Estrategias de protección de datos en el comercio electrónico

A. Daniel Oliver Lalana*

Sumario: 1. Introducción – 2. Código, tratamiento invisible y perfilación en línea – 3. Estrategias tecnológicas de protección de datos – Estrategias regulativas de protección de datos – 5. ¿Qué queda del derecho fundamental a la protección de datos? – 6. El modelo de sociedad de la información.

1. Introducción

Puede decirse que dos hipótesis elementales vertebran el modo de concebir la relación entre el desarrollo del comercio electrónico (*B2c*) y el régimen jurídico de la protección de datos. De una parte, suele considerarse que la legislación de protección de datos supone un obstáculo para la expansión tecnológica y comercial y, por tanto, para el comercio electrónico. De otra, el derecho a la protección de datos es percibido como un simple derecho de los consumidores, quienes podrían negociar sobre él con libertad –por algo son consumidores *soberanos*–. Estas dos ideas se entrecruzan en la práctica, ya que la mejor forma de eliminar los obstáculos que impone la legislación parece ser conseguir que los ciudadanos legitimen con su consentimiento las prácticas empresariales de tratamiento de datos personales. Creo que ambas ideas son muy conflictivas, y que uno de los retos capitales que afrontamos hoy es justamente explicar qué factores pueden determinar la sustitución de una concepción de la protección de datos como *obstáculo comercial* y como un simple *asunto del consumidor*, por una concepción de la protección de datos como *ventaja comparativa en el mercado* y como derecho fundamental del *ciudadano*.

Anticipo ya que tengo serias dudas acerca de que este doble cambio de concepción se imponga en un futuro inmediato. Pero lo cierto es que hace tiempo que se intenta alcanzar un determinado equilibrio entre los legítimos intereses de las compañías electrónicas y las exigencias derivadas de un modelo fuerte o tuitivo de legislación como el diseñado por la Directiva 95/46/CE. Antes de discutir si –y en su caso, en qué medida– puede alcanzarse este equilibrio, conviene fijar los términos o las dimensiones del conflicto.

Apenas reconocido como un derecho fundamental de la persona, el derecho europeo de protección de datos encuentra en el entorno virtual un panorama desolador. Primero, el grado de cumplimiento de la legislación, hasta hace poco tiempo, es todavía relativamente bajo en Internet; segundo, gran parte de los agentes que operan en Internet y de los servidores a los que nos conectamos se ubican en países en los que no existe legislación de protección de datos en sentido estricto (señaladamente en Estados Unidos y en Asia);¹ y tercero, el propio diseño

* Profesor asociado de la Universidad de Zaragoza [www.unizar.es/fyd/prodatos]. Todas las páginas web citadas en este trabajo fueron verificadas por última vez el 31 de agosto de 2003. Los documentos del Grupo de Trabajo sobre Protección de datos de la Comisión Europea (en adelante, Working Party), se obtienen en http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs.

¹ Véase D. Banisar, y S. Davies, «Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection and Surveillance Laws and Developments», *The John Marshall Journal of Computer & Information Law*, vol. XVIII No. 1 (1999), pp. 1-111; y A. Téllez Aguilera, *La*

de Internet facilita el acopio y proceso indiscriminado de información personal. Estos tres problemas, por demás solapados entre sí, conforman los ejes del programa de investigación en materia de protección de datos y comercio electrónico. ¿Cómo hacer que las empresas electrónicas europeas cumplan la legislación? ¿Cómo proteger a los consumidores europeos en un entorno sin fronteras? ¿Y cómo minimizar los riesgos que la propia infraestructura tecnológica comporta para la protección de datos personales? Comenzaré con esta última cuestión [2], para presentar luego las estrategias tecnológicas [3] y regulativas [4] que pueden seguirse para derribar la primera de las ideas o hipótesis mencionadas. Así, en este trabajo sostendré que resulta posible armonizar los intereses del comercio electrónico con un nivel aceptable de protección de datos, de modo que éste pueda considerarse como una ventaja competitiva en el mercado electrónico.

Ahora bien, la segunda transformación, que pasa por considerar el derecho a la protección de datos como un derecho del ciudadano, y no sólo del consumidor, resulta mucho más problemática [5]. Esto se debe a paulatina privatización del derecho de protección de datos, esto es, a la convicción generalizada de que, en calidad de consumidor, el ciudadano puede libremente disponer de sus datos personales conforme a las reglas del mercado.² Mientras la protección de datos continúe siendo irrelevante para una gran mayoría de ciudadanos europeos, la privatización del derecho de protección de datos –y esta es mi segunda tesis central– no es compatible con una concepción de este derecho como derecho fundamental.

2. Código, tratamiento invisible y perfilación en línea

En los últimos años, Lawrence Lessig ha cobrado fama mundial por defender que la arquitectura y configuración técnicas de Internet constituyen su verdadero “código” regulador. «El hardware y el software, que hacen del ciberespacio lo que es, regulan el ciberespacio tal como es».³ Esta tesis condensa una idea muy conocida en el mundo de la informática jurídica, a saber, que la configuración técnica de las cosas determina sus posibilidades de uso y condiciona, por tanto, a sus usuarios, sean o no conscientes de ello. En sede de protección de datos, el “código” ocupa una posición axial, porque de él depende que se pueda o no obtener y procesar gran cantidad de datos personales sin que lo sepa su titular y, por tanto, sin que haga falta que éste realice libremente un acto positivo de revelación de información. Como sabemos, esta posibilidad resulta especialmente atractiva para quien desea hacer negocios en Internet.

protección de datos en la Unión Europea: divergencias normativas y anhelos unificadores, Madrid, Edisofer, 2002.

² Asimismo, en el plano internacional, en especial por lo que hace a las relaciones con Estados Unidos, parece que la Unión Europea ha tenido que renunciar a la estructura procedimental y a las debidas garantías de cumplimiento de los principios básicos de la protección de datos a fin de asegurar un nivel aceptable de protección para sus ciudadanos en el entorno virtual. Esta renuncia implica, a su vez, una velada concesión al régimen de propiedad sobre la privacidad de filiación norteamericana. Véase D. Oliver Lalana, «Notas sobre la autorregulación y la privatización del derecho de protección de datos en la sociedad del conocimiento», *XVI Encuentro sobre Informática y Derecho*, Elcano, Aranzadi, 2004.

³ L. Lessig, *El código y otras leyes del ciberespacio*, Madrid, Taurus, 2001, p. 207.

La supervivencia de una empresa depende de la cantidad, profundidad y calidad de la información que posea sobre sus clientes (actuales o potenciales). En cierto modo, el paradigma empresarial en cuanto a la información personal puede resumirse como “cuanta más, mejor” (*the more, the better*). Pues bien, como trato de explicar en otro lugar,⁴ las empresas que operan en Internet, en especial las dedicadas al cibermarketing, se aprovechan de la arquitectura técnica y de la configuración de los productos de software para recopilar masivamente datos personales. Hoy es casi imposible, en efecto, utilizar Internet sin verse confrontado con una serie de prácticas «que llevan a cabo todo tipo de operaciones de tratamiento de datos personales de manera invisible para el interesado».⁵ La combinación del llamado *chattering* del navegador, los hipervínculos invisibles, los *webbugs* y las *cookies* –todos ellos pueden considerarse elementos vinculados al “código”– proporciona los medios necesarios para elaborar un perfil invisible de todo usuario que utiliza un navegador instalado por defecto.

