XIX Edición del Premio Protección de Datos Personales de Investigación
de la Agencia Española de Protección de Datos

PREMIO 2015

La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)

Amaya Noain Sánchez

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

BOLETÍN OFICIAL DEL ESTADO
MINISTERIO DE LA PRESIDENCIA

LA PROTECCIÓN DE LA INTIMIDAD Y VIDA PRIVADA EN INTERNET: LA INTEGRIDAD CONTEXTUAL Y LOS FLUJOS DE INFORMACIÓN EN LAS REDES SOCIALES (2004-2014)

LA PROTECCIÓN DE LA INTIMIDAD Y VIDA PRIVADA EN INTERNET: LA INTEGRIDAD CONTEXTUAL Y LOS FLUJOS DE INFORMACIÓN EN LAS REDES SOCIALES (2004-2014)

Amaya Noain Sánchez

Premio Protección de Datos Personales de Investigación 2015

Agencia Española de Protección de Datos

Agencia Estatal Boletín Oficial del Estado

Madrid, 2016

NIPO: 007-16-101-3
ISBN: 978-84-340-2311-6
Depósito Legal: M-16327-2016

IMPRENTA NACIONAL DE LA AGENCIA ESTATAL
BOLETÍN OFICIAL DEL ESTADO
Avda. de Manoteras, 54. Madrid 28050

A mi padre Ricardo,
por enseñarme a disfrutar del cine, la música
y las nuevas tecnologías, entre otras muchas cosas.

A mi apreciado «círculo íntimo».

Índice

PARTE II
MARCO CONCEPTUAL Y ACLARACIÓN DE TÉRMINOS

PARTE V
CONCLUSIÓN DE LA INVESTIGACIÓN

Lista de figuras y tablas

PRÓLOGO

La promoción y el impulso de la investigación sobre el derecho fundamental a la protección de datos es uno de los objetivos del Premio Protección de Datos Personales en la modalidad de Investigación, un galardón que la Agencia Española de Protección de Datos comenzó a convocar en 1997. En esta XIX edición (2015), el jurado, compuesto por los miembros del Consejo Consultivo de la Agencia, decidió otorgar el premio al trabajo *La protección de la intimidad y vida privada en Internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014),* de Amaya Noain Sánchez.

Las redes sociales se han convertido en una herramienta de comunicación y contacto habitual para millones de personas en todo el mundo. De hecho, se calcula que más de un 75% de las personas que se conectan habitualmente a Internet cuentan con al menos un perfil en una red social. La autora plantea en el texto si las empresas propietarias de estos servicios ofrecen una información suficiente a los usuarios sobre qué datos recogen, para qué los van a utilizar y si van a ser cedidos a terceros. En una reflexión posterior, propone como posibles soluciones el hecho de que estas empresas pudieran implantar directrices técnicas compartidas y una adaptación normativa, fundamentalmente con la privacidad desde el diseño, la privacidad por defecto y el consentimiento informado. Así, el resultado sería un sistema de información por capas, en el que el usuario fuera conociendo gradualmente las condiciones del tratamiento de su información personal.

El trabajo explica el funcionamiento de una red social, comenzando por la creación del perfil de usuario en el que se suministran datos, y analiza cómo la estructura del negocio está basada en la monetización de los datos personales, con sistemas como el *targeting* (catalogando al usuario según sus intereses, características y predilecciones) y el *tracking down* (cruzando información dentro y fuera de la red). La autora distingue entre intimidad y vida privada, introduciendo conceptos como TIC, Internet, sociedad de la información, web 2.0 y redes sociales, con la teoría de los seis grados de separación y sus características, historia y orígenes. Plantea la evolución de la distinción

entre espacio público y privado, y la relatividad de las teorías actuales, estudiando también la evolución del comportamiento de los usuarios y hasta qué punto pueden estos desarrollar estrategias de autoprotección.

Las empresas y organizaciones tienen unas obligaciones para con los ciudadanos que están recogidas en la legislación de protección de datos, y estos pueden acudir a la Agencia cuando consideren que el tratamiento de sus datos no ha sido adecuado. La Agencia está apostando de manera decidida para que aquellos que tratan datos adquieran un compromiso con la transparencia, una responsabilidad que sin duda se vería recompensada con una mayor confianza por parte de sus usuarios. Esa transparencia implica, entre otras decisiones, informar huyendo de tecnicismos, ofreciendo la información de una manera clara, concisa y sencilla, y dando herramientas y posibilidades a los ciudadanos para que estos puedan ejercer el control sobre su propia información personal. En paralelo al trabajo con las empresas, la AEPD también está desarrollando y participando en diferentes proyectos de concienciación cuyo núcleo es la protección proactiva del propio usuario, explicando al ciudadano qué puede hacer por sí mismo para proteger su privacidad. Estudios como el que leerá a continuación ponen de manifiesto la necesidad de que la Agencia trabaje en diferentes frentes, con empresas y organizaciones, por un lado, y con los ciudadanos, por otro. Sólo así se podrá conseguir una protección eficaz de este derecho fundamental.

Mar España Martí
Directora de la Agencia Española
de Protección de Datos

AGRADECIMIENTOS

Cualquier experiencia vital —y escribir una investigación de este calibre sin duda lo es— se torna incompleta si no es compartida. Este no es el caso. En la elaboración del presente estudio he tenido la inmensa suerte de contar con el apoyo de las siguientes personas e instituciones, a las cuales quiero mostrar mi profunda gratitud.

En primer lugar, a la Universidad Complutense de Madrid por acoger esta investigación y, más en concreto, a todos los profesionales que trabajan en la Facultad de Ciencias de la Información.

A los investigadores del Institut für Kulturanthropologie und Europäische Ethnologie de la Goethe-Universität Frankfurt am Main. Especialmente a Petra Ilyes, Manfred Faßler, Martin Deschauer, Kevin Hall, Franziska Sperling, Alexander Schwinghammer, Laura Kocksch y Andreas Kramm por la confianza depositada en mis líneas de investigación desde el primer momento.

Al Fraunhofer-Institut für Sichere Informationstechnologie (SIT) de Darmstadt y, en particular, a Andreas Poller por permitirme colaborar en algunas de las investigaciones que esta prestigiosa entidad lleva a cabo, experiencia que me ha servido para aplicar mucho de lo aprendido a mis escritos.

Un agradecimiento más que merecido le debo al equipo de la Biblioteca de Ciencias de la Información por su inestimable ayuda a la hora de asesorarme en mis búsquedas de fondos bibliográficos.

No puedo olvidar, del mismo modo, la inestimable ayuda de Janice Mcpherson y Simon Hughes, sin cuyo soporte no me hubiera podido enfrentar a muchos de los textos que aquí se dan cita.

