LA INFRACCIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS COMO MODELO DE NEGOCIO: EL CASO *FACEBOOK*

Thilo WEICHERT[1]
Ricardo MORTE FERRER[2]

SUMARIO: I. *Introducción*. II. Facebook*: notorio infractor*. III. *La protección de datos como anacronismo*. IV. *¿El código es ley?* V. *La estrategia de comunicación*. VI. *En ningún caso aportar aclaraciones jurídicamente vinculantes*. VII. *Conclusiones.*

I. INTRODUCCIÓN

Las normas de la protección de datos en el sector privado protegen "derechos individuales" o personales aun cuando su infracción pueda tener o no "efectos en los negocios" o en las "reglas de comportamiento en el mercado", de acuerdo con la jurisprudencia dominante y en concreto con la del OLG (Audiencia Territorial

[1] Director de la Autoridad de Protección de Datos del Land Schleswig-Holstein, Alemania. Jurista y politólogo, cursó sus estudios en las universidades de Friburgo y Genf (Suiza). Entre 1984 y 1986 fue miembro del Parlamento del Land Baden-Württemberg, y desde 1982 ha desarrollado actividades como abogado, político, publicista y docente en Friburgo, Stuttgart, Dresden y Hannover.

[2] Colaborador jurídico del Proyecto Europeo TClouds en el Unabhängigen Landeszentrums für Datenschutz (ULD). Licenciado en derecho, máster en sociedad de la información y el conocimiento por la Universidad Oberta de Cataluña; máster en derecho deportivo por la Universidad de Lérida, y estudiante del máster en *software* libre de la Universidad Oberta de Catalunya. Desde septiembre de 2009 es tutor de seguimiento del grado en derecho de la Universidad Oberta de Cataluña. Ha sido vocal del Tribunal Balear del Deporte. Desde 2010 es colaborador de Mendo Abogados (*www.mendo.es*).

por sus siglas en alemán), de München.[3] Sin embargo, el Kammergericht (Audiencia Territorial) de Berlín ha afirmado que los *like buttons* de *Facebook*, situados en la página *web* de una tienda *online*, no representan ningún problema desde el punto de vista de la competencia, incluso en el caso que supongan una infracción de la normativa de protección de datos.[4] Estas afirmaciones producen extrañeza, teniendo en cuenta que Facebook efectuó su aparición en el mercado bursátil el 17 de mayo de 2012 con un valor inicial de 100,000 millones de dólares, y que su modelo de negocio, al menos desde el punto de vista alemán y europeo, está basado en una infracción sistemática de la normativa de protección de datos personales.[5]

Hasta el momento, la jurisprudencia europea ha sido más rápida que el legislador en lo que afecta a los retos planteados por Internet. No quedaba —ni queda— otra salida, dado que existen numerosos conflictos para los cuales el legislador no ha encontrado una solución precisa, sin que quepa duda alguna al respecto. Con la protección de datos en Internet se repite lo que ya sucedió con la protección de la personalidad hace 50 años: la protección de las personas prominentes y figuras públicas encontró rápidamente una solución; mientras que la protección del ciudadano común sigue esperándola. Las actuales propuestas de solución, ofrecidas por los tribunales en casos concretos, deberían ser fijadas de forma general y vinculante por el legislador. Mientras el legislador no establezca normas explícitas y practicables,

3 OLG München, *MMR*, *Revista sobre Derecho de Internet y Multimedia*, 2012, p. 317; en sentido contrario Weichert, *VuR, Revista sobre Derecho de la Economía y de los Consumidores*, 2006, pp. 377 y ss., y Huppertz y Ohrmann, *CR, Revista Computador y Derecho*, 2011, pp. 449 y ss.

4 KG Berlin, *CR, Revista Computador y Derecho*, 2011, pp. 468 y ss.; anteriormente y en el mismo sentido LG Berlin, *DuD*, *Revista dedicada a la Protección y Seguridad de los Datos*, 2011, p. 429.

5 Sobre la mercantilización de la esfera privada en general Hess/Schreiner *DuD*, *Revista dedicada a la Protección y Seguridad de los Datos*, 2012, pp. 105 y ss.; desde el punto de vista legal Weichert, *NJW, Nuevo Semanario Jurídico*, 2001, pp. 1463 y ss.

podrán seguir estableciéndose y funcionando modelos de negocio basados en la infracción de la normativa de protección de datos.

Nos encontramos en una fase de rasante desarrollo de la sociedad de la información, a nivel cultural, social y económico, y se trata de un desarrollo guiado esencialmente por los avances tecnológicos. En las secciones de sociedad y de economía de la prensa escrita, se puede leer desde hace ya tiempo que la moneda en Internet la constituyen los datos de carácter personal.[6] La consecuencia lógica de esta afirmación es que la captación de esos datos, si se hace basándose en infracciones de la normativa de protección de datos, supone un acto de competencia desleal, además de una infracción de la normativa en materia de competencia. En esta materia, los tribunales no han tomado las decisiones que cabría esperar. Tampoco se puede observar que los políticos sean realmente conscientes de la situación.

En este texto demostraremos, basándonos en el ejemplo de *Facebook*, cómo funciona —al menos de momento— un modelo de negocio basado en la infracción de la normativa de protección de datos personales. Esta red social demuestra de forma preocupante lo ineficaz que puede resultar nuestro sistema legal cuando entran en juego influyentes intereses políticos y económicos.

