecho fundamental. Sería muy difícil para la quinta generación negar tal desarrollo aunque nuestros logros pueden verse afectados.

En mayo del 2003 se ha publicado el Primer Informe de la Comisión Europea sobre la transposición de la Directiva de Datos Personales.[14] En conjunto con su evaluación, la Comisión recogió informes de países individuales sobre los problemas que habían sido detectados. Sus resultados son tranquilizadores. Los mayores problemas no estaban asociados con la Directiva misma.

Por otro lado, la Comisión nos recuerda que, debido a la lenta transposición, es prematuro sugerir cualquier enmienda que pudiera ser necesaria. Así, las primeras enmiendas pueden esperar hasta 2005 cuando menos. No obstante, cierto número de directivas especiales han sido adoptadas al mismo tiempo, lo cual ilustra que inclusive a nivel de directivas nos estamos moviendo hacia una normativa especial.[15] La protección de los datos personales es difícil de obtener con una directiva singular. Esta permanece para ser vista mediante los principios establecidos en la Directiva de Datos Personales que serán retenidos en las directivas especiales. El Informe de la Comisión no hace mención a modificación alguna, ni a la necesidad de ella. Así es como debe ser, los principios centrales de la Directiva Europea sobre Datos Personales gozan de buena salud.

2.1. Comprendiendo la Protección de Datos

Uno de los problemas más visibles de la protección de los datos ha sido –y continúa siéndolo– el desarrollo e identificación de los principios legales que informan la protección de los datos personales. Desde que la información cambia de formas muchas veces durante su curso vital, la ley sobre protección de datos debe necesariamente permanecer en un nivel comparativamente abstracto. No podemos adoptar decisiones con directa referencia a otras leyes; enfatizo, las leyes deben ser genuinamente interpretadas. Esta es una paradoja por lo que concierne al rol social de la legislación sobre protección de datos. La protección de datos es un derecho que se aplica a todos nosotros en el día a día. A partir de aquí, la legislación debería ser tan informativa como fuere posible e inteligible de buena gana, pero esto no puede ser dada su naturaleza necesariamente abstracta.

Tengo en mente cuatro diferentes soluciones para este problema: la información suministrada al público por las autoridades de protección de datos, los códigos de conducta, los principios legales de la protección de datos y leyes especiales para contextos específicos. Unas breves palabras sobre cada uno de ellos parecen necesarias.

[13] Sección 10 de la Constitución de Finlandia. El derecho a la privacidad: Todos tienen vida privada, honor e inviolabilidad del hogar garantizada. Serán materia de ley las provisiones que detallen la protección de los datos personales.

[14] Com (2003) 265(01) Comisión de las Comunidades Europeas, *"Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46/CE)"*, Bruselas, 15 de mayo de 2003.

[15] La más significativa de tales directivas es la Directiva 2002/58/CE del Parlamento Europeo y el Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad de las comunicaciones electrónicas).

La legislación de protección de datos es institucional, en el sentido que, desde la primera ley de datos de Suecia, las autoridades de protección de datos han supervisado y conducido la protección de los datos personales. Esta constituye también una exigencia de la Directiva Europea, donde la cuidadosa elaboración y difusión de las orientaciones emitidas por las autoridades forman una importante parte de la información sobre protección de datos suministrados al público. Desafortunadamente, la disponibilidad de recursos ha sido insuficiente –cuando menos en los países europeos– y hay pocos países cuyas autoridades mantienen al público informado tan activamente como hace la Inspección de Protección de Datos de Suecia, por ejemplo.

Una manera muy interesante de hacer comprensible la legislación sobre datos personales, que además complementa las instrucciones decretadas por las autoridades, es la adopción de códigos de conducta. Un artículo específico sobre los códigos de conducta fue incluido en la Directiva sobre Datos Personales, en gran medida a partir de los ejemplos suministrados por Noruega e Irlanda en la materia. Los códigos de conducta pueden ser redactados por los actores relevantes en distintos contextos y pueden ser revisados por las autoridades de protección de datos. Es esencial tener en mente que los códigos de conducta no son instrucciones oficiales, sino que la concepción del estado de las cosas en un contexto específico tal como es apreciada por los actores de tal sector y que es legalmente aceptable. Esto hace que los códigos incidan en el campo de aplicación de nuestras leyes.