Igualmente, y aunque no ha tenido que ver directamente en la consecución de este trabajo, a David Robert Jones por acompañarme con sus canciones desde que tengo uso de razón e inspirarme en muchos de los temas que aquí se dan cita.

Y en mayúsculas, quiero destacar el sostén de mi propio *círculo íntimo:* mi familia, pilar maestro de mi existencia y sin cuyo ánimo estas páginas no hubieran abandonado su inicial estadio de ensoñación.

RESUMEN

Objetivo: La presente tesis explora las actuales preocupaciones relativas a las intromisiones en la intimidad y vida privada de las personas producidas en los entornos digitales, concretamente, en las redes sociales. Con el objetivo de entender y explicar los principales riesgos en el uso de estos servicios de Internet, se pretende identificar y evaluar los flujos de información y la transferencia de datos personales que tienen lugar en dichos entornos. Asimismo, tras reseñar los problemas a los que habitualmente se enfrentan los usuarios para preservar, activamente, su esfera privada, se aporta una propuesta destinada a solventar dicha situación de vulnerabilidad, luchando contra la desinformación imperante en estos novedosos contextos. Subrayamos así, el papel esencial que ostenta el conocimiento, no solo para prevenir las citadas injerencias, sino para posibilitar que los individuos ejerzan su autodeterminación informativa.

Diseño/Metodología/Aproximación: En nuestro estudio haremos uso de las técnicas de análisis de contenido y comparativo aplicadas a una muestra de los más relevantes artículos e informes científicos relativos a las interacciones entre tecnologías digitales de la Web 2.0 e intimidad y vida privada (existe una cantidad creciente y substancial de literatura que aborda la confrontación entre ambas variables). Ulteriormente, mediante el marco teórico de la «integridad contextual» aportado por Helen Nissenbaum, evaluaremos cómo la naturaleza de la Web 2.0 cambia la ecuación de lo público y lo que se considera privado. A través de las lentes de esta aproximación, analizaremos los flujos de información que se ocultan bajo la estructura de las herramientas de la Web 2.0, centrándonos, primordialmente, en la red social Facebook.

Hallazgos/Resultados: Las principales contribuciones de nuestro estudio se resumen en dos. En primer lugar, se consigue ilustrar el papel esencial que ostenta el conocimiento en la propia protección que los usuarios ejercen sobre sus informaciones privadas, un factor capaz de ayudarles a tomar decisiones críticas y conscientes en lo que respecta a la preservación de su ámbito privado. Como segundo aporte, destacamos la presentación de una serie de recomendaciones, así como la propuesta de un sistema creado para proporcionar a los indi-

viduos ese flujo de información necesario para satisfacer sus deseos de autodeterminación informativa, sin que dejen de usar las redes sociales por miedo a ver su ámbito reservado comprometido.

Originalidad/valor: Junto con las conclusiones, presentaremos una proposición sobre cómo aportar a los interactores de las tecnologías esa información que requieren para entender los contextos digitales. Para ello, presentaremos algunas recomendaciones centradas en posibles mejoras, subrayando especialmente la importancia de implementar medidas educativas así como otros instrumentos técnicos tales como la protección «desde el diseño/por defecto» y el «consentimiento informado». La introducción de la protección «desde el diseño» o «por defecto», junto con la implementación del «consentimiento informado» puede prevenir muchas de las injerencias que los sujetos experimentan en estos escenarios, prioritariamente, en las redes sociales. Por dicho motivo, en nuestra propuesta final consideraremos la introducción de dicho consentimiento, aunque redefinido bajo nuevas condiciones. Así presentaremos el «consentimiento informado activo («*Opt-in*» *model*) por capas». Los regímenes *«opt-in»* ya han sido aplicados a las *cookies*, pero nunca a otros servicios de la Web 2.0 como, por ejemplo, las citadas redes sociales.

Palabras Clave: Intimidad y vida privada, Redes sociales, Internet, Integridad contextual, Consentimiento informado, Web 2.0, Tecnologías de la Comunicación y la Información (TIC) Flujos de información, Esfera privada.

ABSTRACT

Purpose: This dissertation explores present day concerns about privacy breaches on digital environments. In order to examine the main risks the Internet may involve for our private sphere, it identifies and evaluates the information flows and personal data transfer behind the visible structure of Web 2.0 services, focusing on Social Networks Sites (SNS). Additionally, the essay lays out an alternative approach to addressing the problem of privacy protection underlining the essential role played by user's knowledge in order to both prevent infringements and make them capable of exercising their right for informational self-determination.

Design/Methodology/Approach: We arrive at this point in our study by comparative and content analysis of the most relevant scientific papers and dossiers relating to personal data protection –There is a growing and substantial literature that confronts privacy issues raised by the development and general dissemination of Web 2.0. Subsequently, by using Nissenbaum's «contextual integrity» framework we evaluate how the nature of Web 2.0 and data sharing on SNS changes the privacy equation. Following, through the lenses of this benchmark we analysis the flows of information which make up each specific context, especially pointing at SNS Facebook.

Findings: The goal of this paper is twofold. The first finding is to illustrate the fact that users' knowledge is a key concept not only to prevent privacy breaches from taking place, but to become people more capable of making conscious decisions as far as their data preservation is regarded. The second goal is to introduce a system of «informed consent» redefined under new conditions, in such a way that users are able to obtain the basic information they may need to satisfy their desires for data protection and, at the same time, their requirements for social interaction on SNS.

Originality/value: In the final chapter, we make some recommendations for improvements and place emphasis on the importance of improving educational measures and an updated legislation, as well as technical implementations such as «privacy by design». Finally, together with suggestions we present a proposal on a new model of

«informed consent» aim to supply users with information to ensure they understand how their data will be shared or if their contents are visible to others. For this purpose, we put forward the implementation of «informed consent» redefined as «Opt in» or active model by layers –«Opt in» regimens have already been applied to cookies but never to 2.0 applications such as SNS. We expect the implementation of «privacy by design» working in conjunction with «informed consent» to prevent people from suffering much of the violations of privacy they experiment on SNS.

Keywords: Privacy, Social Networks Sites (SNS) Internet, Contextual Integrity, Informed Consent, Web 2.0, Information and Communication Technologies (ICT) Information Flow, Private Sphere.