De acuerdo con la información aportada en el prospecto bursátil emitido por *Facebook* en febrero de 2013, esa empresa facturó en 2011: 3,700 millones de dólares (unos 2,800 millones de euros) y generó un beneficio de 1,000 millones de dólares (unos 47,000 millones de pesos mexicanos). Ahora bien, 3,150 millones de dólares (82% de la facturación), se generaron por medio de publicidad específica. Veintidós millones de los 901,000 millones de usuarios de *Facebook* (cerca de 15% de la población mundial) son alemanes. Según un estudio de la agrupación Bitkom, 32% de las empresas alemanas utilizan las *Facebook-Fanpages*[7] que son gratuitas. Con un valor bursátil de 100,000 millones de dólares,

6 Lill *et al*., "Falsche Fans", *Der Spiegel*, núm. 30, 2012, pp. 128 y ss.

7 Kleinz, die Milliarden-Maschine, *c't Revista sobre Técnica Informática*, núm. 12, 2012, p. 82.

se puede afirmar, al menos *a priori*, que el valor de una cuenta de *Facebook* es de unos 100 dólares. Cabe recordar que *Facebook* entra en competencia directa con *Apple, Google* y *Amazon*, cuyos modelos de negocio se basan en gran parte en la recopilación a través de la red de perfiles de datos para publicidad específica y en la posterior comercialización de éstos.[8]

II. *FACEBOOK*: NOTORIO INFRACTOR

Que la red social *Facebook* infringe la normativa de protección de datos ha sido puesto de manifiesto por autores, autoridades de protección de datos y algunos tribunales, así como por diferentes medios de comunicación *online* y *offline*.[9] A continuación aportamos una lista de las principales infracciones, especialmente en lo que afecta al BDSG (la Ley Federal de Protección de Datos de Alemania):

- No se recoge el consentimiento del titular de los datos previsto en la Ley, por ejemplo en el caso de transferencias de

8 Bethge *et al*., "Die fanatischen Vier", *Der Spiegel*, núm. 49, 2011, pp. 70 y ss.

9 Konferenz der Datenschutzbeauftragten des Bundes und der Länder (Conferencia de las Autoridades de Protección de Datos a nivel federal y de los Länder), 28 y 29 de septiembre de 2011, München, Datenschutz bei Sozialen Netzwerken jetz verwirklichen; LG Berlin, U. v. 06.03.2012, Az. 16 O 551/10; al respecto Schwenke, Nutzer dürfen nicht zur Ware werden, *www.lto.de*, del 13 de marzo de 2012; LG Aschaffenburg, U.v., del 19 de agosto de 2011, Az. 2 HK 54/11, BeckRS 2011, 24110; Bahr, Facebook: Eine datenschutzrechtliche Analyse, website boosting, del 11 de diciembre de 2010; Big-Brother-Award 2011, FIfF-Kommunikation, núm. 2, 2011, pp. 20 y ss.; Ernst, *NJOZ, Revista Jurídica Online*, 2010, 1917, y *NJW, Nuevo Semanario Jurídico*, 2010, 2989; Jandt/Roßnagel, *ZD, Revista sobre Protección de Datos*, núm. 4, 2011, pp. 160 y ss.; Laue, Datenschutz-Berater 6/2011, 11 ff.; Polenz, *VuR, Revista sobre Derecho de la Economía y de los Consumidores*, núm. 6, 2012, pp. 207 y ss.; Roosendaal, Facebook Tracks and Traces Everyone: Like This!, Tilburg Law School Legal Studies Research Series, núm. 3, 2011; ULD, Soziale Netzwerke: Wo hört den Spaß auf? Blaue Reihe 7; a.A. Voigt/Alich, *NJW, Nuevo Semanario Jurídico*, 2011, 3541.

datos fuera de Europa, o en la utilización de *cookies* que no son necesarias para el servicio prestado (§ 4c. Abs 1 Nr.1 BDSG, artículo 5.3 de la Directiva Europea de Protección de Datos, 95/46/CE).

- Los consentimientos que se recogen no cumplen los requisitos en materia de protección de datos personales (§ 4a. BDSG, § 13 Abs. 2, 3 TMG (la Ley de Telemedios de Alemania).
- Las condiciones generales de contratación, es decir, las condiciones de uso, contienen cláusulas sorprendentes y lesivas para el consumidor y por distintos motivos nulas de pleno derecho (§§ 305 ff. BGB (el Código Civil Alemán).[10]
- El requisito legal para ejercer los derechos de acceso, rectificación, cancelación y oposición se ve incumplido; en algunos casos es totalmente imposible y en otros se establecen barreras al mismo (§§ 6, 34, 35 BDSG).
- El deber de eliminación o borrado total de los datos, por ejemplo en caso de violación de los derechos de la personalidad, por cancelación de la cuenta o por el transcurso del tiempo establecido para ello, no se cumple (§ 35 Abs. 2 BDSG)
- Se recogen y procesan datos de terceros sin su consentimiento ni base legal para ello (§§ 28, 29 BDSG, §§ 14, 15 TMG).
- En la aplicación del procedimiento biométrico de reconocimiento facial no se hacen valer los derechos del sujeto de la información o titular de los datos (§ 28 Abs. 1 Nr. 2 BDSG).[11]
- Los requisitos de legitimación para el tratamiento de datos sensibles, como los de salud, no se cumplen (§§ 3 Abs. 9, 4a. Abs. 3, 28 Abs. 6-9 BDSG).

10 Sobre las nuevas cláusulas de privacidad de *Google*, Becker/Becker, *MMR, Revista sobre Derecho de Internet y Multimedia*, 2012, pp. 351 y ss.

11 HmbBfDI, *DuD, Revista dedicada a la Protección y Seguridad de los Datos*, 2011, p. 743; HmBfDI, Verfahren gegen Facebook vorläufig ausgesetz, PE vom, 7 de junio de 2012.

- En la creación de perfiles no se aporta suficiente información al usuario y no se ofrece la posibilidad de oponerse al tratamiento de datos (§ 15 Abs. 3 TMG).
- La utilización de la red social con seudónimos o anónimos no está permitida, pese a ser posible (§ 13 Abs. 6 TMG).
- No se cumple con la protección de los menores de edad (§§ 106 ff. BGB).
- Los procedimientos de pago ofrecidos no cumplen la normativa de protección de datos personales.
- Los contenidos de las comunicaciones individuales son controlados por motivos de seguridad, lo cual supone una violación del secreto de las telecomunicaciones (§ 88 TKG) (la Ley de Telecomunicaciones de Alemania).[12]
- Las medidas de seguridad, tanto técnicas como organizativas, son insuficientes (§ 9 BDSG mit Anlage).