El conflicto queda tajantemente planteado, precisamente, porque las prácticas colaborativas de acopio de datos personales (*tracing networks*) y la perfilación en línea de los usuarios se conciben como presupuestos indispensables para la supervivencia y el éxito empresariales.⁶ Como apuntan Hagel y Singer, «quien posea los derechos sobre los perfiles de los clientes será quien determine los ganadores y los perdedores de esta nueva era».⁷ La generalización de prácticas de tratamiento invisible de datos personales es un buen ejemplo de la contradicción que parece mediar entre el desarrollo del comercio electrónico y el derecho de protección de datos.

Uno se pregunta si realmente se pueden conciliar los intereses del comercio electrónico con un nivel aceptable de protección de datos; o dicho al revés ¿podemos implantar modelos de tratamiento de la información personal que cumplan con la legislación europea, pero que no desestructuren los sistemas de comercio electrónico? Aprovechando una distinción ya usual,⁸ presentaré a continuación dos grupos de estrategias (tecnológicas y regulativas) que puede seguirse para *disolver* este conflicto entre el derecho de protección de datos y el sistema del comercio electrónico.

3. Estrategias tecnológicas (PETs)

⁴ D. Oliver Lalana, «El derecho fundamental “virtual” a la protección de datos. Tecnología transparente y normas privadas», en *La Ley. Revista jurídica española de doctrina, jurisprudencia y bibliografía*, núm. 5592 (2002).

⁵ Working Party 17: *Recomendación 1/1999 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware*.

⁶ Working Party 37: *Privacidad on-line. Enfoque comunitario integrado de la protección de datos en línea*. Véase también Federal Trade Commission, *On-line profiling: A Report to Congress* (June 2000) [www.ftc.gov/os/2000/07/onlineprofiling.pdf]

⁷ J. Hagel. y M. Singer, *Net Worth: Shaping Markets When Customers Make the Rules*, Cambridge-MA, Harvard Business School Press, 1999, p. xiii.

⁸ Véase, por ejemplo, W. Kilian (2002), «Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung?», en: *Freundesgabe für A. Billesbach*, Stuttgart, J.F. Steinkopf Druck, pp. 151-160; y D.W. Scharthum, «Privacy Enhancing Employment of ICT: Empowering and Assisting Data Subjects», *IRLCT-International Review of Law, Computers and Technology* vol. 1 num. 2 (2001), pp.157-170.

No es casual que me haya referido al código o infraestructura tecnológica de Internet para ilustrar el conflicto entre protección de datos y comercio electrónico. En la red, la primera estrategia de privacidad para el comercio electrónico pasa por emplear la propia tecnología. Las soluciones técnicas de protección de datos se agrupan bajo el epígrafe de tecnologías favorecedoras de la privacidad (PETs: *Privacy Enhancing Technologies*). La categoría es muy heterogénea,⁹ pero puede definirse como un sistema de medidas técnicas que protegen la privacidad eliminando o reduciendo los datos personales que se facilitan en Internet, o impidiendo el tratamiento innecesario o no deseado de los mismos; todo ello sin que se pierda la funcionalidad del sistema informático.¹⁰ En nuestro caso, de lo que se trataría es de integrar las PETs, como mecanismos de protección de la privacidad, dentro de los sistemas de comercio electrónico. Hasta ahora, las posibilidades en este sentido son básicamente tres: (1) la modificación general del código apadrinada por la industria del ciberespacio; (2) lo que podríamos llamar la solución de mercado; y (3) la incorporación de reglas de protección de datos que minimicen los riesgos asociados a determinadas tecnologías usuales en el comercio electrónico (los agentes de software). Presentaré a continuación, en forma resumida, los caracteres de estas tres soluciones.

3.1. Plataforma de Preferencias de Privacidad (P3P)

La Plataforma de Preferencias de Privacidad (P3P) es la propuesta que el “estado mayor” del ciberespacio ofrece para incorporar al código salvaguardas de privacidad de una forma compatible con los intereses comerciales. A grandes trazos, esta plataforma funciona como una lista de preguntas y respuestas sobre el nivel de privacidad entre nuestro navegador y el sitio web al que nos hemos conectado. Por eso, en un sentido amplio, puede decirse que la P3P forma parte del código de Internet. Esta plataforma permite a los sitios web “expresar” sus prácticas de privacidad en un formato estándar de modo que puedan ser leídas e interpretadas automáticamente por un agente de software que utiliza el usuario. Éste, en fin, no precisa leer las políticas de privacidad de los sitios que visita, pues lo hace el software en su lugar, comprobando si tales prácticas coinciden con las preferencias de privacidad previamente definidas por el usuario.

Mediante esta forma de “autorregulación tecnológica” se busca, en definitiva, la forma de delegar determinados aspectos problemáticos de la interacción virtual en un protocolo destinado a “negociar” las protecciones de privacidad.¹¹ Al integrarse directamente en el código, esta solución parece óptima en punto a reconciliar los intereses contrapuestos de la protección de datos y el comercio electrónico. Así lo reflejaría el que esté siendo utilizada por los sitios web más populares.¹² Indudablemente, la P3P representa un adelanto, pero no es suficiente,

⁹ Esta categoría abarca desde los anuladores de *cookies*, hasta los repetidores de correo (*remailers*) y los *anonimizadores* de navegación, pasando por los servidores *proxy*, los agentes de software y las aplicaciones criptográficas como PGP.

¹⁰ J. Borking, y Ch. Raab, «Laws, PETs and Other Technologies for Privacy Protection», 2001 (1), *The Journal of Information, Law and Technology* [<http://elj.warwick.ac.uk/jilt/01-1/borking.html>]

¹¹ Lessig, *op cit.*, pp. 294-95.

¹² W. Adkinson, J. Eisenach y T. Lenard, *Privacy Online: A Report on the Information Practices and Policies of Comercial Websites*, Washington, The Progress & Freedom Foundation, 2002 [www.pff.org], p. 26. Véanse también L.F. Cranor, S. Byers y D. Kormann, «An Analysis of P3P

por sí sola, como garantía de protección de datos en la red. Una solución técnica debería siempre aplicarse dentro de un marco o contexto normativo que proporcionara un nivel mínimo de protección para todas las personas. Y aquí la plataforma muestra sus limitaciones. De una parte, no protege al usuario de Internet en los países que carecen de ese marco legislativo. De otra, no proporciona ninguna forma de asegurar que las compañías que la utilicen sigan sus propias políticas de privacidad, ni que el sitio web que visitamos esté realmente haciendo lo que afirma hacer.¹³ Por último, la Plataforma no utiliza las categorías propias del modelo de legislación europea (Directiva 95/46/CE) sino otras más genéricas y, por tanto, más débiles. La visión industrial de la protección de la privacidad diseña un escenario asimétrico en beneficio del propietario del sitio o del servidor web.

3.2. Agentes de software con protecciones de privacidad

Uno de los elementos básicos del sistema de comercio electrónico son los agentes (inteligentes) de software, es decir, programas o aplicaciones que actúan en representación del usuario intentando alcanzar ciertos objetivos o realizando determinadas tareas sin su intervención o supervisión directa. Quizá los más conocidos sean los programas diseñados para acompañar al usuario en la navegación o para mejorar su comportamiento de consumo en la red.