He descrito los códigos de conducta como una manera de leer la ley y hacerla inteligible. Los códigos dan a conocer qué es importante en cualquier contexto en que se verifique el procesamiento de datos en cuestión. Los códigos de conducta han sido escasamente usados en Europa como instrumentos legislativos, y la actitud hacia ellos ha sido incluso algo escéptica. En mi concepto, ellos constituyen, en una perspectiva amplia, un importante medio para comunicar la ley en una sociedad como la nuestra en que progresivamente lo jurídico cobra mayor presencia.

Sin embargo, los códigos de conducta no deben ser simplemente una casuística descripción de procedimientos que no tengan en cuenta el porqué uno debe proceder en un modo particular. Ellos deberían ser formulados incluyendo puentes entre el texto de la ley y descripciones de cómo actuar. Tales puentes son provistos por los principios aplicables a la protección de datos. Nosotros usamos los principios para dirigir y, antes de todo, identificar los problemas directamente relacionados con ellos. Sin tales principios, la protección de los datos fácilmente se quedaría en una simple consideración técnica, que se apreciaría como una interrupción a nuestra vida diaria.

Sí, principios. Ellos requerirían una o dos presentaciones adicionales para examinar los aspectos esenciales de los mismos en relación con la protección de datos en Europa con algún detalle. Con casos humanos tan diversos como ellos, hemos encontrado cierto número de diferentes tipos de principios. He dividido estos en tres categorías: aquellos que se aplican a todos; aquellos que se aplican principalmente al responsable de tratamiento; y aquellos aplicables a los derechos individuales. Una disgregación tal como ésta en ellos nos llevará a percatarnos del gran número de principios esenciales. En mi análisis, los principios relevantes están insertos en la presentación.

Me interesa ocuparme de dos de tales principios en particular; estos son el principio de derecho fundamental y el principio del consentimiento.

La protección de los datos personales en Europa es un derecho fundamental. He descrito este como un derecho fundamental cotidiano. Como un derecho fundamental, la protección de los datos personales debe comenzar en la ley, no en un nivel normativo inferior, tal como decretos u órdenes administrativas. Aun más importante, el punto de partida para la interpretación de la ley es precisamente la protección de un derecho fundamental o, en rigor, en general, los derechos fundamentales.

El principio del consentimiento por su parte conecta la protección de los datos personales con nuestro derecho a la autodeterminación. En el sentido de tal derecho, nuestros datos personales son parte de la información que está primordialmente bajo nuestro control. En expresiones estadounidenses, podemos decir que tenemos información que nos concierne. Aun cuando, como ciudadanos, nosotros obtenemos un número de identidad personal, retenemos el poder para decidir como él es usado. Esto es central, ya que la Directiva Europea sobre Datos Personales procede desde la premisa que nuestros datos personales pueden ser tratados sólo con nuestra autorización. Excepciones a esto deben, por regla general, ser dispuestas en la ley. Esta es precisamente la intervención revolucionaria que representa la Directiva, al realzar nuestro derecho a la autodeterminación. Por ejemplo, la primera Ley de Protección de Datos de Finlandia disponía que al responsable del registro le estaba esencialmente permitido procesar datos personales, sin considerar necesario requerir nuestra autorización.

En lugar de, o a veces en adición a, las orientaciones, los códigos de conducta y los principios, la protección de los datos puede ser hecha más comprensible mediante legislación especial. En tales casos, el propósito es generalmente dirigir cierto grupo de materias o contextos especiales mejor y en un modo más concreto. La protección de los datos en las telecomunicaciones es un buen ejemplo de ello. La preocupación por la protección de los datos ya ha incitado una regulación especial al nivel de directiva. Sin embargo, esta aproximación involucra ciertas desventajas. Primero, como he mencionado al comienzo, la legislación especial puede ser promulgada en una variedad de modalidades y ser objeto de la influencia de varios intereses en mayor medida que la apropiada legislación sobre protección de datos personales. En realidad, en Finlandia, por ejemplo, el Ministerio de Justicia es responsable de la legislación sobre protección de datos en general, y el Ministerio de Transporte y Comunicaciones lo es de la protección de datos en las telecomunicaciones. Los dos ministerios trabajan de manera bastante distinta. Una segunda desventaja de la legislación especial es que la legislación sobre protección de datos puede formar parte de otra legislación, la cual disminuye su relación con la legislación general y la significancia de los principios generales de la ley puede ser descuidada. Los decretos especiales también están de acuerdo con una cultura de aplicación diferente. Y este puede vincularse a distintos tipos de supervisión dependiendo de si otras autoridades de control llegan a involucrarse conjuntamente o en lugar de las autoridades de protección de datos.