Facebook demostró que es consciente de estas infracciones con su salida de la bolsa de valores. En las 20 páginas dedicadas a los riesgos en el prospecto bursátil se mencionaban los imponderables que suponen normativas estrictas de protección de datos. Ello podría suponer costes incalculables, retrasos en la introducción de nuevos productos, o comentarios negativos en prensa.[13]

Cuando se produce una ilegalidad o infracción, los afectados no pueden estar seguros de obtener aquello a lo que tienen derecho, que se reconozca la ilegalidad y que derive en una sanción. El caso *Facebook* es un ejemplo paradigmático, que podría servir de ejemplo para todas las empresas que quieran conseguir benefi-

12 Menn, *http://www.reuters.com*, 12.07.2012; Paukner, *http://www.süddeutsche.de*, del 13 de julio de 2012; LfDI Rheinland-Pfalz, PE v., del 19 de julio de 2012.

13 Bernau, Datenschatz, *SZ, Süddeutesche Zeitung*, núm. 16, del 17 de mayo de 2012; sobre el riesgo que la protección de datos puede suponer (en este caso) en la Bolsa Weichert, Illegal und vergoldet, *http://theeuropean.de/thilo-weichert/11075-facebooks-umgang-mit-benutzerdaten*.

cios mediante infracciones de la normativa de protección de datos personales.

Las infracciones en materia de protección de datos son, si se cometen con el objetivo de enriquecerse, constitutivas de delito según lo previsto en el § 44 Abs. 1 BDSG. Cabe preguntarse entonces ¿por qué motivo las infracciones en materia de protección de datos cometidas de manera sistemática como modelo de negocio no son perseguidas como constitutivas de delito, concretamente de un delito económico?

III. La protección de datos como anacronismo

Facebook nunca ocultó sus intenciones económicas. En contraste con otras empresas del ramo de las tecnologías de la información con sede en los Estados Unidos, *Facebook* se abstiene de negar sus infracciones en materia de protección de datos exponiendo razones técnicas o jurídicas. En realidad, se trata de algo más grande que la mera forma técnica o jurídica; se trata de un cambio de valores sociales que esta empresa quiere promover, donde las personas de vanguardia y que siguen el ritmo de las tecnologías no deberían alegar pequeñeces.

1. *Posprivacidad*

Uno de los primeros en manifestarse en esta dirección fue el jefe de Sun Microsystems en 1999, cuando afirmó "You have zero privacy anyway. Get over it".[14] Ya entonces se podía apreciar que datos de contenido y de usuarios de *Internet* valían su peso en oro para las empresas de servicios en ese ámbito y que, por lo tanto, no debían ponerse barreras legales a su uso. Así que lo mejor era mostrar lo económicamente deseable como algo inevitable. En el credo de Mark Zuckerberg, la protección de datos personales su-

14 "Ya tenéis cero privacidad, olvidad el tema", *Sun on Privacy*, 26 de enero de 1999, en *http://www.wired.com/politics/law/news/1999/01/17538,* consultado en noviembre de 2013.

pone un anacronismo en el mundo global de *Internet* desde hace tiempo. Así, en febrero de 2010, a sus 26 años, Zuckerberg manifestaba que las personas se habían "acostumbrado a intercambiar más informaciones, de manera más abierta, de diferentes formas y con cada vez más personas". La oferta de *Facebook* pretendía con sus servicios e innovaciones estar a la altura de las circunstancias.[15] El concepto que tiene *Facebook* de la crítica quedó ilustrado en palabras de Richard Allan, director para Europa de esta empresa:

> Mark Zuckerberg tiene buen olfato para saber qué servicios querrá la gente en el futuro. A veces surgen protestas contra los cambios. Ha habido casos en los que millones de usuarios dijeron respecto a algunos cambios: por favor retírenlos. Pero hemos visto que, después de algún tiempo, la mayoría dice: así es mejor.[16]

Todavía más simple y llamativa es la filosofía de *Google*: "Don't be evil", o sea "no te enfades" o "no hagas algo malo". El equipo de *Google* explicó este principio de la siguiente forma: "En *Google* creemos que más información supone más posibilidad de elección, más libertad y, en definitiva, más poder para las personas".[17] El mensaje de empresas como *Google* y *Facebook* es que ellos son los buenos, hacen cosas buenas y que, especialmente a través de su participación en temas de responsabilidad, honestidad, democracia y transparencia en la sociedad, defienden los derechos civiles. Ante la grandeza y bondad de esos objetivos, hay que entender que infracciones contra anacrónicas normativas nacionales y europeas, son desde el punto de vista de una red de información global o, lo que para ellos es lo mismo, desde el punto de vista de estas empresas, aceptables e inevitables.

15 Adamek, *Die facebook-Falle*, 2011, S. 59.

16 Conversación con Lars Reppersgard, en Datenschutz, Hrsg. Schmidt/Weichert, 2012, S. 259

17 Reppesgaard, *Das Google Imperium*, 2008, S. 26; *cfr*. Rieschl, *Die Google Falle*, 2008, S. 16, pp. 19 y ss.

2. *La privacidad moderna*

El Tribunal Constitucional alemán y, siguiendo su jurisprudencia, los tribunales nacionales y la jurisprudencia europea tienen otro enfoque sobre este asunto. En la sentencia referente al censo poblacional emitida en 1984, el Tribunal Constitucional alemán sentó como consecuencia de la digitalización de nuestras vidas, un derecho fundamental a la autodeterminación informativa,[18] y en 2008 lo complementó con un derecho fundamental a la privacidad informática, así como el derecho a garantizar la integridad y confidencialidad de los sistemas informáticos.[19] No cabe alegar que se trata de resoluciones constitucionales pertenecientes a épocas predigitales, más bien, éstas decisiones jurisdiccionales son consecuencia directa de la revolución de las tecnologías de la información.

En los Estados Unidos, el hogar de *Facebook*, *Google* y compañía, la protección de datos tiene una importancia distinta de la que disfruta Alemania y la Unión Europea. Valga decir que no son objeto de este trabajo explicar las razones que han provocado que la protección de datos, cuyas raíces intelectuales están en los Estados Unidos, carezca de desarrollo alguno a nivel político y jurisprudencial desde hace decenas de años. Pese a ello, en ese país también se tiene un reconocimiento constitucional de la figura de "reasonable expectations of privacy".[20] Sin embargo, hay que considerar que las empresas estadounidenses de tecnologías de la información tienen en su país menos problemas legales en materia de privacidad que fuera de éste.