INTRODUCTION

The widespread adoption of the Internet, especially as far as some Web 2.0 services is regarded has led many scholars[1], as well as the mass media to examine and raise pragmatic concerns about the disclosure of private information associated with participation on the digital environment. Particularly, it is the issue of privacy protection on the Internet which has received considerable attention since the increased collection of personal data online and the enhanced capabilities for searching, tagging and aggregating this information it provides. As Professor Helen Nissenbaum states:

> As adoption of the Internet and Web has surged and as they have become the primary sources of information and media for transaction, interaction, and communication, particularly among well off people in technologically advanced societies, we have witnessed radical perturbations in flows of personal information[2].

---

1 See: GROSS, R. and ACQUISITI, A. (2005): «Information revelation and privacy in online social networks», in *Proceedings of ACM Workshop on Privacy in the Electronic Society'05*, New York: ACM Press, pp. 71-80; BARNES, S. B. (2006): «A privacy paradox: social networking in the United States», in *First Monday*, vol. 11, n. 9; GOVANI, T. and PASHLEY, H. (2005): «Student awareness of the privacy implications when using Facebook», in *Privacy Poster Fair at the School of Library and Information Science*, Pittsburgh: Carnegie Mellon University; YOUNG, A. L. and QUAN-HASSE, A. (2013): «Privacy protection strategies on Facebook», in *Information, Communication and Society*, vol. 16, n. 4, pp. 479-500; MADDEN, M. and SMITH, A. (2010): «Reputation management and social media» in *Pew Internet & American Life Project*, Washington; LENHART, A. and MADDEN, M. (2007): «Teens, privacy & online social networks: how teens manage their online identities and personal information in the age of MySpace», in *Pew Internet & American Life Project, Washington, DC.*; DEBATIN, B., *et al.* (2009): «Facebook and online privacy: attitudes, behaviours, and unintended consequences», in *Journal of Computer-Mediated Communication*, vol. 19, n. 2, pp. 83-108.

2 NISSENBAUM, H. (2011): «A Contextual Approach to Privacy Online», in *Daedalus*, vol. 140, n. 4, pp. 32-48, p. 33. Helen NISSENBAUM is Professor of Media, Culture and Communication, as well as Senior Fellow in the Information Law Institute at New York University.

This is not a minor issue, particularly taking into account that digital infrastructures are invisible and ubiquitous but are embedded in everyday life of people. Additionally, as a public good, Internet and the correct use of Information and Communication Technologies (ICT) become crucial to ensure the correct development of a democratic society

Nevertheless, it is currently highly complicated for users to receive suitable information about which of their personal data are being storing by ICT and which principles are being used for processing them and passing them on to third parties. In conjunction with the information that they knowingly provide to the Internet services, users leave many traces behind which they might not be conscious of. Furthermore, once all of these data have been gathered, new technology can be applied to them in order to obtain and extrapolate supplementary information. Yet again, this is a process that users are not always aware of[3]:

> This can lead to the danger of decontextualisation; where personal data are used in contexts that their owners would not agree to if they knew about it. In addition to decontextualisation, there is also the danger of persistence, where personal data are held for longer than necessary. Users do not always know what happens to their data once it is no longer needed for a particular service. […] This is where the third danger of re-identification comes in. It is now possible to use advanced analysis techniques to reassign many anonymous records to individuals[4].

In this respect, we try to draw a correlation between the flow of information users receive —and are capable of fully understanding— and their chances to have their personal content protected. Accordingly, we can state the following hypothesis: «The respect of a correct flow of information may help users to maintain a desirable grade of autonomy as far as their privacy is concerned, becoming they capable of choosing whether or not to post their personal data on the Internet».

---

[3] BUCHMANN, J. (ed.) (2013): *Internet Privacy: Taking opportunities, assessing risk, building trust,* Acatech–Deutsche Akademie der Technikwissenschaften, HEIDELBERG *et al.*: Springer Verlag, p. 19.

[4] Ídem.

CONCEPTUAL FRAMEWORK

It may seem obvious that to assess the current impact of ICT in our private sphere we must start from defining a concept of «privacy». Nevertheless, attempt for conceptualization can be seen as almost unfeasible, particularly taking into account that we are forced to operate in a global environment although having in mind local conceptions of «private sphere», «personal data» and other similar whose definition enrooted in each culture hails from socially accepted conventions or ancient juridical tradition.

All in all, the mentioned shortcomings come to underline the necessity of rethinking the idea of privacy, delineating a reconceptualization capable of acting in the global digital environment and, at the same time, be adopted by every culture or region. To fulfil this purpose and to address some of these afore-mentioned questions the first part of this dissertation provides a solid theoretical framework in order to be consistent with terms[5] and therefore to proportion the conceptual support needed to carry out the subsequent analysis.

In view of this, this essay reviews the traditional approaches which have relied on a long-established distinction between «private» and «public» spheres[6], making particular mention of how as our lives become mediated by both mass media[7] and digital tools[8], the difference between «private» and «public» becomes weak and inconsistent. As a result, «predominant approaches used to define and protect privacy

---

5 For instance, in *Contextual Framework* chapter we explain why we use terms such as: «personal information» and «personal data»; «mediated communication» and «Information and Communication technologies» or «Web 2.0» and «Social Web».

6 See HABERMAS, J. (1989): *The structural transformation of the public sphere: An inquiry and category of bourgeois society*. Cambridge: Polity; and ARENDT, H. (1958): *The human condition*. Chicago: The University of Chicago Press.

7 THOMPSON, J. B. (1995): *The media and modernity: A social theory of the media*. Cambridge: Polity.

8 NISSENBAUM, H. (2004): «Privacy as contextual integrity», in *Washington Law Review*, n. 79, vol. 1, pp. 119-158; and NISSENBAUM, H. (2010): *Privacy in context: Technology, policy and integrity of Social Life*. Stanford, CA: Stanford University Press.

have persisted despite their limits results, and as it is discussed some of they should be challenged»[9].

In line with this, Solove cautions against the attempt at producing a full theory:

> The quest for a traditional definition of privacy has led to a rather fruitless and unresolved debate. In the meantime, there are real problems that must be addressed, but they are either conflated or ignored because they do not fit into various prefabricated conceptions of privacy […]. In this way, conceptions of privacy can prevent the examination of problems[10].

In what follows, we mention Nissenbaum's analysis of privacy breach in terms of «contextual integrity» as a framework for understanding the privacy implications of ICT and evaluating the flows of information hidden behind the interface of some Web 2.0 tools. Nissenbaum's benchmark «is not aiming for a full theory of privacy, but only a theoretical account of a right to privacy as it applies to information about people»[11] as that information is gathered by ICT.

In addition, we review existing legislation and privacy conception in the United States, the country where the main Internet enterprises headquarters are currently based, drawing a brief evolution of the theoretical framework starting by Samuel and Brandeis *right to privacy*[12] definition. At the same time, we review the set of rules which guide the activity of main Internet enterprises in Europe, making especial mention of Spanish law.