Dentro de la comunidad de protección de datos, este tipo de agentes son vistos con mucho recelo. Se han granjeado una reputación muy negativa al desvelarse cómo, en muchos casos, se camufla en ellos alguna forma de *spyware* o software E.T.¹⁴ No todos los agentes se dedican a espiarnos, pero lo cierto es que, dado su carácter de representantes y acompañantes, tienen que acumular y manejar gran volumen de información sobre su usuario (su perfil completo), de modo que plantean siempre problemas de protección de datos (y de seguridad). El perfil de usuario puede extraviarse, o cederse por error; y también otros agentes más potentes, actuando en representación de otros usuarios (también más poderosos), pueden atacar a nuestro agente y “robar” nuestro perfil personal. La segunda solución tecnológica surge precisamente en este terreno.

El reto es diseñar agentes de software que incorporen reglas de protección de la privacidad (PISA: *Privacy Incorporated Software Agent*) y que sean capaces de eliminar o minimizar la recogida y uso de información personal.¹⁵ Respecto de la Plataforma de Preferencias de Privacidad, la ventaja que muestran este tipo de agentes es que aspiran a implementar en sus especificaciones técnicas un modelo

Deployment on Commercial, Government, and Children's Web Sites», Florham Park, NJ (Technical Report prepared for the 14 May 2003 Federal Trade Commission Workshop on Technologies for Protecting Personal Information), [www.research.att.com/projects/p3p/p3p-census-may03.pdf] y Working Party 11: *Dictamen 1/1998, sobre la Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS)*

¹³ Working Party 37: *cit.*, pp. 94 ss.

¹⁴ «A new wave of privacy invasions (...) take Internet snooping to a new level: software that commanders your computer to spy on you (...). In Netspeak these programs are known as E.T. applications because after they have lodged in your computer and learned what they want to know, they do what Steven Spielberg's extraterrestrial did: phone home (A. Cohen, «Spies among us», en *Time (Europe)*, July 31, 2000 [www.time.com/time/europe/digital/2000/09/future.html])

¹⁵ J. Borking, *Proposal for building a privacy guardian for the electronic age*, La Haya, Registrariekamer, 2000 [www.registratiekamer.nl/bis/content-1-1-9-5-7.html]

fuerte de legislación de protección de datos (Directiva 95/46/CE). La aplicación del modelo europeo se propone ya desde la fase de diseño de los agentes. Se recomienda, por ejemplo, aplicar algún tipo de *checklist* de criterios de cumplimiento de la legislación europea para que los agentes sean construidos integrando tecnologías de protección de la privacidad, e incluso que se establezca un marco de certificación de privacidad para el diseño y fabricación de los agentes.

La realidad del comercio electrónico, por el momento, no permite ser demasiado optimista en esta dirección: además de las barreras psicológicas que plantea el uso de agentes,¹⁶ estos pueden ser vetados por ciertos sitios web, que los consideran incómodos o perjudiciales para el negocio (porque sólo comparan precios), de modo que no se mantiene la funcionalidad del sistema.

3.3. El modelo de mercado: los infomediarios

Para solucionar este último problema, el propio mercado ha alumbrado un nuevo tipo de proveedor virtual de servicios de privacidad: los *infomediarios*. Se trata de gestores o intermediarios que ayudan a los consumidores a maximizar el valor de sus datos personales.¹⁷ La función del infomediario es representar al consumidor y optimizar el valor que éste recibe a cambio de sus datos. Agregando la información y utilizando el poder de mercado que le dan los muchos clientes de su “club virtual de compras”, los infomediarios aspiran a crear una suerte de mercado inverso, a través del cual los consumidores recuperen parte del poder de negociación que les atribuía el paleocapitalismo.

Pese a que su funcionamiento y caracteres pueden variar según los casos, en general, el infomediario protege los datos del usuario frente a los abusos y cesiones inconsentidas proporcionándole herramientas de privacidad (*privacy tool kit*) que tratan de asegurar un determinado nivel de anonimato (e-mail anónimo, filtros de *spam* o anuladores de cookies). Asimismo, el proveedor del infomediario genera y pone a disposición del consumidor perfiles sobre los vendedores, que incluyen sus ratios de venta, el volumen de devoluciones y reclamaciones, así como el grado de satisfacción de los clientes. Al mismo tiempo, el infomediario recoge y trata información completa del usuario y elabora un perfil informativo extraordinariamente profundo (*profiling tool kit*) que cubre preferencias y transacciones del consumidor, tanto dentro como fuera de la red. Algunos infomediarios ofrecen, en este sentido, la posibilidad de utilizar *cookies* para analizar el propio comportamiento de navegación del usuario (*cookies* inversas o *reverse cookies*).

El siguiente paso es la negociación sobre la privacidad. La filosofía del infomediario es que las empresas sólo podrán tratar los datos de este perfil, disociados o no, en un ámbito de marketing consentido (*permission marketing*).¹⁸ El marketing del permiso opera en dos direcciones: el cliente de un infomediario tiene la opción de permanecer en el anonimato o de revelar su perfil a los

¹⁶ «Many consumers are hesitant to divulge (...) intimate details about their lives to anybody let alone an electronic entity that might expose their information inappropriately as it crawls across the Web» (Hagel/Singer, *op. cit.*, p. 27).

¹⁷ Véase J. Hagel y M. Singer, *op. cit.*

¹⁸ Véase S. Godin, *Permission Marketing*, Simon & Schuster, 1999.

vendedores o a las empresas de marketing directo. Cuando opte por revelar su información, el usuario recibirá siempre un beneficio determinado, como pequeños pagos en metálico, descuentos en el precio de los productos, acceso gratuito a determinados servicios online, etc. Quien prefiera el anónimo, perderá estos beneficios pero asegurará un respeto escrupuloso a su información personal.

En línea de principio, este tipo de respuestas del mercado merecen una valoración positiva, en la medida en que la privacidad gana terreno en el mercado y es tomada incluso como una posibilidad de negocio.¹⁹ Pero la utilización de infomediarios no está exenta de riesgos.²⁰ Al igual que ocurría en el caso de la Plataforma de Preferencias de Privacidad, esta solución, con ser un buen ejemplo de utilización de las fuerzas del mercado para garantizar la privacidad, no puede desplazar el régimen jurídico de la protección de datos. Dado que la relación entre el usuario y el infomediario se basa exclusivamente en la confianza, es preciso que existan recursos legales efectivos para el caso de que el segundo no cumpla lo que promete. Con todo, este parece ser el mejor mecanismo para compatibilizar los intereses comerciales con la privacidad del usuario. El sistema del comercio electrónico percibe las exigencias normativas de su ambiente y las reformula conforme a su propio código de funcionamiento.²¹ En este sentido, el mayor problema es precisamente la mercantilización o “economización” del bien jurídico. Sobre este particular volveré más adelante.

4. Estrategias regulativas

Tras repasar las posibilidades técnicas de protección de datos, queda todavía por resolver, de una parte, cómo hacer que las empresas (electrónicas) europeas cumplan la legislación; y, de otra, cómo proteger a los ciudadanos y consumidores europeos en un entorno global. Dado que la tecnología sólo ofrece una respuesta parcial a estas cuestiones, hay que buscar una solución en el plano de las estrategias regulativas. En este plano se discute cuál debe ser la morfología del modelo de regulación jurídica de la protección de datos en el comercio electrónico. Me gustaría abordar esta cuestión a propósito de tres problemas: (4.1) la autorregulación del sistema del comercio electrónico; (4.2) las formas híbridas de regulación; y (4.3) la implantación del sistema de propiedad de los datos.