18 BVerfG, *NJW, Nuevo Semanario Jurídico*, 1984, pp. 419 y ss.

19 *Ibidem*, 2008, pp. 822 y ss.

20 Weichert, *RDV, Revista sobre Derecho del Tratamiento de Datos*, 2012, pp. 113 y ss.

IV. ¿El código es ley?

Tras el debate sobre el valor material de la privacidad se encuentra una cuestión que se plantea de forma reiterada como consecuencia del desarrollo tecnológico: ¿qué valor les corresponde a las leyes con legitimación democrática? Después de que algunos políticos descubrieran aterrorizados que algunas leyes, que podríamos calificar de analógicas, no eran apropiadas para el mundo digital, se apresuraron a afirmar que Internet no era un espacio sin ley.

A pesar de ello, los políticos no han encontrado una respuesta a la provocadora afirmación de las empresas de tecnologías de la información según la cual las normas político-sociales son fijadas por programas informáticos. En el año 2000, Lawrence Lessig afirmaba "Code is Law".[21] Tras esta breve afirmación se esconde como tremenda consecuencia que el legislador democrático debería apartarse en la materia de Internet y que las leyes no se hacen en los estrechos marcos o jurisdicciones nacionales. Más bien, las normas son programadas por las empresas de tecnologías de la información mediante estructuras reguladoras y ratificadas por el mercado global.

Por lo tanto, el legislador democrático tiene que ajustarse a las posibilidades tecnológicas existentes. Esto no debe significar en ningún caso que el desarrollo tecnológico se deje a merced del mercado y a sus anárquicos efectos, como sucede en la actualidad con *Facebook*, *Google* y compañía en materia de protección de datos. Para estas empresas lo relevante es el comportamiento de los consumidores, interpretado desde un concepto de bien común que cabría calificar de predemocrático. Un ejemplo clarificador lo encontramos en el proceso de votación de los usuarios establecido por *Facebook* para sus *Terms of Use* y *Privacy Policies*, es decir para sus normas de tratamiento de datos en forma de condiciones

21 *Code is law-On Liberty in Cyberspace*, en *http://harvardmagazine.com/2000/01/code-is-law.html*; Weichert, Gesetze, Geld und Gadgets, *https://www.datenschutzzentrum.de/vortraege/20120418-weichert-keynote.html.*

generales de contratación. Esas condiciones son fijadas de forma unilateral, presentadas a los usuarios para que las discutan y sean ratificadas en caso de que no exista un rechazo por parte de la mayoría de los usuarios.[22] En lugar del moderno concepto de democracia, que supondría un *Opt-in* colectivo, sólo está previsto un *Opt-out* colectivo, aunque en realidad es casi imposible alcanzar las cuotas previstas. El verdadero *Opt-out* sólo es posible mediante el comportamiento en el mercado, es decir, por medio de la decisión de un *click* que nos traslade a la competencia.[23] Con el procedimiento elegido por *Facebook* la empresa puede demostrar que ha consultado sus políticas con sus usuarios. Mientras tanto, a los especialistas y autoridades de protección de datos que exigen que se cumpla la normativa vigente se les responde de la siguiente forma: "¿Qué tiene usted contra *Facebook*? Todos los usuarios participan libremente".

V. La estrategia de comunicación

Facebook es un ejemplo paradigmático de estrategia de comunicación organizacional a corto y mediano plazo en cuanto a sus infracciones de la normativa de protección de datos. De hecho, reproduce la estrategia seguida por *Google* durante el tiempo en que hubo una gran inquietud respecto a *Google Search, Street View* y *Analytics*. Actualmente, *Facebook* concentra la atención pública y mediática, mientras *Google* sigue cometiendo sus infracciones sin sufrir sanción alguna. La finalidad de estas estrategias no es el cumplimiento de la normativa (*compliance*) sino el beneficio económico. Sólo de esta forma es comprensible que *Facebook* rompiera unas ya muy avanzadas negociaciones con el Grupo Hollzbrink para la compra de la red social *Studi VZ*, ya que dicha red

22 Sobre el tema Oberbeck, *Datenschutz Berater*, núms. 7 y 8, 2012, pp. 160 y ss.; ULD e Initiative Europe-v-Facebook, *DANA Revista de la Asociación para la Protección de Datos*, núm. 2, 2012, p. 72.

23 Reppesgaard, *Das Google Imperium*, 2008, pp. 245 y ss.

sí estaba obligada a cumplir con la legislación alemana en materia de protección de datos.[24]

1. *Ignorar*

En la fase inicial del conflicto sobre protección de datos personales, *Facebook* optó por desaparecer, o mejor dicho, por ignorar la existencia de ese problema. Esta decisión pudo deberse en parte a la escasez de personal dedicado y especializado en el tema, que hacía imposible mantener un nivel de comunicación adecuado con el resto de partes implicadas. Las reclamaciones de los afectados no recibían respuesta alguna o recibía respuestas basadas en formatos de respuesta ya establecidos vía correo electrónico. Las preguntas planteadas por autoridades de protección de datos también eran ignoradas, mientras no supusieran un riesgo de sanción directa.

2. *Comunicar*

El 19 de agosto de 2011, el *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (*ULD*), la Autoridad de Protección de Datos del *Land de Schleswig-Holstein*, hizo público un comunicado en el que llegaba a la conclusión que el uso de *Fan Pages* y *Social Plugins* por parte de entidades alemanas era ilegal y podía tener como consecuencia que:

> después del correspondiente trámite de audiencia y administrativo podía originar amonestaciones para las administraciones públicas, de acuerdo con lo previsto en el § 42 LDSG SH, y procedimientos de interdicción para las empresas privadas, según lo previsto en el § 38 Abs. 5 BDSG, así como sanciones económicas.[25]

24 Facebook kaufte Studi VZ nicht wegen Datenschutz, *DANA Revista de la Asociación para la Protección de Datos*, núm. 2, 2012, p. 76.