ANALYSIS

The *Analysis* section place emphasis on personal data transfer and information flows among some Web 2.0 services, focusing on those unclear flows of information which are neither obvious nor clear for user on SNS.

---

9 NISSENBAUM, H. (2011): *Op. cit.,* p. 33.

10 SOLOVE, D. J. (2007): «I've Got Nothing to Hide' and other misunderstandings of privacy», in *San Diego Law Review*, n. 44, pp. 745-772, p. 759.

11 NISSENBAUM, H. (2004): *Op. cit.,* p. 106.

12 WARREN, S. and BRANDEIS, L. D. (1890): «The right to privacy», in *Harvard Law Review*, n. 4, pp. 193-219.

Among the myriad of Web 2.0 tools, there is an aspect that has drawn particular attention: the collection of large amount of personal information on Social Networks Sites (SNS). According to Boyd and Jenkins[13], the popularity of these sites lies in the users' ability to communicate with friends, acquaintances and others; create personal identity online; share digital information and articulate their social networks in a public way. Nonetheless, despite the benefits accruing from the use of such tools, the exposure of large amounts of personal information on these sites has raised concerns about privacy risks. There are three main reasons for this increased attention. Firstly, what distinguishes such sites from precedent services is that they symbolize an exceptional social sphere which is highly mediated and where huge amounts of personal data are stored, aggregated and linked to an individual[14]. By their very nature and design, SNS encourage users to disclose significant personal information, consequently profiles constitute unique pages where one can «type oneself into being»[15]. Secondly, data supplied can be «copied, forwarded, replicated, and taken out of context»[16] with ease. Finally, users make explicit their social network, showing who their contacts are and, by omission, who they aren't. It is perhaps because of this that «social networking sites give the impression of a semi-public stage on which one can act in the privacy of one's social circle»[17], and this fact have a detrimental effect on the strategies users carry out to preserve their personal contents.

Apart from SNS, another point worth mentioning is the role played by browsers and the consequences derived from aggregation in Web 2.0. To address this, *Analysis* section illustrates different aspects such as the provision of personal data to third parties. Additionally, we will discuss how SNS and many services operating inside

---

13 BARNES, S. B. (2006): *Op. cit.*

14 GOVANI, T. and PASHLEY, H. (2005): *Op. cit.*

15 SUNDÉN, J. (2003): *Material Virtualities: Approaching Online Textual Embodiment*, New York: Peter Lang, p. 3.

16 BOYD, D. (2006): «Friends, friendsters, and MySpace top 8: writing community into being on social network sites», in *First Monday*, vol. 12, n. 11.

17 CHEW, M., BALFANZ, D. and LAURIE, B. (2008): «(Under) mining Privacy in Social Networks». Google Inc. Available at: http://w2spconf.com/2008/papers/s3p2.pdf. Under mining privacy. [28/01/2012].

and outside the boundaries of these platforms are able to target, track people down or even both at the same time.

The analysis mentioned above is juxtaposed with a deep insight into user's behaviour and level of understanding when interacting on SNS. In recent years much research has been done aim to comprehend their actions and weigh up their real knowledge[18]. As it is well-documented in the literature[19], Internet users report high levels of concern as far as the release of personal information on the Web is regarded. Despite this, users continue to post private content, creating their digital identity through the disclosure of large amounts of data[20]. This apparent contradiction between the concern people state and their willingness to show their personal information has been identified by Barnes as the «privacy paradox»[21].

Nonetheless, much research[22] has emerged suggesting that users «are not necessarily naïve in their disclosure practices […] and em-

---

18 We can mention three examples: POLLER, A., KRAMM, A. and ILYES, P. (2013): «Designing privacy-aware online social networks –A reflective socio-technical approach», in *CSCW '13 Measuring Networked Social Privacy Workshop*, February 23-27, 2013, San Antonio, Texas, United States; YOUNG, A. L. and QUAN-HASSE, A. (2013): *Op. cit.;* LIPFORD, H. R., *et al.* (2012): «Reconciling Privacy with Social Media», in *Proceedings of the 2012 ACM Conference on Computer Supported Corporative Work Companion*, pp. 19-29.

19 GOVANI, T. and PASHLEY, H. (2005): *Op. cit.*; GROSS, R. and ACQUISITI, A. (2005): *Op. cit.*

20 SUNDÉN, J. (2003): *Op. cit.;* and BOYD, D. (2008): «Why youth (heart) social network sites: the role of networked publics in teenage social life», in *Youth, Identity, and Digital Medias*, D. BUCKINGHAM (ed.): Cambridge, MA: MIT Press, pp. 119-142.

21 See, BARNES (2006): *Op. cit.;* and NORBERG, P. A., HORNE, D. R. and HORNE, D. A. (2007): «The privacy paradox: personal information disclosure intentions versus behaviours», in *Journal of Consumer Affairs*, vol. 41, n. 1, pp. 100-126. For other studies consistently finding a contradiction between the privacy concerns that users express and their disclosure of personal information on SNS see: GOVANI, T. and PASHLEY, H. (2005): *Op. cit.;* TUFECKI, Z. (2008): «"Can you see me now?" Audience and disclosure regulation in online social network sites», in *Bulletin of Science, Technology and Society*, vol. 28, n. 20, pp. 20-36.

22 See, DEBATIN, B., LOVEJOY, J. P., HORN, A. K. and HUGHES, B. N. (2009): *Op. cit.*; MADDEN, M. and SMITH, A. (2010): *Op. cit.;* STUTZ-

ploy a wide range of privacy protection strategies to address their concerns»[23]. In this essay, we support the idea that the phenomena of privacy paradox can be explained by the fact that users do not receive enough information to understand the particular characteristics of each digital context. As a consequence, they find themselves incapable of completely understanding and interpret the nature of those sceneries where they operate and post personal information. And the same happens when they try to apply Nissenbaum's informational norms.

DISCUSSION

From these considerations, we observe data sharing on SNS through the theoretical approach of «contextual integrity». As we underline, since the characteristics inherent to digital contexts created by SNS are neither clear nor explicit, it is extremely complicated for users to interpret the characteristics of such sceneries and how their contents can be used and distributed. Therefore, owing to the particular attributes of digital communication they find it more difficult to apply the informational norms which govern in every specific context, than in real life. Besides, the structure of SNS is mediated not only by technical media but also by the Internet enterprises which supports the social networks and their structure is not design to respect the integrity of every context. As an example, users may not be capable of carrying out their requirements for privacy in SNS since are limited in their ability to freely choose how their privacy preferences are configured and «online services do not always provide them with the desired options»[24]. Moreover, «its functionalities do not fit their individual concepts or because they do not, or only insufficiently, understand specific terms or the functional processes of the system at large»[25]. Taking these conditions into account it is unlikely users

---

MAN, F., CAPRA, R. and THOMPSON, J. (2011): «Factors mediating disclosure in social network sites», in *Computers in Human Behaviour*, vol. 27, n. 1, pp. 590-598.