Espero no les importe que enfatice una vez más la premisa más simple subyacente en la protección de datos, como sostengo ha de comprenderse: la protección de los datos personales es para la gente. Al final, esto deriva desde las consideraciones de los derechos humanos. Si este hecho no es claramente apreciado, tal como lo hemos investigado, enseñado y aplicado, podemos terminar –como ha sido por lo demás frecuentemente el caso– pensando que la protección de datos es un fenómeno negativo que nos complica nuestra vida diaria. Nada puede estar más lejano de la verdad. Como frecuentemente sostiene el Ombudsman de Protección de Datos de Finlandia, *Reijo Aarnio,* la protección de datos es un asunto afortunado.

Pero como un problema regulatorio, la protección de los datos es un asunto verdaderamente muy complicado, que sucede en el largo y complejo camino que la información toma; justo cuando creemos haber cogido el problema a ser regulado, éste nos es arrebatado de nuestro alcance, como la fruta de Tantalus, lo cual se explica por el desarrollo tecnológico, el uso de redes de información, la transformación digital o alguna otra razón.[16] Por otra parte, la relación entre privacidad y publicidad en la sociedad está constantemente en cambio. Ella se dirige en diferentes modos, en diferentes épocas. A modo de conclusión, examinaré brevemente algunas de las cuestiones más difíciles que hoy enfrenta el desarrollo de la protección de los datos en Europa.

2.2. Problemas actuales de la regulación legal

La Directiva Europea de Datos Personales contempla diversas modalidades mediante las cuales supervisar la implementación del instrumento y los límites de tiempo establecidos en el mismo. El principal elemento a considerar es el conocido Grupo de Trabajo del Artículo 29, un cuerpo compuesto de representantes de las autoridades de protección de datos. El Grupo de Trabajo emite opiniones y recomendaciones sobre los problemas que advierte en la aplicación de la Directiva. El Grupo de Trabajo ha aprobado 79 opiniones, en las cuales se ha extendido desde la relación con los medios de comunicación y la protección de los datos a la protección de ellos en la vida laboral e incluye, por ejemplo, una posición respecto de si era posible transferir datos personales a la Argentina. Todas las consideraciones que siguen también han surgido en el Grupo de Trabajo. Sin embargo, no revisaré sus posiciones en detalle, algunas de las cuales son tentativas en este punto, pero, antes bien, echaré un vistazo a cuatro asuntos en término de los principios implicados. La privacidad en el lugar de trabajo, la regulación de la videovigilancia, los propósitos periodísticos en el empleo de redes de información abiertas, y el estado de la protección de los datos en el desarrollo de *e-government.* Todos son actualmente temas de cuestionamiento.

El 2001, en Finlandia entró en vigencia una ley sobre protección de la privacidad en los lugares de trabajo. Es el primer país en Europa en hacer tal. La ley brinda protección a los datos personales en el contexto de una relación laboral, pero, como su nombre lo significa, es más que ello. Previamente, la ley general de protección de datos fue naturalmente aplicada en los lugares de trabajo y ella contenía algún número de disposiciones especiales relativas al tema. Sin embargo, el Ministro del Trabajo y las organizaciones laborales deseaban una ley especial que regulara ciertos aspectos de la privacidad de los trabajadores además del tratamiento de datos personales. Particular preocupación existía respecto de varias pruebas. La ley prohíbe las pruebas genéticas y permite los tests psicológicos si ellos satisfacen apropiados estándares de calidad. Sin embargo, la

[16] En la mitología griega, Tantalus, rey de Phrygia, es condenado a permanecer en el Hades, con el agua hasta el nivel de su mentón alzado y bajo ramas cargadas de frutas, pero siendo incapaz de beber o comer de ellas, pues tanto el agua como los frutos retrocedían a su alcance al intentar hacerse de ellas (N. de T.).

ley no especifica tales criterios. Una importante y nueva solución organizacional en la ley, cual es que la protección de los datos en la vida laboral es supervisada, a la vez, por las autoridades de protección de datos y las de salud laboral. Como Finlandia no cuenta con autoridades de protección de datos locales, la inclusión de las autoridades de salud laboral representa una imagen de supervisión por las autoridades "entre la gente" a nivel local.