25 El ULD a los titulares de páginas web: "Facebook-Reichweitenanalyse abschalten", *DuD Revista dedicada a la Protección y Seguridad de los Datos*,

Este texto originó un intenso debate público, que tuvo como consecuencia que tres días más tarde *Facebook* mostrara una primera reacción y que el 25 de agosto del mismo año emitiera una primera respuesta al contenido del mencionado comunicado de la autoridad.[26] El 7 de septiembre de 2011, el *Policy-Chef* de *Facebook* visitó en Kiel tanto al ULD como a la Comisión de Justicia e Interior del Parlamento regional de Schleswig-Holstein, y un mes más tarde a la Subcomisión de Nuevos Medios del Parlamento alemán.

Los argumentos presentados fueron que las autoridades alemanas de protección de datos no eran competentes, y que la competencia le corresponde a la autoridad irlandesa, ya que la sede de la central europea de *Facebook* está en Dublín. Asimismo, se dijo que el alcance del análisis de la *web* que realiza *Facebook* (el cual se refiere a sus servicios de análisis, equivalentes, por ejemplo, a los de *Google Analytics*), tiene únicamente fines estadísticos, y es por lo tanto irrelevante en materia de protección de datos personales. En lo que afecta a los no usuarios de *Facebook*, las *cookies* no se utilizan para desarrollar un registro de personas, sino sólo "para apoyar la seguridad de la página *web*". Los habitantes de Schleswig-Holstein se encontrarían en una "situación extremadamente complicada" si no pudieran comunicarse con o a través de *Facebook*. Por lo tanto, el tratamiento de los datos de los usuarios de *Facebook* está legitimado por el consentimiento por ellos otorgado. Estos argumentos se presentaron mostrando gran interés y comprensión por la protección de datos y por las cuestiones planteadas por el ULD; sin embargo, *Facebook* es una empresa global y no puede someterse a innumerables normativas de protección de datos; pero desde luego existe una voluntad de diálogo sin barrera alguna.

2011, en *https://www.datenschutzzentrum.de/presse/20110819-facebook.htm*; el análisis técnico está disponible (en alemán) en *https://www.datenschutzzentrum.de/facebook/kommunikation/20110819.pdf*.

26 *https://www.datenschutzzentrum.de/facebook/kommunikation/20110825_Facebook_deutsch.pdf*.

En noviembre de 2011 *Facebook* se comprometió a proporcionar al ULD amplia documentación técnica que fue elaborada en el marco de la auditoría efectuada por la autoridad irlandesa de protección de datos. Dado que los argumentos presentados por *Facebook* no representaban ninguna voluntad de cambio y no refutaban las consideraciones jurídicas planteadas, el ULD mantuvo su valoración y siguió con el procedimiento iniciado.

3. *Remitir*

La caravana siguió su camino y la discusión había alcanzado ya nivel europeo. Después de una reclamación planteada por el estudiante vienés Max Schrems,[27] la autoridad irlandesa de protección de datos se ocupó de forma intensiva del tema *Facebook* y la empresa se limitó a hacer referencia al procedimiento de auditoría en curso. El informe de auditoría emitido en diciembre de 2011 es extremadamente moderado y no realiza ninguna valoración jurídica, limitándose a formular metas a alcanzar en materia de buenas prácticas.[28] Pese a nuevas reclamaciones, el ULD al día de hoy no ha recibido documentación alguna que permita realizar una valoración de la situación.[29]

La Conferencia Alemana de Autoridades de Protección de Datos a nivel federal y regional (*Düsseldorfer Kreis*) emitió a finales del 2011 un documento sobre comunidades sociales y envió un escrito a *Facebook* que incluía diferentes críticas. La respuesta de *Facebook* no asumía compromiso alguno, sino que se remitía a la auditoría irlandesa y consideraba que podía ser útil realizar una

27 Véase *http://europe-v-facebook.org/DE/de.html*.

28 *https://www.datenschutzzentrum.de/presse/20111222-facebook-irland.htm*; Eiermann, *DANA, Revista de la Asociación para la Protección de Datos*, núm. 2, 2012, pp. 53 y ss.; informe de auditoría en *http://www.europe-v-facebook.org/Facebook_Ireland_Audit_Report_Final.pdf*.

29 Posteriormente a la elaboración de este trabajo, la autoridad irlandesa de protección de datos emitió un nuevo informe, que sigue sin entrar en el fondo de la cuestión. El documento está disponible en *http://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf*.

visita a *Facebook* y su equipo en Irlanda. El entonces nombrado director de *Public Policy* en Alemania, Gunnar Bender, dedicó el verano de 2012 a un "*Tour* de DPA" (*Data Protection Authority*).

4. *Siempre ser amistoso*

Facebook, a diferencia de otras grandes empresas en Alemania, no se enfrentó al ULD con amenazas abiertas. Tampoco intentó que se iniciara una vigilancia o control del ULD a nivel parlamentario, jurídico o de cualquier otro tipo. Puede que esta actitud estuviera motivada por la agresiva campaña de relaciones públicas llevada a cabo por el ULD. Otra posible causa puede ser que el ULD implicara por iniciativa propia al Gobierno y al Parlamento y, además, a los ministerios del interior y de presidencia de *Schleswig-Holstein* que fueron objeto de procedimientos de control y de amonestaciones por parte del ULD. *Facebook* tampoco recurrió a plantear posibles reclamaciones de daños y perjuicios por cantidades exorbitantes, como intentaron otras empresas sometidas a controles en materia de protección de datos. *Facebook* se mantuvo, tanto en el tono como en las formas, servicial y amistosa, sin proporcionar ninguna información que permitiera un control jurídico adecuado de la situación.

VI. En ningún caso aportar aclaraciones jurídicamente vinculantes

La estrategia central de *Facebook* consiste en evitar una aclaración jurídicamente vinculante o, como mínimo, trasladarla a un futuro lo más lejano posible. La empresa se ha visto favorecida por el hecho de que la autoridad irlandesa de protección de datos, competente para la sede europea de *Facebook*, hasta ahora no ha buscado esa aclaración jurídicamente vinculante. De hecho, el control de la implementación de la auditoría elaborada en Irlanda debía haberse llevado a cabo en julio de 2012, y hasta ahora sólo se han emitido recomendaciones sin que se haya producido san-

ción alguna. Según parece, la autoridad irlandesa de protección de datos no acostumbra imponer sanciones, tradición desarrollada en Alemania a partir de los años noventa. La autoridad irlandesa de protección de datos dispone de escasos recursos, tanto en cuanto al personal como en otros niveles. A la vista de esa situación, la mera elaboración del informe de auditoría supone una tarea de proporciones descomunales. Cabe recordar que Irlanda requiere de los puestos de trabajo y los impuestos que pagan las empresas de tecnologías de la información que se instalaron en ese país, especialmente debido a las condiciones favorables que les fueron ofrecidas.