4.1. Autorregulación

En general, las normas de protección de datos constituyen para el sistema de comercio electrónico una imposición externa que incrementa los costes de transacción de las empresas y constituye, por tanto, una barrera no tarifaria para su desarrollo. Al ser percibidas como una injerencia en el sistema, éste tiende a no cumplir las normas. Pues bien, si aceptamos que la eficacia de la legislación que

¹⁹ Véase www.lumeria.com, www.digitalme.com, www.timkane.com/enonymous

²⁰ «Some infomediaries (e.g. matchmakers) handle extremely sensitive information. In addition, data subjects are not always consumers; they may participate e.g. in political activities on the web and have to consider carefully whether to engage an agent in doing so» (International Working Group on Data Protection in the Telecommunications, «Common Position on Infomediaries: a privacy-friendly business model?» [www.privacy.de/doc/int/iwgdp/agent_en.htm])

²¹ Véase N. Luhmann, *Das Recht der Gesellschaft*, Frankfurt, Suhrkamp, pp. 452 ss.

pretende aplicarse a un sector de la sociedad no puede asegurarse exclusivamente a través de las sanciones, sino que depende de la colaboración de los agentes que participan en este sector, la solución a esta tendencia de incumplimiento legislativo es la autorregulación.

Existen dos formas elementales de concebir la autorregulación social. En un sentido débil o impropio, cualquier tipo de regla privada constituye un mecanismo de autorregulación. Esta es, por así decir, la visión estadounidense del término. El problema de esta concepción débil es que permite que las posiciones sociales subyacentes, que son posiciones económicas y de poder, operen directamente y sin que medie ningún control jurídico. En cambio, en un sentido fuerte o propio, la autorregulación denota el “control jurídico” de la autorregulación social, esto es, el diseño de un marco de derecho cogente dentro del cual los agentes sociales involucrados puedan dotarse de sus propias normas específicas. Sólo entonces las normas privadas sirven para articular un cierto consenso social, y no se limitan a imponer unilateralmente los intereses de una empresa, una asociación o un grupo determinados.

Como sabemos, en Europa venimos aplicando este segundo concepto, del cual el art. 32 de la Ley Orgánica 15/1999 (España), de protección de datos de carácter personal (en adelante, LOPD) y su modelo, el art. 27 de la Directiva 95/46/CE, son una muestra paradigmática. Merced a la apertura de la legislación oficial a las formas privadas de regulación podemos combinar un elevado nivel de protección con mecanismos de autorregulación generados y por tanto aceptados por los agentes sociales. Cuando se trata del comercio electrónico, esta posibilidad es muy ventajosa desde el punto de vista de la protección de datos.

En primer lugar, la autorregulación (fuerte) supone un valor añadido respecto de la legislación general o básica, ya que un sistema de autorregulación adapta esta legislación a los conceptos y a las necesidades del comercio electrónico, e incluso amplía el nivel de protección y cubre determinados huecos legislativos, como el tratamiento de los datos de menores o la utilización de *cookies*.²² Esto hace que la protección de datos deje de ser algo extraño al sistema de comercio electrónico y pase a integrarse en él, como un aspecto más de la relación entre empresario y consumidor. Desde el punto de vista del Estado, al incremento de la eficacia de la legislación de protección de datos se suma la posibilidad de aprovechar los mecanismos privados de composición y resolución alternativa de conflictos que incluyen estos programas de autorregulación. Esto es muy importante, ya que la generalización del consumo electrónico abre una fuente inagotable de litigiosidad para el sistema general de protección de datos. La implantación de sistemas privados de composición aparece así como un mecanismo idóneo para gestionar riesgos jurisdiccionales y evitar la saturación de los organismos estatales encargados de velar por el cumplimiento de la legislación de protección de datos. A través de la autorregulación social pueden minimizarse, por último, los problemas de cumplimiento y aceptación de la legislación de protección de datos por parte del sistema de comercio electrónico. Lo que resta entonces es dar solución al problema de cómo articular una protección eficaz de los ciudadanos europeos en un entorno internacionalizado como Internet.

²² Así, www.confianzaonline.org, www.aece.org. Véase Working Party 77: *Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing*.

4.2. Instituciones híbridas: el Acuerdo de Safe Harbor

Es un hecho relativamente asumido que la protección de datos personales en Internet no puede lograrse sin protección de datos en (y desde) Estados Unidos²³. En un mundo interconectado, sometido a la hegemonía de las compañías estadounidenses en la red, el derecho fundamental a la protección de datos reconocido por las legislaciones europeas sólo puede asegurarse si dichas compañías cumplen determinados estándares de protección que, además de ser en extremo onerosos para ellas, son completamente ajenos a su cultura jurídica. La idea que cobra vigor es, entonces, que sólo a través de nuevas formas de autorregulación resulta posible compatibilizar dos culturas jurídicas tan diferentes. La solución pasa por la creación de instituciones jurídicas “híbridas”, capaces de funcionar en una sociedad global plagada de marcos jurídicos contradictorios. Estas instituciones ofrecerían una versión embrionaria de la futura regulación de la sociedad del conocimiento.

En materia de protección de datos, este es el papel que juega el Acuerdo de Safe Harbor.²⁴ Este acuerdo resuelve la incompatibilidad entre un sistema de disciplina legislativa y estatal de la protección de datos y otro sistema basado en la autorregulación débil en casi todos los sectores de su economía.²⁵ El nuevo sistema, además, trasladaría a la cultura jurídica estadounidense, de una forma no traumática, el modelo fuerte de autorregulación, equilibrando así la concepción iusfundamental que el derecho de protección de datos tienen en Europa con la concepción meramente comercial de los datos personales como información (casi) libremente transmisible integrada en el patrimonio de las compañías. En este sentido, hay quien piensa incluso que las instituciones híbridas muestran la reafirmación del sistema jurídico estatal en la sociedad del conocimiento, en especial en ámbitos como la protección de datos o la regulación de contenidos en la red.²⁶ Se trataría, en realidad, de mecanismos destinados a gestionar la interdependencia entre diferentes sistemas jurídicos que acarrea la sociedad actual. Safe Harbor no sería una simple respuesta al debilitamiento del Estado, sino un esfuerzo estatal por articular formas de regulación internacional que permitan a los sistemas jurídicos particulares coexistir armónicamente. De tal

²³ «Without American participation at this level, privacy rights on the Internet will remain exposed in the U.S. and, in turn, in the global forum» (W.S. Challis y A. Cavoukian, «The Case for a US Privacy Commissioner: A Canadian Commissioner's Perspective», *The John Marshall Journal of Computer & Information Law*, vol. XIX No. 1 (2000), pp. 1-36, p. 36). «As the Internet is neither an exclusively American nor an European phenomenon, a global regulatory framework is needed» B. Holznapel y R. Werle, «Sectors and Strategies of Global Communication Regulation», *Zeitschrift für Rechtssoziologie* 23 (2002), Heft 1, pp.3-24, p. 9). Véase también H. Burkert, «Privacy-Data Protection – A German/European Perspective», en Ch. Engel and K.H. Keller (eds.), *Governance of global Networks in the Light of Differing Local Values*, Baden-Baden, Nomos, 2000, pp. 43-70.

²⁴ Las reglas de funcionamiento del Acuerdo se encuentran en www.export.gov/safeharbor; para un examen crítico del Acuerdo, véase Working Party 62: *Proyecto de documento de trabajo sobre el funcionamiento del Acuerdo del Puerto Seguro* y Working Party 32: *Dictamen 4/2000, sobre el nivel de protección de los principios de puerto seguro*.

²⁵ H. Farell, «Hybrid Institutions and the Law: Outlaw Arrangements or Interface Solutions», *Zeitschrift für Rechtssoziologie* 23 (2002), Heft 1, pp. 25-40, p. 37.