23 YOUNG, A. L. and QUAN-HASSE, A. (2013): *Op. cit.,* p. 481.

24 BUCHMANN, J. (ed.) (2013): *Op. cit.,* p. 19.

25 POLLER, A., KRAMM, A. and ILYES, P. (2013): «Designing privacy-aware online social networks –A reflective socio-technical approach», in *CSCW '13*

have chances of protect themselves applying Nissenbaum's «contextual integrity».

PROPOSALS AND CONCLUSIONS

A number of conclusions can be drawn from the analysis of preceding points, providing a basis for concrete recommendations and proposals. To fulfil this part, we focus on the urge for improving educational measures, update the existing regulation and implement technical tools. Finally, we present a proposal on how to provide users with the amount of information to help them to maintain a desirable grade of autonomy as far as their own data protection is regarded, that is to say, we focus on how make them capable of deciding whether or not to display their personal data on SNS. To fulfil this purpose, we have elaborated a proposal which goes hand in hand with future Data Protection Regulation Draft from European Commission and includes a redefinition of «informed consent». Hence, the importance this essay has.

This implementation is a technical tool aim to explain users how their data will be used and with whom will be shared, as well as the use given by third companies' applications. In other words, it is an imposition upon actors who collect or use information to provide and explain users the purposes of such data collection and how they will manage it[26]. After receiving such flow of information, users being aware of the possible consequences of disclosing personal data on the Internet (informed) are supposed to be capable of deciding whether they display personal information or not (consent). Therefore, the moral legitimating of informed consent stems from the belief that it respects individual autonomy, particularly, that it reflects rational and informed decisions as far as the managing of personal data is concerning[27].

Measuring Networked Social Privacy Workshop, February 23-27, 2013, San Antonio, Texas, United States.

26 NISSSEMBAUM, H. and BAROCAS, S., (2009): «On Notice: The Trouble with Notice and Consent», in *Media, Culture, and Communication*. New York: New York University.

27 Ídem.

To conclude, we must accept that once again there are no catch-all solutions with regards to the preservation of privacy on the Internet and every context has to be examined on its own merits. However, the spread of information in conjunction with some other improvements, measures adopted by governments and the updated legislation would be warmly welcome for all citizens, whether they feel a certain degree of reluctance when interacting on digital environments or not.

We expect our findings to point to viable and constructive solutions for users to improve their privacy protection and, at the same time, safeguard the benefits expected from ICT and the Internet.

THESIS STRUCTURE

The paper proceeds as follows: In the first section, *Introduction,* we clarify the methodology, research bases, hypothesis, main expectations and principles followed throughout the whole essay. Subsequent to this, in *Contextual Framework* section, we carry out thorough terms delimitation, providing the definitions of the research object together with some remarks on the current situation.

In the next section, *Analysis,* we start from discussing Web 2.0 as a more general phenomenon, making particular mention of Social Networks Sites (SNS). After that, in the following chapters we consider Facebook's heuristics, focusing on the information transfer between the platform and its many services associated such as applications from external developers.

In order to clarify as well users' behaviour, risk perceptions and level of understanding of digital environments, afterwards there is considerable discussion of what the widespread adoption of Web 2.0 means for users' privacy and their informational self-determination, particularly in terms of information flows and personal data transfer. Throughout, we will attempt both to shed light on what the privacy repercussions of those features might be and to outline the role played by users' knowledge in such situations.

Finally, we offer some concluding recommendations as well as the most relevant findings in *Conclusions and proposals* section.

PARTE I

PRESUPUESTOS DE PARTIDA E INTRODUCCIÓN A LA INVESTIGACIÓN

CAPÍTULO I. INTRODUCCIÓN Y PLANTEAMIENTOS GENERALES

SÍNTESIS

Comenzaremos nuestro escrito esbozando las premisas que motivan la presente investigación, detallando las líneas de actuación que seguiremos durante el desarrollo de la misma. Para ello, en este primer capítulo trataremos aspectos básicos para circunscribir correctamente el desempeño que nos ocupa. Partiremos, en primer lugar, de la exposición y planteamiento de la problemática, aportando sus antecedentes más cercanos para contextualizarla adecuadamente, toda vez que relataremos la justificación y la pertinencia de la misma. Seguidamente, se especificarán los objetivos que pretendemos cumplir, así como la premisa primigenia que origina este texto, estableciendo, paralelamente, las hipótesis cuya comprobación vertebrará nuestro cometido. Igualmente, daremos cuenta de la metodología seguida para la verificación de dicha proposición de partida, junto con las fuentes que nutrirán su progreso. Finalmente, se demarcarán los límites a los que se atiene la presente memoria, delineando el alcance de los hallazgos y reseñando los posibles inconvenientes que pudieran lastrar los resultados.

1. INTRODUCCIÓN Y PLANTEAMIENTOS GENERALES

La complejidad que conlleva conjugar la protección de la esfera privada de la persona, indudable supraderecho fundamental, con las enormes posibilidades que ofrecen las tecnologías digitales, conforma uno de los dilemas éticos más reseñado, controvertido y difícil de solventar de la presente Era de la Información. Denostado en no pocas ocasiones e, incluso, ignorado en según qué épocas o por ciertos regímenes, el amparo al recinto reservado del ser humano supone la salvaguarda de la dimensión propia del individuo: aquella que le es irrenunciable, por ser inherente a su esencia como persona. Empero, la llegada de Internet ha posibilitado nuevas vías de acceso a espacios considerados propios de la intimidad y vida privada, nutriendo el escenario digital con poderosas herramientas de divulgación ampliada,

a través de las cuales nuestra vida se vuelve pública y nuestra identidad conocida. Un cambio de paradigma que ha propiciado que pilares cardinales, asumidos por la sociedad como inalienables, se hayan visto sometidos a novedosas formas de transgresión.