Por lo que respecta al ULD el objetivo era —y sigue siendo— alcanzar una sentencia judicial. Por ese motivo, el ULD no permitió que ofertas o anuncios sobre posibles nuevas rondas de diálogo le desviaran del procedimiento planeado. A pesar de ese procedimiento, los efectos se van mostrando sólo muy lentamente.

1. *Sector público*

En el sector público, el ULD, después de las audiencias anunciadas, procedió a emitir las amonestaciones previstas en el § 42 Abs. 2 LDSG SH.[30] Después de que las irregularidades no se subsanaran, el ULD contactó a los ministerios competentes como instancias de control jurídico. Esos ministerios se negaron a efectuar su labor de control alegando que la situación legal no estaba clara; cabe mencionar que algunos de esos ministerios habían sido objeto de amonestaciones por parte del ULD. Como consecuencia de esta situación, el ULD se dirigió al Parlamento regional como órgano de control parlamentario.[31] La Comisión de Interior y Justicia de ese parlamento fue informada por el Ministerio del Interior de que los ministerios de presidencia de las diferentes re-

30 Weichert, *DuD Revista dedicada a la Protección y Seguridad de los Datos*, 2012, p. 6.

31 *https://www.datenschutzzentrum.de/presse/20111213-facebook-landtag.htm*.

giones habían solicitado un dictamen sobre el tema a la Conferencia de Ministros del Interior, mismo que debía ser presentado en diciembre de 2011. Ese documento, que debía ser preparado por el Ministerio del Interior de Baviera, seguía sin haber sido presentado en julio de 2012. Sin disponer del mencionado dictamen, la Comisión de Interior y Justicia del Parlamento regional consideró que no podía llevar a cabo valoración alguna. Por lo tanto, la reclamación que el ULD dirigió al Ministerio de Presidencia y a la Cámara de Industria y Comercio para que presentaran una demanda declarativa contra el ULD, a efecto de conseguir una aclaración rápida de la situación, fue rechazada. El Parlamento y las instituciones responsables del control, en principio obligados a cumplir con la legalidad, se negaron por lo tanto a tomar posición en el tema, permitiendo que se siguieran produciendo infracciones. De esta forma, las posibilidades de actuaciones legales del ULD como autoridad de protección de datos quedaban agotadas.

2. *Sector privado*

Después de nueve procedimientos sobre el uso ilegal de *FanPages* de *Facebook*, en los que estaban implicadas nueve grandes empresas, se emitieron tres órdenes de prohibición de acuerdo con lo previsto en el § 38 Abs. 5 BDSG, contra las cuales se presentaron en diciembre de 2011 recursos de anulación ante el Tribunal de lo Contencioso (*Verwaltungsbericht*) *Schleswig*. Anteriormente, parlamentarios del FDP (Partido Liberal Alemán), tanto a nivel federal como regional habían encargado a los servicios de sus parlamentos dictámenes que estudiaran la crítica valoración del ULD.[32] Al mismo tiempo, varios parlamentarios regionales intentaron convencer al ULD para que no tomara las medidas legales previstas en materia de protección de datos, por considerar que esas medidas podrían tener efectos negativos a ni-

32 Landtag Schleswig-Holstein, en *http://www.landtag.ltsh.de/infothek/wahl17/umdrucke/2900/umdruck-17-2998.pdf*, Bundestag, *https://www.datenschutzzentrum.de/facebook/material/WissDienst-BT-Facebook-ULD.pdf.*

vel de competitividad para la economía de la región de *Schleswig-Holstein*.[33] El ministro del interior del gobierno federal afirmó, pese a no ser un tema de su competencia, después de una conversación con Richard Allan, representante de *Facebook*, que "la discusión sobre si la normativa alemana en materia de protección de datos y telemedios era aplicable a *Facebook* o no" quedaba desactivada, después de que Allan declarara que iba a apoyar iniciativas de autorregulación en la red social.[34] El presidente de la Cámara de Industria y Comercio de *Schleswig-Holstein*, durante la reunión anual de esa institución, se mostraba molesto con las iniciativas del ULD para aclarar la situación y tomar las medidas necesarias.[35] La mencionada Cámara publicó un dictamen que había encargado sobre el tema, el cual, como los documentos de igual tipo emitidos por los servicios parlamentarios, exponía los mismos razonamientos jurídicos que el ULD, pero intentaba relativizar las consecuencias legales.[36]

Los procesos en el ámbito de lo contencioso, pese a que las cuestiones planteadas eran muy claras, permanecieron bloqueados durante meses, en un caso medio año, de forma que al día de hoy no se ha fijado fecha para el juicio. Como consecuencia, ha pasado más de un año desde que el ULD tuvo constancia de la existencia de infracciones en materia de protección de datos, sin que se haya dado paso alguno en el tribunal de primera instancia y, por lo tanto, sin que se haya producido cambio alguno en la situación. Si se tuviera que llegar a la última instancia en el Tribunal Federal de lo Contencioso (*Bundesverwaltungsgericht*) —como cabe esperar, ya que ninguna de las partes en litigio va a ceder en sus pretensiones— se tardarían años, durante los cuales

33 *https://www.datenschutzzentrum.de/presse/20110907-facebook-muss-sich-gewaltig-bewegen.htm*.

34 *https://www.datenschutzzentrum.de/presse/20110908-innenminister-facebook.htm*

35 *https://www.datenschutzzentrum.de/presse/20120112-ihk.htm*.