²⁶ Un ejemplo de esta posición en J. Goldsmith, «Unilateral Regulation of the Internet: A Modest Defence», *European Journal of International Law* 11 no. 1 (2000), 135-48

modo, los Estados podrían asegurar a sus ciudadanos un nivel pragmáticamente aceptable de protección. Como observa Farrell, las instituciones híbridas son esfuerzo para crear interfaces entre diferentes sistemas jurídicos que están siendo interconectados crecientemente por efecto de la globalización: buscan un mínimo de coordinación para evitar que formas de regulación en un sistema tengan repercusiones negativas en otro, sin imponer una única solución jerárquicamente. Se trata de interfaces legales que operan como un “derecho-bisagra”.²⁷ Este derecho preserva la autonomía de los sistemas jurídicos nacionales o regionales (como el europeo), pero la compatibiliza con el orden económico mundial, ya que incrementa las opciones de los usuarios y se amolda perfectamente a una estructura organizativa descentralizada y global, así como a la configuración técnica (heterogénea y abierta) de Internet.²⁸

En este punto, bien es verdad, el acuerdo de Safe Harbor ha introducido estándares de protección de la privacidad muy superiores a los que ofrecen la autorregulación privada (o impropia) y la legislación doméstica estadounidense.²⁹ Pero el panorama de protección que promete el Acuerdo de Safe Harbor no es tan halagüeño como parece. Y su mayor problema no son tan sólo los débiles seis principios “sustantivos” de protección de datos que se pretenden exportar al sistema estadounidense, sino más bien el entramado procedimental que fija el séptimo principio para asegurar su observancia o cumplimiento (*enforcement*). Pero no es caso ahora discutir las muchas inseguridades del puerto seguro.

4.3. El sistema de propiedad de la privacidad (y de los datos)

Tanto la autorregulación como las soluciones tecnológicas pueden vincularse a una determinada concepción acerca de la disponibilidad de los derechos, en concreto de la disponibilidad del derecho a la protección de datos, que puede concebirse como un elemento sujeto a la omnímoda propiedad del interesado, negociable por tanto en los mismo términos que cualquier otro bien. Estos aires *liberales* llegan de los Estados Unidos.

El modelo que concibe los datos personales como un bien sujeto a la propiedad omnímoda de su titular, quien puede negociar libremente con ellos, es el que mejor conviene al desarrollo del comercio electrónico. El reconocimiento de posiciones de propiedad sobre los datos personales es una presuposición funcional para la sociedad de mercado.³⁰ Cuando alguien posee un derecho de propiedad sobre los datos, quien desee tratarlos ha de negociar con él un precio adecuado o una contraprestación antes de poderlos obtener.³¹ Esto hace que el sistema proteja a los individuos en la medida exacta en que cada cual valore su privacidad.

²⁷ Véase Farrell, *op. cit.*, p. 27. La expresión alemana es *Scharnierrecht* (B. Holznel y R. Werle, *op. cit.*, pp. 20-21).

²⁸ Asimismo, Europa y EE.UU. no deben bregar sólo con sus mutuas diferencias, sino que han de buscar un marco de entendimiento y una definición global de la protección de datos para las comunicaciones electrónicas que abarque también los sistemas jurídicos asiáticos (vgr. el chino).

²⁹ Véase Challis/Cavoukian, *op. cit.*, pp. 29-30.

³⁰ Kilian, *op. cit.*, p. 153.

³¹ Lessig (2001, 295-98) aboga por una suerte de derecho de propiedad referido a la privacidad. Frente a lo que denomina “sistema de responsabilidad”, que estaría basado en la regla de obtener primero y pagar después, el régimen de propiedad resulta mucho más ventajoso.

El sistema de propiedad puede combinarse con las dos versiones de la autorregulación. Así, en Estados Unidos prevalece un sistema de propiedad ligado a la autorregulación débil, mientras que en Europa los defensores de este sistema lo integran con la autorregulación fuerte. Kilian sostiene que resulta posible ahorrarse el creciente número de regulaciones en el sector privado si se concibe la autodeterminación informativa como una posición análoga a la propiedad (*eigentumsähnlich*), que puede operar como tal en los procesos del mercado. La naturaleza iusfundamental que el derecho de protección de datos tiene entre nosotros no impediría configurarla como una posición de propiedad, pues ésta constituye también un presupuesto de la sociedad democrática y de mercado. De donde la legislación estatal debería limitarse al aseguramiento de un marco de condiciones para la aplicación de derechos de disposición conforme a las leyes del mercado.³² El modelo de propiedad de los datos no sólo encaja perfectamente en el sistema de comercio electrónico, sino que cuadra también con el principio jurídico básico en esta materia: el principio del consentimiento (modelo europeo) y también con las soluciones tecnológicas (PETs). En general, las empresas pueden mejorar su nivel de protección de datos si lo consideran una ventaja comparativa en el mercado y son capaces de anticiparse a la imagen del mercado inverso.³³ Parece pues que *e-commerce* y protección de datos son perfectamente compatibles. Hemos derribado la primera hipótesis elemental apuntada al inicio de este trabajo. Con todo, la convergencia implica ciertos costes y es evidente que el derecho de protección de datos no le sale gratis a la empresa electrónica.

4.4. Impacto real de la protección de datos para el comercio electrónico

La legislación de protección de datos impone a las empresas (electrónicas) dos grupos de obligaciones: unas afectan a la relación externa de la empresa con los clientes (información, consentimiento, transparencia, ejercicio de derechos...), otras a la organización interna de la propia empresa (medidas de seguridad, relaciones con la autoridad de protección de datos...). Así como las empresas tienen que reestructurarse internamente en atención a la legislación tributaria o de seguridad laboral, así también la legislación de protección de datos les obliga a hacer todo tipo de cabriolas para encajar –afectándola en la menor medida posible– su organización actual en el marco normativo. Este puede considerarse el verdadero impacto de la legislación de protección de datos en las empresas. Mi hipótesis es que, mientras este segundo grupo representa directamente un incremento de los costes empresariales, el primer grupo de obligaciones no implica un costo significativo de modo inmediato,³⁴ ya que se trata de obligaciones meramente “informativas”.

En realidad, la legislación, tras el breve periodo de desconcierto que siguió a la publicación de la Directiva 95/46/CE de protección de datos, y a las respectivas legislaciones nacionales, permite a la empresas hacer prácticamente lo mismo que

³² Kilian, *op. cit.*, p. 154-157.

³³ «The company's goal is simple and straightforward: use privacy to win and keep customers. And that goal is today's emerging business issue» (A. Cavoukian y Hamilton, *The Privacy Payoff. How Successful Business Build Customer Trust*, Whitby, McGraw-Hill/Ryerson, Toronto, p. 4).