El ejemplo de Finlandia ha incitado a otros países –Suecia, por ejemplo– para comenzar proyectos con el propósito de crear la legislación correspondiente. Semejantemente, a nivel de la Unión Europea se está considerando la necesidad de una Directiva especial al respecto.

Adicionalmente a los tests de empleados, el asunto más delicado de la protección de datos se encuentra en su práctica en los lugares de trabajo, se trata de cómo proteger adecuadamente el correo electrónico de los empleados. La situación actual es clara. El correo electrónico de un trabajador queda amparado por la protección de la confidencialidad de las comunicaciones. El secreto de las comunicaciones electrónicas es análogo al de otra correspondencia. El empleador no tiene derecho a abrir un e-mail del trabajador, a menos que la dirección haya sido puesta a su disposición para su uso por un cierto número de trabajadores y hubiere sido definido de otra manera que como cuenta de correo personal. En la práctica, la protección de la confidencialidad de las comunicaciones electrónicas es habitualmente violada. El grupo que actualmente trabaja en la reforma de la Ley de Privacidad ha propuesto que a los empleadores se les confiera un derecho limitado para abrir los correos electrónicos de los trabajadores cuando ello resulte esencial para la ejecución del trabajo en relación con sus responsabilidades. Esta propuesta ya ha generado reparos en los foros públicos.

La videovigilancia también ha generado enormes disputas. La Ley de Privacidad en los lugares de trabajo la permite, pero los trabajadores están conscientes de que ella y su empleo debe ser abordado en las negociaciones entre empleadores y trabajadores. En la práctica, este proceder no siempre ha sido seguido y en algunos casos los empleadores han sido multados por el uso clandestino de videovigilancia.

Sin embargo, la *videovigilancia* es también un asunto más general. La Directiva de Datos Personales no se refiere al tema con detalles, pero todos los Estados miembros consideran que la videovigilancia está entre los asuntos cubiertos por la Directiva. La imagen de una persona y su voz son datos personales –porque él o ella pueden ser identificados–, por lo tanto, las leyes sobre protección de datos pueden ser aplicadas a la videovigilancia. Sin embargo, desde que la vigilancia toma lugar como una medida significativa para mantener el orden público y la seguridad, algunos países –tal como Dinamarca y Suecia– han preparado leyes especiales sobre videovigilancia. Finlandia está a la espera de los resultados por ahora. En Finlandia, el asunto es visto en los términos de la Ley de Datos Personales y de la prohibición en el Código Criminal contra la fotografía clandestina. Por ejemplo, la videovigilancia en los probadores de tiendas, que eran frecuentes con anterioridad, están hoy prohibidos por el Código Penal como vistas ilícitas. Cuando estamos en un probador, el espacio es parte de nuestra privacidad hasta en tanto permanezcamos allí.

Una tensión existe entre la protección de datos y los medios de comunicación; ello es inevitable. En Europa, especialmente en los países Nórdicos, los medios disponen de un particularmente extenso derecho para procesar información oficial. Así, el alcance de la Ley de

Protección de Datos de Finlandia ha sido limitado a fin de que las excepciones de la ley no sean aplicables, de modo general, a los medios de comunicación. Recordemos que los objetivos de la ley se aplican en principio a los medios de comunicación también, pero esto es hasta donde se ha ido. Entre las disposiciones individuales de la ley, está el amplio derecho de las autoridades de protección de datos para inspeccionar los archivos de los medios de comunicación relacionados con la protección de los mismos a efectos de cerciorarse si son apropiadamente protegidos. Los derechos de los medios están contemplados en la Ley sobre Transparencia de las Actividades Gubernamentales, la cual distingue entre información de dominio público e información secreta. El Código Penal prohíbe la publicación de información relativa a la vida privada de una persona sin su consentimiento, a menos que tal persona sea conocida como un personaje público que tiene un perfil público. A pesar de sus amplias libertades, los medios de comunicación constantemente abogan por ensanchar sus derechos de acceso a información, invocando la función de vigilancia de lo que ellos mismos denominan *el cuarto poder del Estado*.