Este hecho, tan universal como lo es el usuario[28] de las aplicaciones tecnológicas, no es en absoluto baladí. La imbricación de la tecnología digital en todos los aspectos de la existencia del ser humano es tal, que la propia Red se ha convertido en «el tejido de nuestras vidas, que constituye, actualmente, la base tecnológica de la forma organizativa que caracteriza la era de la información»[29]. Sin embargo, este espacio de «flujos de información»[30] constituye un entorno mediado, a la par de mediático, en el que la licuefacción de la frágil barrera que determina lo que es comunicable y lo que no, esto es, lo que se define por su carácter público en contraposición a lo que se desea ocultar de la mirada ajena, provoca que una miríada de contenidos privados naveguen sin control por Internet. En consecuencia, la visibilidad de los datos no viene ya determinada por la naturaleza de los mismos, sino por la capacidad de acceso y la publicidad que estos adquieren, independientemente de si se trata de informaciones públi-

---

28 Al hablar de «usuario/s» hacemos referencia a aquella «persona física o jurídica que utiliza o solicita un servicio de comunicaciones electrónicas disponible para el público», tal y como se describe en el Anexo II de la *Ley de Telecomunicaciones española*.
Habitualmente, para referir a la persona que navega por la Red se utiliza el término «internauta» no admitido por el Diccionario de la RAE, por ello, en numerosas ocasiones nos apropiaremos del término «interactor». A este respecto, señala Wenceslao Castañares: «las nuevas textualidades de la realidad virtual exigen otro tipo de actividad. Tanto es así que hay que reconocer que las antiguas terminologías de «lector»,«espectador», «intérprete», «usuario», etc., ya no nos sirven porque no hacen justicia a lo que designan. Es posible que aún no hayamos encontrado el término adecuado. Se ha propuesto el término «interactor», que no es ni original ni especialmente agradable, pero al menos describe mejor a un nuevo sujeto textual que está entre el autor y el destinatario de los antiguos medios». CASTAÑARES, W. (2011): «Realidad virtual, mimesis y simulación», en *Cuadernos de Información y Comunicación,* vol. 16, 59-81, p. 76; y MACHADO, A. (2009): *El sujeto en la pantalla. La aventura del espectador, del deseo a la acción*. Barcelona: Gedisa, p. 132.

29 CASTELLS, M. (2001): *La galaxia Internet,* Barcelona: Areté, p. 15.

30 CASTELLS, M. (1999): *La era de la información. Economía, sociedad y cultura*. Madrid: Siglo XXI, p. 409.

cas o contenidos otrora reservados. Y en este escenario, Internet se configura como el actual ágora del nuevo espacio público mediatizado, estructurado en ocasiones por elementos que proceden de la esfera privada, es decir, del ámbito de no intromisión que, por esencia, le es propio al individuo.

Consecuentemente, en nuestro mundo deslocalizado nos asomamos al abismo de la paradoja constante, aquella que se produce y retroalimenta de un continuo tira y afloja entre la democratización de la técnica y la desigualdad que genera la falta de protección del individuo, protagonista, a la postre, del progreso tecnológico. Y dicha colisión se reproduce a escala mundial, navegando entre marcos normativos desiguales, usos sociales distintos y concepciones culturales de intimidad y vida privada divergentes, de suerte que los gobiernos no poseen fórmulas para erradicarla o combatirla.

Nos movemos, consecuentemente, en el farragoso terreno del contrasentido continuo, aquel en el que las tecnologías digitales se constituyen en poderosas armas de doble filo: correctamente empleadas, contribuyen a cimentar y promocionar los pilares que sustentan los principios democráticos, promoviendo valores fundamentales como la educación, el acceso a la información, la libertad de expresión y el respeto a la integridad humana. Conforman, en definitiva, un vehículo necesario para el desarrollo y evolución de la sociedad. Mal enfrentadas, en cambio, promueven la desinformación y la vulneración de los derechos del ciudadano.

No resulta ajeno, por tanto, que la mediación tecnológica inherente al entorno digital crea un terreno propicio para la emergencia de contraprestaciones que se ceban, sustancialmente, con el respeto al anonimato y autodeterminación informativa del individuo. Especialmente reseñable resulta la complejidad de preservar nuestras informaciones personales tras la llegada de la Web 2.0, un nuevo tejido digital social que, a pesar de sus indudables bondades, posee unas atribuciones propias que complican la ecuación. Así, tras la popularización de las herramientas relacionales de la Web semántica, la vida entera de una persona puede traducirse en una serie de datos digitalizados, una colección infinita de unos y ceros, cuyo transporte, agregación y acceso posibilitan que, en la otra punta del mundo, pueda

crearse una réplica exacta de nuestra identidad[31]; con carácter virtual, pero con capacidad real para dañar la integridad del individuo. Como ya anunciara McLuhan, con clarividencia visionaria, «en la Era Eléctrica nos vemos cada vez más traducidos a términos de información, dirigiéndonos hacia la extensión tecnológica de nuestra conciencia»[32].

Que el citado fenómeno parece lastrar e, incluso, ensombrecer en cierta medida los múltiples beneficios imputables a la nueva realidad comunicativa, es un hecho que se ha visto reflejado por muchos agentes de la sociedad. No en vano, desde el ámbito periodístico las injerencias en lo privado protagonizan cada vez más informaciones encaminadas a denunciar aquellas que resultan especialmente llamativas. Asimismo, la nombrada problemática ha sido profusamente reflejada en los análisis e investigaciones de infinidad de académicos, observaciones que se perpetran desde un abanico disciplinario cada vez más amplio[33] y que plasman cómo las inquietudes se incrementan a medida que la Red se puebla de aplicaciones sociales. Analizar este dilema nos azuza a mirar más allá del horizonte que enmarcan los desvelos del presente y abrir los ojos al verdadero reto que supone la integración de la dimensión humana en el progreso tecnológico, hecho que recuerda que las tecnologías comunicativas no son solo una realidad técnica.

Ciñéndonos a las demarcaciones de la presente investigación, entendemos que el entramado actual, configurado por la emergencia de espacios sociales mediados e innovadoras formas de interacción que desbordan los preceptos comunicativos clásicos, nos obliga a clarificar en qué condiciones se está dando el intercambio de nuestros datos privados en la Red. Para ello, en el estudio que nos ocupa abordare-

---

31 Para una conceptualización del término «identidad» en relación a los medios de comunicación social resulta interesante revisitar los escritos de Dominique Wolton. En concreto: WOLTON, D. (2000): *Internet, ¿y después?: una teoría crítica de los nuevos medios de comunicación,* Barcelona: Gedisa, p. 238.

32 MCLUHAN, M. (1999): *La piel de la cultura*. Barcelona: Gedisa, p. 169.

33 Aunque parezca recurrente, resulta necesario traer a colación los postulados de Edgar Morin, para quien el pensamiento complejo constituye la puerta de entrada en el s. XIX y el sentido interdisciplinario se conforma necesario para asomarse a las Ciencias de la Comunicación. MORIN, E. (1990): *Introducción al pensamiento complejo*. Barcelona: Gedisa.

mos algunas de las claves que encierra este fenómeno, intentando arrojar algo de luz sobre los puntos más controvertidos y aportando, en última instancia, soluciones prácticas nacidas de la observación rigurosa precedente.