³⁴ Sí puede ser determinante para generar una conciencia de privacidad (efecto diferido), en la medida en que supone la visibilización de las prácticas de tratamiento de datos (Véase Oliver Lalana, «El derecho fundamental “virtual”...», *cit.*

venían haciendo cuando no existía legislación en este campo.³⁵ Es cierto que ahora hay que informar y obtener el consentimiento del ciudadano o del cliente, pero satisfechas estas dos condiciones (lo cual no es demasiado caro), el empresario puede hacer –casi– lo que quiera con los datos personales que ha obtenido. Y ello, precisamente, porque los obtiene y procesa con el consentimiento informado del cliente. De ahí que, superados los costes organizativos iniciales, el sistema de propiedad de la privacidad aplicado a la legislación de protección de datos no perjudique demasiado a las empresas de comercio electrónico, ni obstruya sus prácticas de tratamiento de la información personal. Antes al contrario, cumplir con la legislación se puede convertir en un aliciente para el consumo y, en consecuencia, en un factor beneficioso para el sistema del comercio electrónico. No olvidemos que a este sistema pertenecen también los consumidores y que uno de los elementos imprescindibles para su desarrollo es justamente la confianza.³⁶ Un buen ejemplo de cómo el cumplimiento de la legislación de protección de datos puede ser instrumentalizado para obtener la confianza del consumidor son los sellos de cumplimiento de la ley de protección de datos.³⁷ Conviene notar que no se trata de sistemas de autorregulación, sino de meros indicadores simbólicos de cumplimiento de la ley dirigidos a neutralizar las barreras psicológicas que frenan la expansión del comercio electrónico.³⁸

Con todo, no conviene sobreestimar la importancia que el consumidor otorga al nivel de protección de datos que proporciona una empresa. ¿Podemos afirmar que existe algún tipo de relación entre el nivel de desarrollo del comercio electrónico y las opciones legislativas en materia de privacidad? Dicho de otro modo, ¿existe alguna relación entre el nivel de protección de datos que ofrece una empresa *online* y su ratio de ventas o su volumen de negocios? Creo que la respuesta es negativa en ambos casos. Estados Unidos, cuyo modelo de regulación es más bien rácano en cuanto a salvaguardas legales, lidera sin embargo las estadísticas de comercio electrónico. Por su parte, ya entre nosotros, una de las compañías que más han facturado en la red en los últimos dos años puede presumir de tener una buena política “informativa” de privacidad.³⁹ Hasta cierto punto, el grado de protección de la información personal que proporcionan las empresas electrónicas parece ser independiente respecto de su volumen de negocio. Esta aparente contradicción se explica por la escasa concienciación ciudadana sobre el derecho de protección de datos. En España, por ejemplo, tan sólo un 13,7 % de los usuarios de Internet expresan su preocupación respecto del

³⁵ En este sentido, Leith señala agudamente cómo las legislaciones europeas sobre protección de datos no han tenido otro efecto que permitir al usuario verificar o comprobar que sus datos están siendo procesados electrónicamente, pero poco más. Todo tipo de datos personales pueden ser legítimamente procesados conforme a la legislación europea y, prácticamente, en la medida en que la información personal satisfaga determinados requisitos de exactitud y actualidad, su titular primigenio apenas tiene control sobre ella (P. Leith, «Confidentiality, Privacy and E-Government: Clarifying the Notion of ‘Public Space’», en F. Galindo y R. Traunmüller (eds.), *E-Government: Legal, Technical and Pedagogical Aspects*, Zaragoza, pp. 105-122, pp. 110-111).

³⁶ Véase Cavoukian y Hamilton, *op. cit.*

³⁷ Véase www.camerfirma.com/mod_web/sello/sello.html. Según observa el Grupo de Trabajo de la Comisión Europea, la proliferación de este tipo de sellos –con merecer una valoración general muy positiva– puede producir cierta confusión entre los usuarios (Working Party 37, *cit.*, p. 94).

³⁸ Esto ilustra cómo la protección de datos es planteada como un problema de consumo, pero no como un derecho fundamental del ciudadano.

³⁹ Véase www.iberia.com

tratamiento de datos personales como una barrera a la hora de realizar transacciones electrónicas (comerciales).⁴⁰ Así las cosas, las empresas no sólo pueden adaptarse con cierta flexibilidad a la legislación, sino que incluso pueden instrumentalizar el derecho de protección de datos para mejorar el negocio.

5. ¿Qué queda del modelo de derecho fundamental?

Como vemos, la legislación de protección de datos y el comercio electrónico se pueden conjugar operativamente a través del modelo de propiedad de los datos. Ahora bien, ¿qué pierde entonces el sistema europeo de protección? Es decir, ¿se puede vender y negociar con un derecho fundamental, sin que este derecho deje de ser fundamental y sin que se produzca una merma significativa en la protección del ciudadano?

En principio, parece que la mera idea de asignar valores monetarios a los derechos humanos subordinaría la legalidad a las exigencias económicas, y «pondría en duda el significado normativo de las garantías constitucionales».⁴¹ Sobre la base de esta intuición, una concepción fuerte o garantista de la protección de datos puede defender que existen restricciones a la disponibilidad de este bien jurídico, precisamente, en atención a su carácter fundamental. En otras palabras, puede sostenerse que el consentimiento no es ilimitado como mecanismo de legitimación del tratamiento de los datos personales y que, por tanto, el sistema de propiedad de los datos es inaceptable en Europa.

Que el derecho de protección de datos es un derecho fundamental de la persona es una cantinela especialmente frecuente desde su inclusión en el catálogo de derechos fundamentales de la Unión Europea. Sin embargo, creo que este derecho es percibido todavía como un derecho (fundamental) menor o accesorio, que no es tomado en serio y que, por tanto no se han derivado de su naturaleza jurídica privilegiada todas las consecuencias que serían deseables.

1. La concepción garantista de este derecho parte de la asunción de que los derechos fundamentales no sólo son derechos de la persona o derechos subjetivos, sino que tienen un componente indisponible para su titular, en tanto que estos derechos pertenecen al llamado orden público objetivo. En el caso de la protección de datos, ya el Tribunal Constitucional Federal alemán configuraba en su día el derecho de autodeterminación informativa a partir del art. 1.1 de la Ley Fundamental de Bonn, que protege la dignidad humana, y lo relacionaba con el art. 1.2, que garantiza el libre desarrollo de la personalidad.⁴² De ambos mandatos constitucionales derivaba la facultad de la persona para «decidir básicamente por sí misma cuándo y dentro de qué límites procede relevar situaciones referentes a su vida privada». El Tribunal alemán diferenciaba de seguido dos facetas del derecho de autodeterminación informativa: una subjetiva y otra objetiva. De una

⁴⁰ Véase «Estudio de Comercio Electrónico B2C AECE-FECEMD 2003», en www.aece.org

⁴¹ W. Heydebrand, «From Globalisation of Law to Law under Globalisation», en D. Nelken y J. Feest (eds.), *Adapting Legal Cultures*, Hart Publishing, Oxford/Portland, 2001, pp. 117-140, p. 131. Como señala S. Garfinkel (*Database Nation: The Death of Privacy in the 21st Century*, O'Reilly & Associates, 2000), el sistema de propiedad tiende a degenerar en una situación en la que los individuos que desean proteger sus datos personales están obligados a pagar por recuperarlos o, de no hacerlo, a cargar con las consecuencias de haberlos vendido.