La relación entre los medios y la protección de datos ha empezado a destacar en conexión con el uso de redes abiertas de información. En último término, esto representa una pregunta en torno a si las acciones de trabajo de un ciudadano privado en una red satisfacen los criterios de finalidad periodística. Si es así, él o ella puede ser comparado con un miembro de los medios de comunicación. Estas son las bases sobre las cuales un caso fue decidido en Suecia. La Corte Europea de Justicia, por su parte, decidió que tal asunto no estaba dentro de su jurisdicción.

Finlandia pronto dispondrá de una nueva ley sobre libertad de la prensa y medios de comunicación. La ley asimila una persona que mantiene una página web parcialmente con un miembro de tales medios, lo que significa que la persona dispone de protección de sus fuentes, o el derecho a no revelar su fuente de información. Sin embargo, la prohibición en el Código Penal finlandés que penaliza la publicación de detalles sobre la vida privada de una persona también resulta aplicable a quien mantiene una página web.

La cuarta cuestión sensible desde la perspectiva europea corresponde al desarrollo del gobierno electrónico. Como parte del devenir de la sociedad de la información estamos experimentando una rápida transición hacia el *e-Government*. Este es un objetivo que ha sido también puesto en común en la Unión Europea. El 2005, los Estados miembros de la UE deben tener funcionando adecuadamente, servicios orientados hacia el gobierno electrónico que sus ciudadanos puedan utilizar a través de un eficiente y razonable precio de conexión. El plan llamado a desarrollar servicios de salud electrónicos cursa estas mismas líneas.

La transición hacia el gobierno electrónico requiere de un extenso trabajo de cimientos con respecto a redes de información y legislación. Finlandia se ha encaminado a ser un líder en este sector también. De hecho, nosotros disponemos de una Ley sobre Servicio Electrónico en el Gobierno, la que se aplica a todas las comunicaciones electrónicas con la excepción de los llamados de voz. El objetivo de la ley es que todas las autoridades lleguen a disponer de sistemas de información oportunamente en funciones y ofrecer fácil acceso mediante los softwares apropiados. Adicionalmente, una autoridad debería siempre acusar a la brevedad recibo de todos los mensajes recibidos y responderlos en un tiempo razonable. Ello crearía una infraestructura en el sector público con la cual podría hacer posible las comunicaciones por las autoridades y servicios de gobierno electrónico.

A pesar de ello, la transición hacia el gobierno electrónico está lejos de constituir un asunto sin problemas. Un problema práctico y financiero por supuesto es el relativo a la cobertura de las redes de información. Pero no entraré en tal materia. El asunto más complejo surge cuando uno comienza a pensar sobre las implicancias de la protección y seguridad de los datos.

Cuando emprendemos la instalación del gobierno electrónico vía redes de información abiertas, nos encontramos cara a cara con la circunstancia de que la Internet es esencialmente una autopista de la información que carece de seguridad para los datos. Esta seguridad debe ser suministrada como objetivo del gobierno. Si es el ciudadano que usa los servicios quien termina asumiendo el pago por ellos, estamos bastante lejanos de los principios del buen gobierno.

El meollo del asunto lo enfrentamos cuando en retrospectiva observamos cómo en tales situaciones la identificación de los ciudadanos tiene lugar con motivo del empleo del gobierno electrónico. Los europeos que piensan sobre los derechos humanos y fundamentales sugerirían que, en primer lugar, debemos usar los servicios del gobierno anónimamente. Nosotros deberíamos proporcionar nuestros datos personales sólo cuando ellos son necesarios para la obtención de algún beneficio, o bien para liberarnos de alguna responsabilidad. La misma naturaleza del gobierno electrónico pone en riesgo el anonimato. Y, más interesante aún, en Europa el desarrollo del gobierno electrónico ha general y ampliamente procedido desde la premisa de que la firma digital será la principal solución técnica. Aunque nadie desea abandonar el refugio del anonimato en el sistema, o bien nadie se percata de su importancia.

3. CONCLUSIÓN

En numerosas ocasiones he puesto de relieve un rasgo especial de la legislación sobre protección de datos finlandesa, el concepto de buenas prácticas de procesamiento de información. Buenas prácticas de procesamiento de información es también uno de los objetivos centrales de la Ley. Nos esforzamos por llegar a una situación en la cual el procesamiento de datos personales tiene lugar en armonía con buenas prácticas de procesamiento y sin la intervención de los tribunales, del Ombudsman de Protección de Datos o del legislador.