36 Weichert, *DANA, Revista de la Asociación para la Protección de Datos*, núm. 1, 2012, pp. 18 y ss. *https://www.datenschutzzentrum.de/facebook/20120222-web20 -in-verwaltung.html*.

el modelo de negocio basado en la infracción de la normativa de protección de datos seguirá funcionando y generando beneficios.

Otros procedimientos disponibles en el ordenamiento jurídico alemán, como la imposición de multas económicas o una orden de ejecución inmediata, no van a ser utilizadas por el ULD. La posibilidad de acudir al Juzgado de Primera Instancia (*Amtsgericht*) o de iniciar acciones penales queda fuera de las competencias del ULD, siendo responsabilidad de los mencionados juzgados o de la Fiscalía, y plantea cuestiones sobre el hecho subjetivo (dolo o negligencia de los responsables de las *Fan-Pages*) y desplaza el tema de la discusión de la legalidad del tratamiento de datos a la legalidad de la sanción. La orden de ejecución de la resolución prevista en el § 38 Abs. 5 BDSG, de acuerdo con lo previsto en el § 80 Abs. 2 Nr.4 VwGO, sería difícil de fundamentar mientras miles de *Fan-Pages* sigan funcionando sin que nadie haga nada al respecto.

VII. Conclusiones

Mientras a nivel social no se produzca una condena al ostracismo, la sombra de la ilegalidad en materia de protección de datos no supondrá un motivo para dejar de llevar a cabo prácticas beneficiosas desde el punto de vista económico. Hasta ahora *Facebook* ha conseguido evitar la mencionada condena. Desde el presidente de los Estados Unidos, Barack Obama, hasta el alcalde de Hamburgo, Olaf Scholz,[37] los políticos se sitúan bajo el brillante sol del progresismo y el éxito económico que *Facebook* representa. De vez en cuando la imagen de esta red social sufre debido a las ilegalidades, desfachateces y arbitrariedades que comete, por ejemplo cuando decide desconectar las *Fan-Pages* de

37 Bürgermeister Scholz für Facebook und gegen Verbraucherdatenschutz, *DANA, Revista de la Asociación para la Protección de Datos*, núm. 2, 2012, p. 79.

algunos ayuntamientos,[38] o cuando anima a algunos "amigos" a proporcionar los nombres de usuarios que utilizan seudónimos,[39] o cuando las direcciones de correo electrónico, propias y ajenas, de usuarios son modificadas, de forma que muchos correos se pierden.[40] Pero el prestigio sólo se ve reducido mínimamente. El reconocimiento por parte de políticos, empresas y la administración se mantiene, en parte por la inmensa cantidad de información y comunicación ofertada, al menos en apariencia, sin coste alguno de la que se pueden beneficiar esos grupos. En un Estado de derecho, que tiene como uno de sus pilares básicos la autodeterminación informativa, incluso algunas escuelas y cuerpos de seguridad, con funciones pedagógicas y de mantenimiento del orden respectivamente, olvidan la heteronomía y el incumplimiento de la ley, mientras parece que la posible utilidad a obtener brilla más que esos otros conceptos.

Hay motivos para considerar que el modelo de negocio basado en las infracciones de la normativa de protección de datos no es sostenible. Mientras pueda seguir presumiendo de moderno y progresista y no lleve la marca de la ilegalidad en la frente, seguirá funcionando. Por eso *Facebook* mantendrá la imagen del "amigo" mientras pueda. Eso dejará de funcionar cuando la ilegalidad quede comprobada (quizás en la última instancia judicial) y cuando se haga público el daño que *Facebook* infringe a los valores sociales. En ese momento puede ser que las masas se busquen otra plataforma de comunicación y que la utilidad económica de *Facebook* se quiebre. *Google* demuestra hasta el día de hoy cómo se puede evitar la llegada de ese momento por medio de mínimas concesiones y sin renunciar a las bases del modelo de negocios.

38 Staudinger, Niemandsland, *SZ, Süddeutesche Zeitung*, del 28 de junio de 2012, p. 10.

39 Kuhn, en *http://www.sueddeutsche.de/digital/verwendung-von-pseudonymen-facebook-fragt-nutzer-ueber-freunde-aus-1.1406925*, Lischka/Reißmann, en *http://www.spiegel.de/netzwelt/netzpolitik/pseudonyme-facebook-nutzer-sollen-freunde-verpetzen-a-843326.html*

40 Facebook macht Fehler, *c't, Revista sobre Técnica Informática*, núm. 16, 2012, p. 52.

Es de temer que en el caso de *Facebook* tampoco se produzca ninguna depuración.

Por parte de la política en Alemania no cabe esperar ayuda alguna. A nivel europeo se está debatiendo desde enero de 2012 un nuevo Reglamento de Protección de Datos. En ese Reglamento se plantean reformas que podrían poner fin al modelo de negocios de *Facebook*: mecanismos de sanción más rápidos, decisivos y efectivos para las autoridades de protección de datos, los usuarios y sus asociaciones. La Comisión Europea reconoce algo que la jurisprudencia alemana ha negado hasta ahora, la protección de datos como instrumento de regulación del mercado. Aparte de eso, también en Europa el debate social es una condición fundamental para conseguir estructuras esenciales a nivel social, jurídico, técnico y organizacional que permitan la puesta en práctica de la autodeterminación informativa.

1. *Actualización (febrero 2013)*

Después de que tanto *Facebook Inc*. (Estados Unidos) como *Facebook Ltd*. (Irlanda) se negaran a permitir el uso de pseudónimos en cuentas de su red social, segun lo exige la Ley de Telemedios alemana (TMG) y como le solicitó el *Unabhängiges Landeszentrum für Datenschutz* (ULD), Autoridad de Protección de datos *Schleswig-Holstein* con base en reclamaciones planteadas por personas afectadas, el ULD emitió una orden administrativa exigiendo a ambas empresas la ejecución inmediata de la orden.

En una declaración *Facebook* expuso su opinión sobre los puntos esenciales en este tema, que es diametralmente opuesta a la del ULD y a la de otras autoridades de protección de datos en Alemania:

- Para el procesamiento de datos de *Facebook,* el único responsable es *Facebook Ltd*. en Irlanda y no la empresa principal en Estados Unidos, que únicamente procesa datos por encargo de su filial.