⁴² *BVerfGE* 65, 1

parte, «un orden social y jurídico en el que el ciudadano ya no pudiera saber quién, cuándo y con qué motivo sabe algo sobre él» sería contrario a la facultad de autodeterminación y «menoscararía las oportunidades del desarrollo de la personalidad» (aspecto subjetivo), pero también, de otra, lesionaría «el bien público, porque la autodeterminación constituye una condición elemental de funcionamiento de toda comunidad fundada en la capacidad de obrar y de cooperación de sus ciudadanos» (aspecto objetivo). Es justamente este aspecto objetivo de los derechos fundamentales lo que impide su venalización.⁴³

2. Quienes defienden el sistema de propiedad acusan a esta posición de ideología izquierdista y paternalista⁴⁴. Como hemos dicho antes, el principio del consentimiento y, por tanto, la disponibilidad sobre el propio derecho de protección de datos, pertenece también a su núcleo esencial. De donde la protección estatal de la esfera privada debería incluir también la libertad para abandonarla a las reglas del juego del mercado.⁴⁵ Esta línea argumental tiene un fuerte componente pragmático, pues

no estamos debatiendo si debemos movernos en un mundo en el que los datos se recojan, se utilicen y se vendan: ya vivimos en ese mundo (...). Yo defiendo un régimen de propiedad, no basándome en la santidad de la propiedad, sino en su utilidad a la hora de servir a un ideal diferente pero igualmente importante.⁴⁶

Concedido. Sin embargo, también en este mundo nuestro –precisamente por él– pueden aducirse buenas razones para sostener que la protección de datos, en tanto que derecho fundamental, es (al menos, relativamente) indisponible para el individuo.

3. Los argumentos de Kilian y Lessig plantean dos objeciones que han de tomarse muy en serio. Es verdad, en primer lugar, que no existen derechos absolutos, y que tampoco lo es el derecho de protección de datos. Por eso este derecho puede «ceder ante intereses constitucionalmente relevantes, siempre que el recorte que aquél haya de experimentar se revele como necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho (SSTC 57/1994, FJ 5 y 143/1994, FJ 6). En algunos supuestos, el derecho a la protección de datos puede también flexibilizarse frente a la satisfacción de legítimos intereses empresariales (libertad empresarial).⁴⁷ Hay quien defiende la prioridad absoluta de la protección de datos porque se trata de un derecho fundamental, mientras que la libertad empresarial no lo es. Pero puede fácilmente argüirse que la economía de mercado constituye un bien jurídico colectivo que forma parte del mismo orden público al

⁴³ Esta parte indisponible u objetiva, junto con las facultades de control y disposición sobre los propios datos que corresponden al sujeto, integra lo que llamamos el contenido esencial del derecho. Este contenido esencial resulta indisponible para el individuo, como también lo es para el mismo legislador. Un segundo argumento, más alambicado, es el de la “plurirrelacionalidad” (*Mehrrelationalität*) de los datos, que imposibilitaría asignarlos como propiedad a un sólo individuo (Roßnagel/Pfitzmann/Garstka, *op. cit.*, p. 39)

⁴⁴ «The tendency (...) is towards a top-down, “paternalistic” attitude to information which is diametrically opposed to real notions of community, responsibility and citizenship» (Leith, *op. cit.*, p. 110).

⁴⁵ Kilian, *op. cit.*, p. 157.

⁴⁶ Lessig, *op. cit.*, p. 297.

⁴⁷ Véanse arts. 6.2 LOPD y 7.f Directiva 95/46/CE

que pertenece la protección de datos, y que, por tanto, se trata de bienes jurídicos que pueden limitarse mutuamente.⁴⁸ Por otra parte, no puede olvidarse que el contenido esencial del derecho no sólo abarca la posibilidad de control, sino también la de disposición sobre los propios datos y, por tanto, el consentimiento del interesado. De tal suerte, no ha de resultar sencillo justificar que puedan imponerse restricciones a la disponibilidad de (o al juego del consentimiento sobre) los propios datos.

4. La tensión que media entre el derecho de protección de datos y el derecho de propiedad sobre los datos (y la libertad empresarial) puede reformularse como una tensión interna entre dos componentes esenciales del derecho a la protección de datos: el consentimiento y la posibilidad de control sobre los propios datos (STC 254/1993). En el campo del comercio electrónico, ambos elementos suelen entrar en conflicto. Así, por ejemplo, en buena parte de las transacciones en línea, la prestación (inducida o no) del consentimiento se traduce muchas veces en la venta absoluta de las posibilidades de control sobre los propios datos.⁴⁹ Se nos informa debidamente, eso sí, y con ello el problema del consentimiento queda zanjado: ya podemos, con la venia de la legislación, ceder los datos obtenidos a múltiples empresas de aquí o de fuera y para todo tipo de fines genéricamente formulados.⁵⁰ En estas condiciones, que ponen en duda hasta qué punto el titular de los datos puede seguir ejerciendo algún tipo de control sobre los mismos, el consentimiento tiene que ponderarse el resto de los elementos del núcleo esencial del derecho.

Por caminos diferentes, ambas objeciones conducen al mismo destino: la necesidad de ponderación. En un caso, se trata, por así decir, de una ponderación “externa”, entre la economía de mercado (libertad de empresa) y el derecho de protección de datos. En el otro, la ponderación es “interna”, pues tiene lugar entre dos elementos del contenido esencial del derecho que pueden entrar en colisión. Nótese que las colisiones nunca se producen en abstracto, sino que tienen lugar en un contexto histórico concreto. El problema está en decidir, aquí y ahora –no definitivamente, sino para el presente y el futuro inmediato– las relaciones de prioridad entre los dos bienes jurídicos (principios) en colisión.

⁴⁸ Véase R. Alexy, «Derechos individuales y bienes colectivos», en *El concepto y la validez del derecho*, Barcelona, Gedisa, 1994, pp. 179-208.

⁴⁹ Garfinkel (*op. cit.*, p. 264) observa cómo en Estados Unidos el consentimiento del ciudadano se ha convertido en algo así como una mala broma. Los consumidores son forzados a aceptar los términos contractuales impuestos por las empresas so riesgo de perder la oportunidad de negocio. Es obvio, además, que las cláusulas de consentimiento pueden ser redactadas de forma torticera para permitir a las compañías un tratamiento irrestricto de la información personal.

⁵⁰ En www.terra.es, por ejemplo, hay que abrir una nueva página para poder ver los cientos de empresas y países a los que se autoriza la cesión de datos personales. Se puede dar en este contexto una interesante sinergia entre el derecho de protección de datos y el derecho de protección de los consumidores (Ley 34/2002, de servicios de la sociedad de la información y Directiva 2000/31/CE, sobre el comercio electrónico), que ampara también al usuario “que no consume”, ya que muchas cláusulas contractuales sobre protección de datos pueden considerarse abusivas. En todo caso, no dejaría de ser curioso que un derecho fundamental (la protección de datos) esté menos protegido que un derecho que no tiene ese rango (protección de los consumidores). El problema de la articulación práctica de la prioridad del derecho de protección de datos sobre la libertad empresarial podría ser, por ejemplo, la vía de las cláusulas abusivas y del régimen de condiciones generales de la contratación.

Pues bien, al defender el sistema de propiedad, suelen cometerse dos errores. El primero –relacionado con la apreciación o la evaluación de las circunstancias o del contexto concreto en el que se produce la colisión entre bienes jurídicos– es creer en la soberanía del titular de los datos (la soberanía del consumidor). Esta apreciación inadecuada de las circunstancias del caso conduce a un segundo error que afecta a la valoración de la importancia de los bienes en conflicto.

5. Para efectuar una ponderación hay que tener en cuenta todas las circunstancias del contexto. Una de estas circunstancias, que tiene capital importancia en mi argumentación, son las carencias culturales en la materia. Para que pudiéramos hablar de verdadera soberanía el ciudadano debería estar suficientemente informado de las transacciones que realiza sobre sus datos. Esta información debería cubrir dos ámbitos: el valor económico de los datos y la dimensión social y axiológica del su tratamiento. Las carencias culturales de la población en ambos aspectos hacen que el sistema de propiedad perpetúe el desequilibrio informativo entre titulares de datos (ciudadanos) y responsables de ficheros (pequeños grandes hermanos).