Hablamos de Internet, pero para ser más exactos nos circunscribimos a las dinámicas de flujos que se dan bajo la estructura de la Web 2.0, también llamada semántica o relacional y que supone el sustrato sobre el que se realiza el intercambio informativo. En este repaso, las redes sociales, paradigma de la filosofía 2.0, acapararán el protagonismo absoluto. Más en concreto Facebook, conocida genéricamente como «la red social» y que se ha convertido en el mayor banco de datos privados de la historia, superando la cantidad y calidad de información recolectada incluso por los servicios de espionaje e inteligencia gubernamentales. Dicha recogida pormenorizada de informaciones de los ciudadanos es doblemente peligrosa por cuanto los propietarios de la información desconocen, no solo cómo y en qué momento se desarrollan esas prácticas de recolección de datos, sino la finalidad a la que se destina. No obstante, aun cuando nos centremos en la nombrada herramienta, la mencionaremos siempre de manera genérica, en tanto que ejemplifica a la perfección la dinámica que se reproduce a mayor o menor escala en la inmensa mayoría de contextos en los que se presenta problemática a estudiar. Consecuentemente, cuando citemos a Facebook estaremos aludiendo con frecuencia al complejo universo de redes sociales que cohabitan el universo digital, por lo que no deben excluirse de las conclusiones obtenidas las acciones de otras herramientas que operan en la Web social.

Cabe mencionar que un análisis de la magnitud del presente debe estar debidamente delimitado para desembocar en conclusiones reseñables y representativas. Por dicho motivo, no abordaremos la problemática referida a la recolección de información y vigilancia masiva de los gobiernos a través de estas herramientas [como la protagonizada por las estadounidenses Agencia de Seguridad Nacional (NSA) y Agencia Central de Inteligencia (CIA) así como los servicios de inteligencia de otros países], por entender que excede los límites de este escrito y requiere una investigación aparte.

Ahora ya sí, partiendo de esta breve exposición inicial y convencidos de que, tal y como asevera Castells, «la teoría y la investigación […] deben considerarse medios para comprender nuestro mundo y

deben juzgarse por su precisión, rigor y pertinencia»[34], comenzamos este viaje en el que aspiramos a recabar y ofrecer una comprensión válida y útil del fenómeno que nos ocupa, haciendo frente a las nuevas exigencias de nuestro mundo. Pretendemos, en definitiva, entender de un lado cómo funcionan las interacciones entre los individuos y las herramientas tecnológicas digitales, mecanismos que caracterizan la sociedad actual, y de otro la protección de la intimidad y vida privada del verdadero protagonista del cambio tecnológico: el ser humano. Y en este empeño nos encontramos, dando inicio a los primeros pasos de este intenso éxodo que no ha hecho sino despuntar.

1.2 ANTECEDENTES Y ESTADO ACTUAL DEL TEMA

Como acabamos de mencionar, que el advenimiento de las nuevas tecnologías ha diluido los límites de la intimidad y vida privada no es un hecho que resulte ajeno a la producción científica, a la difusión informativa por los medios de comunicación de masas ni, por ende, a la opinión pública. Este fenómeno no es actual. Desde la aparición de las primeras distopías literarias sobre la vigilancia masiva propiciada por el uso perverso de la tecnología, hasta los últimos estudios sobre las intromisiones en el ámbito reservado de la persona, existe un abanico considerable de investigaciones, informes, proyectos de investigación y artículos que centran su interés en la observación, análisis y discusión de este conflicto. Como fin último, se intenta ofrecer propuestas que solucionen esta problemática, intentando conjugar el acceso a la información y el disfrute de los servicios digitales, con la salvaguarda de la dimensión propia del individuo.

Lo que sí resulta novedoso es la licuefacción de contornos que, para Zygmunt Bauman, caracteriza al mundo moderno[35] y que tan acertadamente describe la nueva realidad comunicativa; una atribución que, además, confiere un matiz de complejidad al dilema. No es de extrañar, por ello, que todas las semanas aparezcan diversas informaciones en medios de comunicación relativas bien a la confronta-

---

[34] CASTELLS, M. (1998): *Op. cit.,* p. 393.

[35] BAUMAN, Z. (2003): *Modernidad líquida*. México DF: Editorial Fondo de Cultura Económica.

ción entre esfera privada y los nuevos usos sociales, bien en relación a las dudosas prácticas empresariales enlazadas a estos espacios públicos mediados.

No obstante, si observamos la tendencia general seguida en las informaciones periodísticas, como en la generalidad de estudios científicos, constatamos que ambos aparecen encaminados a solventar la problemática desde el punto de vista legal y/o técnico. Es decir, excluyen las posibles acciones efectuadas desde el otro vértice de la ecuación, a saber: las prácticas desempeñadas por el usuario. Y todo ello, aun cuando este es, en definitiva, el protagonista del cambio tecnológico.

En esta tesis pretendemos, por el contrario, hacer hincapié en un aspecto que se revela capital a la hora de prevenir las mencionadas intromisiones: reforzar el papel activo del individuo cada vez que interactúa con las herramientas digitales. En este cometido, nos proponemos fortalecer su conocimiento y su capacidad crítica de toma de decisiones, proporcionándole información encaminada a concretar las atribuciones de cada escenario digital, con el fin último de capacitar sus actuaciones.

Resulta pertinente remarcar que existen características inherentes al universo digital y a la naturaleza del objeto de estudio en sí, es decir, a la vida privada, que dificultan enormemente la subsanación de esta problemática. A este respecto, la mayoría de las investigaciones topan con el inconveniente que supone abordar un tema como es la protección de «lo privado», noción ligada tanto culturalmente, como por el marco legislativo imperante, a las fronteras físicas de un territorio concreto y que, a la vez, demanda una aproximación heterogénea en tanto que opera en un escenario universal. Enfoque complejo que emana del hecho de que las consideraciones culturales y la protección jurídica son locales, pero no así el entramado tecnológico que no posee más límite que la globalidad.

Dada la complicación de la empresa en la que nos embarcamos, encontramos aquí la justificación para situar nuestra perspectiva en ese agente que siempre se mantiene constante y que, además, es el titular del derecho a la intimidad; sin desdeñar enfoques centrados en la importancia de una buena regulación jurídica o la necesidad de unas aplicaciones y diseños técnicos más seguros y «amables» para el usuario.