- *Facebook Ltd.* cumple la legislación irlandesa de protección de datos que es una implementación completa de la europea en la materia.
- El punto anterior fue confirmado por la auditoría llevada a cabo por la autoridad irlandesa de protección de datos y publicada en septiembre de 2012.
- Lo previsto en el § 13 Abs. 6 TMG no es aplicable a *Facebook*, y además infringe normativa europea de rango superior.
- El objetivo de la cultura de *Facebook* en materia de uso del nombre verdadero es generar confianza y seguridad.
- Incluso en el caso de que el § 13 Abs. 6 TMG fuera aplicable, el abandonar su política de uso de los nombres verdaderos no sería aceptable para *Facebook*.

La posición del ULD y las órdenes emitidas se pueden resumir en los siguientes puntos:

- *Facebook Inc.* y *Facebook Ltd.* son responsables solidarios de la política de uso de nombres verdaderos de *Facebook* y ambos pueden ser considerados responsables en terminos legales.
- El ULD es la autoridad responsible del cumplimiento de la normativa de protección de datos por parte de *Facebook* en lo que afecta a los ciudadanos de *Schleswig-Holstein*.
- *Facebook* debe cumplir lo previsto en el § 13 Abs. 6 TMG, que está en línea con lo previsto en la legislación europea y protege el ejercicio de los derechos fundamentales en general y de la libertad de expresión en Internet. El legislador ha dejado claro que los usuarios de *Facebook* y de otros servicios en Internet deben serlo de forma anónima y sin necesidad de temer consecuencias negativas.
- Permitir usar los servicios de *Facebook* de forma anónima es razonable. La obligación de usar nombres verdaderos no evita el mal uso del servicio para insultos o provocaciones

y tampoco permite prevenir el robo de identidades. A tal fin deben tomarse otras precauciones.

- Para garantizar los derechos de los usuarios y la normativa de protección de datos en general, *Facebook* debe abandonar su política de obligar al uso de los nombres verdaderos.

Thilo Weichert, director del ULD, ha explicado:

> Es inaceptable que un portal estadounidense como *Facebook* viole la legislación alemana de protección de datos y sin que se pueda prever un final de esa situación. El objetivo de las órdenes del ULD es conseguir que de una vez por todas se aclare la situación legal sobre quién es responsable por las actividades de *Facebook* y cuáles son las obligaciones que debe cumplir esta empresa. En realidad ese debería ser también el interés de la empresa. Esperamos que *Facebook* trate este tema de forma profesional y no se limite a intentar dejar pasar el tiempo. Teniendo en cuenta que *Facebook* impide a sus usuarios decidir si quieren ser localizables con su nombre legal, creemos que nuestra iniciativa es especialmente importante.

El Tribunal Administrativo de Schleswig emitió el 14 de febrero de 2013 dos resoluciones en el proceso abierto por *Facebook Inc.* y *Facebook Ltd.* contra el ULD, en las que decide que la única filial de *Facebook* en Europa es *Facebook Ltd.* en Irlanda y por lo tanto también en Alemania debería aplicarse el derecho irlandés. Las órdenes emitidas por el ULD, ya mencionadas en este documento, exigiendo el desbloqueo de las cuentas de ciudadanos de Schleswig-Holstein que habían sido bloqueadas debido a no haber incluido el nombre verdadero o no haberlo hecho de forma completa al registrarse, son rechazadas por el Tribunal. Hay que recordar que la política seguida por *Facebook* en esta materia es claramente contraria a lo recogido en el § 13 Abs. 6 TMG. En el derecho irlandés no existe ninguna regulación expresa sobre uso en formato anónimo o por medio de pseudónimos en telemedios. El ULD hace referencia al derecho alemán.

De acuerdo con la resolución del Tribunal de Schleswig, el derecho aplicable es el irlandés, y no el alemán, pese a que todo el tráfico de datos de *Facebook* con la consiguiente elaboración de perfiles tiene lugar en Estados Unidos. Para el Tribunal, carece de relevancia que *Facebook* tenga una filial en Alemania, *Facebook Germany GmbH.* También carece de relevancia que la mayoría de contenidos no sólo sean captados en Alemania, sino que también son almacenados y tratados por la empresa Akamai.

El director del ULD, Thilo Weichert, comentó sobre las resoluciones:

> Las resoluciones son desconcertantes y van más allá de lo expuesto por *Facebook* en el sentido que el derecho alemán no es aplicable, porque *Facebook Inc.* sólo es el encargado del tratamiento de *Facebook Ireland Ltd.* Son contradictorias en sí mismas, ya que al mismo tiempo fundamentan la falta de relevancia jurídica de *Facebook Germany* porque no trata ningún tipo de datos y afirman que la empresa en Irlanda es responsable pese a que tampoco trata dato alguno. Las resoluciones del Tribunal Administrativo de *Schleswig* tendrían como consecuencia que una regla del *One-stop-shop*, como está prevista en la propuesta de Reglamento Europeo de Protección de Datos, junto con un elaborado sistema de colaboración entre las autoridades de protección de datos, no sería necesaria para grandes empresas TIC. Bastaría con organizar la estructura de la empresa tal como ha hecho *Facebook*, declarando responsable a una filial con sede en un país de la UE con un nivel bajo de protección de datos. Este no era el espíritu de la legislación de la UE.

Por todo lo expuesto, el ULD recurrirá las resoluciones del Tribunal Administrativo de Schleswig ante el Tribunal Superior Administrativo de Schleswig-Holstein.

2. *Actualización (noviembre 2013)*

El Tribunal de lo Contencioso (*Verwaltungsgericht*) de Schleswig emitió sentencia referente al tema que nos ocupa el 9 de octubre.

La sentencia decide que las empresas y administraciones públicas de Schleswig-Holstein pueden utilizar los servicios de *Facebook*. El ULD ha emitido un comunicado de prensa en el que anuncia que ha presentado recurso contra la mencionada sentencia, afirmando además que piensa agotar todas las instancias posibles y necesarias, incluyendo al Tribunal Superior de Justicia de la Unión Europea, ya que el problema planteado y su solución en un sentido o en otro es esencial para el desarrollo de la normativa europea de protección de datos.