La condición elemental para que la tecnificación de la protección de datos, la transferencia de parcelas de regulación al sector privado y el sistema de propiedad no desemboquen en una merma del nivel de protección de los ciudadanos es, en suma, de naturaleza psico-sociológica, a saber: los participantes deberían conocer las verdaderas consecuencias de las transacciones que realizan sobre sus datos. Recordemos que la información es condición para la formación válida del consentimiento (art. 3 LOPD). Ahora bien, raro es a día de hoy el caso en el que el titular de los datos es verdaderamente consciente de la importancia social y económica del tratamiento de sus datos. Por mucho que haya crecido la preocupación del consumidor por su privacidad, la conciencia de protección de datos todavía no está todavía desarrollada.⁵¹ Valga un ejemplo.

A mediados de los años ochenta, se preguntó a los paseantes en una calle de Nueva York acerca de la invasión de la privacidad causada por las nuevas tecnologías. El noventa por ciento de los encuestados manifestó estar preocupado. Al día siguiente, en la misma calle, se ofrecía una nueva tarjeta de crédito con interesantes ventajas: ahora, el noventa por ciento de los paseantes completaba un formulario en el que se solicitaban datos de todo tipo, entre ellos el número de seguridad social o de cuenta corriente.⁵² Este ejemplo ilustra cómo existe un abismo entre la importancia “teórica” de la preocupación por la protección de datos y su importancia real o práctica. Desde todas las instancias se nos dice que la utilización comercial de la información personal representa una seria amenaza para nuestros derechos de ciudadano. Pero a la hora de la verdad, muchos consumidores están más que felices cuando abandonan el control real sobre sus datos a cambio de una tarjeta de fidelización del supermercado.⁵³ Siempre que le premien con un atractivo descuento, a nadie le importa realmente que su historial de consumo sea almacenado y analizado, cedido y exportado al extranjero. Sin

⁵¹ Véase A. Viseu., A. Clement y J. Aspinall, «Situating Privacy Online: Complex Perceptions and Everyday Practice», University of Toronto, Knowledge Media Design Institute, 2003 [http://kmdi.toronto.edu/situating_privacy_online_final_paper.pdf]

⁵² Véase D. Lyon, *The Electronic Eye: The Rise of Surveillance Society*, Minneapolis, University of Minnesota Press, p. 140

⁵³ Véase Leith, *op. cit.*, p. 114.

verdadera conciencia de los riesgos del tratamiento informatizado de los datos personales, la sacralización de la regla del consentimiento, que está en la base del sistema de propiedad, puede terminar desnaturalizando el modelo europeo de derecho fundamental de la protección de datos.⁵⁴

6. Quien defiende el sistema de propiedad equipara normativamente la protección del mercado y de la libertad de empresa con el derecho fundamental de la protección de datos. El problema es sobre qué argumentos puede sostenerse que la propiedad y el mercado *deben prevalecer, en el contexto actual*, sobre la posibilidad de control sobre los propios datos. Podría argumentarse, como en su día hizo nuestro Tribunal Constitucional, que el contenido esencial del derecho está suficientemente garantizado por el sistema legislativo de protección (STC 143/1994). Pero también es cierto que parte del régimen que el Tribunal Constitucional consideró suficiente entonces, fue declarado inconstitucional después (STC 292/2000). Con esto quiero decir que nada impide que puedan adoptarse posiciones críticas frente a las evaluaciones del nivel de protección de datos que tenemos actualmente.

Por lo que hace a la valoración del peso de los bienes en conflicto, hay que tener en cuenta que el derecho de protección de datos no es un derecho fundamental cualquiera, sino que constituye *el* derecho fundamental característico de esa faceta de la realidad social que llamamos sociedad de la información, en la que opera como «un elemento constitutivo de la libertad del ciudadano».⁵⁵ No sólo no es un simple derecho de la personalidad, sino que aparece como un derecho fundamental transversal que aglutina el contenido comunicativo de todos los derechos fundamentales.⁵⁶ Precisamente por ello el derecho de protección de datos puede operar como criterio de legitimidad política.⁵⁷ Como derecho fundamental, el de protección de datos no sólo debe imponer límites a la administración pública, sino también al poder de las empresas, organizaciones y grandes compañías (eficacia horizontal de los derechos fundamentales). En la sociedad actual, una de las tareas esenciales de este derecho es equilibrar las asimetrías “reales” de información –de poder– que median entre éstas y los

⁵⁴ «Las facultades legalmente atribuidas a los sujetos concernidos y las consiguientes posibilidades de actuación de éstos son necesarias para el reconocimiento e identidad constitucionales del derecho fundamental a la protección de datos. Asimismo, esas facultades o posibilidades de actuación son absolutamente necesarias para que los intereses jurídicamente protegibles, que constituyen la razón de ser del aludido derecho fundamental, resulten real, concreta y efectivamente protegidos. De manera que, privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo estará también de su derecho fundamental a la protección de datos, puesto que, como concluyó en este punto la STC 11/1981 (FJ 8), "se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección"» (STC 292/2000, de 30 de noviembre, FJ 10).

⁵⁵ Oliver Lalana, «El derecho fundamental “virtual”...», *cit.*

⁵⁶ Sobre esta idea, véase el informe de A. Roßnagel, A. Pfitzmann y H. Garstka, *Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministers des Innern*, 2002, pp. 19-20 [<http://www.dud.de/dud/documents/modernisierung-dsrecht.pdf>]

⁵⁷ Véase la *Declaración final de la Conferencia Internacional de Autoridades de Protección de Datos* (Declaración de Venecia): <http://www.datenschutz-berlin.de/doc/int/konf/22/declar.htm>; cfr. A. E. Pérez Luño, «Las generaciones de derechos humanos», en *Revista del Centro de Estudios constitucionales* 10 (1991), 203-217; y Working Party 26: *Dictamen 4/1999, sobre la inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos fundamentales*, p. 3.

ciudadanos. Si las exigencias del mercado terminan imponiéndose y el sistema de propiedad transforma el sentido iusfundamental de la protección de datos en términos de valor económico, se abandona precisamente esta función, lo cual puede determinar una pérdida de legitimidad del Derecho y del Estado en la sociedad de la información.⁵⁸

6. El modelo de sociedad de la información

Es evidente que esta concepción tan fuerte del derecho de protección de datos está “condenada” a tropezar con las prácticas habituales del comercio electrónico. Uno puede, desde luego, conformarse con este curso de acontecimientos y pensar que una concepción fuerte de la protección de datos es demasiado exigente y poco operativa. Al igual que ocurre con la protección del medio ambiente, esta concepción presupone que el ciudadano y el empresario no sólo tengan en cuenta el aspecto económico del tratamiento de los datos personales, sino también su dimensión social y axiológica. Lo cual, a día de hoy, es poco menos que ilusorio. Creo, a pesar de todo que, ahora que pensamos en el derecho que conviene a la sociedad interconectada, es bueno mantener este tipo de visiones fuertemente normativas. Lo digo en el convencimiento de que la discusión acerca del modelo de protección de datos es, en último término, una discusión acerca de la sociedad de la información en la que queremos vivir.

⁵⁸ «One of the reasons for the slippery character of privacy is that the word itself points in the direction of the individual, rather than the social. (...) It steers the discussion towards personal, individual preferences. Being biased towards the individual market it is hard, if not impossible, (...) to make visible its value as social good» (Viseu/Clement/Aspinall, *op. cit.*, p. 17)