Desde una perspectiva legal, una apropiada información sobre las prácticas de procesamiento es una forma de optimizar las disposiciones normativas. Ellas obligan a quienes procesan datos personales a dar debida consideración a los objetivos de la ley cuando realizan tratamiento de datos personales. En los hechos, la Ley de Datos Personales de Finlandia conecta el deber de cuidado y las buenas prácticas de procesamiento. La Sección 5 de la Ley reza como sigue:

> **Sección 5 — *Deber de cuidado***
>
> El responsable de tratamiento procesará datos personales legal y cuidadosamente, de conformidad con las buenas prácticas de procesamiento, y también de modo que la protección de la vida privada del titular de los datos y los otros derechos fundamentales salvaguardados por su derecho a la privacidad no sean restringidos sin fundamento en una disposición legal. Cualquier persona que opere en representación del responsable de tratamiento, en la forma de un comercio o negocio independiente, está sujeta al mismo deber de cuidado.

A primera vista, las buenas prácticas de procesamiento pueden parecer una herramienta modesta y poco eficiente. A pesar de ello, las buenas prácticas constituyen una idea básica de la ética de nuestra sociedad. Es también un medio para entender el derecho y alentar interpretaciones en favor del individuo. Por esta razón cuando la ley era aún un proyecto estábamos totalmente unánimes en cuanto a que las buenas prácticas de procesamiento merecían un lugar en la nueva Ley de Registros de Datos Personales también.[17] Esta es una atractiva ayuda para la lectura de la ley. Las buenas prácticas de procesamiento y los códigos de conducta conjuntamente constituyen una contribución significativa para ser capaces de comprender la legislación sobre protección de datos personales más allá de las disposiciones legales individuales. Ellas nos ayudan a visualizar el rostro positivo de la protección de los datos.

Pero, en último término, la protección de los datos personales implica asuntos más anchos e importantes. En su libro sobre filosofía de la tecnología, recientemente publicado, el filósofo finlandés *Timo Airaksinen* adopta una extremadamente pesimista perspectiva del cambio social. Él escribe:

> Uno puede por supuesto hablar sobre democracia y justicia, pero la fuerza obligatoria de ellas es esencialmente una ficción, porque la fuerza que mantiene a la Sociedad intacta opera sobre diferentes principios de la ética individual. La Sociedad y el Estado no son elementos grandes y complejos, pero las agrupaciones de personas son quienes mantienen al mismo tiempo los propósitos estables sobre los cuales las instituciones trabajan. Siempre ha sido difícil describir y explicar cómo sucede esto, pero el vínculo es fuerte y las instituciones resisten los cambios efectivamente, no importando cuán insanas puedan ser sus actividades.[18]

Airaksinen es quizás demasiado pesimista, pero indudablemente él se encuentra en lo cierto. Uno de los grandes desafíos a enfrentar por las disciplinas del derecho en Europa en los próximos años es la ampliación a todos los campos de una educación jurídica que enfatice sobre los derechos fundamentales.[19] En el Estado constitucional moderno, la ley pertenece a cada uno y abandonar la formación jurídica a las Universidades, a las Facultades de Derecho, significará extensos forados en el conocimiento de la ley. La protección de los datos personales es uno de los asuntos más claros al respecto. Un conocimiento de la materia como un derecho cotidiano debe ser efectivamente comunicado a todos quienes procesan datos personales y planean tal procesamiento. Esta será una gran empresa por cierto, especialmente con la transición hacia el gobierno electrónico. Y habrá siempre los que, en oposición a la protección de los datos personales, demuestran su ignorancia sobre los derechos del individuo en el Estado constitucional.

---

17 En la anterior Ley de Registros de Datos Personales el concepto estaba referido a buenas prácticas registrales. La idea viene originalmente de la legislación sueca. Esta también ha sido adoptada en la Ley sobre Transparencia de las Actividades Gubernamentales, donde se las refiere como *"buenas prácticas de administración de la información"*.

18 AIRAKISNEN, *"Tekniikan suuret kokemkset. Filosofinen raportti"* [La gran experiencia de la tecnología. Un informe filosófico (en finlandés)]

19 Me he ocupado de este asunto con profundidad en mi artículo "E-government – Good Government. An impossible equation.", en GALINDO/TRAUNMÜLLER (ed), *"e-Government: Legal, Technical and Pedagogical Aspects"* (2003), Publicaciones del Seminario de Informática y Derecho, Universidad de Zaragoza.