Esta declaración de intenciones viene a colación de señalar una cierta coherencia y continuidad de la premisa seguida en la presente investigación y que enlaza con las aproximaciones desarrolladas desde algunas universidades e institutos de investigación, referentes en esta temática. Viene al caso citar, siguiendo esta tónica, el proyecto *Software Design for Interactional Privacy within Online Social Networks* (*DIPO)*[36] desarrollado entre el prestigioso Fraunhofer-Institut für Sichere Informationstechnologie (SIT) sito en Darmstadt (Alemania) y el Institut für Kulturanthropologie und Europäische Ethnologie, Goethe-Universität Frankfurt am Main[37]. Dicho estudio, del que pudimos formar parte durante el desarrollo de este texto, engloba vertientes como el análisis del comportamiento de los sujetos respecto a la protección de su vida privada en Facebook (proyecto: *Privatsphärenschutz in Online Social Networks/ Estudio de la protección de la esfera privada en redes sociales*) o de las herramientas que ofrecen otras aplicaciones de la Web 2.0 para proporcionar cierta protección al usuario. Todo ello mediante el uso de análisis cualitativos y la aplicación de *softwares* específicos como es ROSE[38] desarrollado por el Instituto Fraunhofer. El citado grupo de investigación colabora, asimismo, con el centro de investigación de Google Zurich Research Center, así como con el European Center for Security and Privacy By Design (EC SPRIDE)[39] de la Technical University Darmstadt y la Goethe-Universität Frankfurt am Main.

Por su parte, desde la Academia Alemana de Ciencias e Ingeniería (*Deutsche Akademie der Technikwissenschaften, Acatech)*[40] se han desarrollado numerosos informes sobre la situación actual de la problemática que, por su rigor y pertinencia, referiremos en varias ocasiones durante el desarrollo de esta tesis. Resulta, igualmente, útil revisar los trabajos de uno de los autores de *Acatech* con más trayectoria en el estudio de las implicaciones éticas de las tecnologías digitales, como es el caso de Rafael Capurro, Catedrático de Gestión

---

36 Toda la información se puede encontrar en: https://www.sit.fraunhofer.de/ y https://dipo.sit.fraunhofer.de/.

37 Más información en: www.uni-frankfurt.de/39023844

38 Programa ROSE: https://dipo.sit.fraunhofer.de/rose-2-is-coming/

39 European Center for Security and Privacy By Design (EC SPRIDE): www.ec-spride.tu-darmstadt.de

40 Deutsche Akademie der Technikwissenschaften: www.acatech.de

y Ética de la Información, y miembro activo del Comité Consultivo del Instituto de Ética Digital (IDE) de la Stuttgart Hochschule der Medien (Alemania). En su haber obran numerosos informes destinados a desentrañar las claves que rodean a este fenómeno, centrándose en los efectos éticos de las nuevas tecnologías, sin perder la perspectiva de la interacción social, política, económica, científica y cultural. Capurro ha participado, igualmente, en el European Group on Ethics in Science and New Technologies (EGE)[41] de la Comisión Europea (2000-2010) y dirige el grupo multicultural e internacional Steinbeis Transfer Institut Information Ethics (STI-IE)[42] así como la Capurro Fiek Fundation[43], ambas entidades dedicadas al análisis de las implicaciones de las tecnologías digitales en la sociedad actual.

En Reino Unido, el Centre for Computing and Social Responsibility, De Montfort University[44], lleva años estudiando la problemática con una visión más amplia que no solo incluye la protección de la intimidad y vida privada, sino otros dilemas éticos como el acceso a la información o la rigurosidad de esta. Desde hace veinte años y coincidiendo con el despegue de Internet a nivel mundial, celebran los congresos internacionales Ethics and Computer (ETHICOMP)[45].

En Estados Unidos destacan los trabajos de Danah Boyd, James Fowler y Deborah Johnson. Boyd, socióloga, es una de las investigadoras principales de Microsoft Research y fundadora del instituto de investigación Data and Society. Por su parte, además de científico social centrado en el estudio de las redes sociales, Fowler está especializado en la observación del comportamiento, la evolución, la política, la genética y el *big data*. En cuanto a Johnson, famosa por sus escritos sobre Ética Informática, se ha convertido en referencia ineludible al sentar los cimientos de esta disciplina desde los años noventa.

---

41 EGE de la Universidad de los Medios de Stuttgart: https://www.hdm-stuttgart.de/

42 Transfer Institut Information Ethics (STI-IE): http://sti-ie.de, Transfer Institut Information Ethics (STI-IE)

43 Capurro Fiek Fundation: www.capurro-fiek-stiftung.org

44 Centre for Computing and Social Responsibility: www.dmu.ac.uk/research/research-faculties-and-institutes technology/centre-for-computing-and-social-responsibility/ccsr-home.aspx

45 Ethics and Computer International Congress: https://ec.europa.eu/digital-agenda/en/news/ ethicomp-2015

Mención aparte merecen los trabajos de Helen Nissenbaum, Catedrática de Medios de Comunicación, Cultura y Comunicación, así como de Informática en la universidad de Nueva York. Sus estudios versan sobre la protección de la vida privada, así como la confianza y la seguridad del ciudadano en los entornos digitales, ya sean Tecnologías de la Comunicación y la Información, bases de datos institucionales o en las tecnologías desarrolladas para la vigilancia pública. Su aproximación, basada en la importancia del contexto en el que se incluyen las informaciones privadas y la justificación de ese despliegue, ha servido de base no solo para muchos ensayos y estudios de campo, sino que se ha tenido muy en cuenta a la hora de abordar conflictos legales en Estados Unidos. En definitiva, la autora es referencia ineludible para la elaboración de una futura legislación estadounidense sobre la protección de la intimidad, así como para la nueva directiva de protección de datos de la Unión Europea. En el presente trabajo, usaremos su marco teórico, la protección de la intimidad y vida privada en base al respeto a la integridad contextual[46], para verificar las premisas de partida.

Por último, se torna necesario añadir una puntualización: gran parte de los estudios sobre invasión de la intimidad y vida privada provienen de las teorías distópicas de la vigilancia, que interpretan la introducción de la tecnología como una forma de control social en un futuro hostil e inevitable en el que el ciudadano de a pie poco puede hacer salvo acostumbrarse. Esta no es la visión del presente texto, ya que no creemos en absoluto que la proliferación en el uso de las tecnología derive en el futuro en una ciudad vigilada al más puro estilo *1984*[47]. Empero y aunque no compartamos esta visión, resulta casi imposible escribir sobre esta temática y no mencionar el clásico de George Orwell. De hecho, a lo largo del desarrollo de la presente investigación hemos revisado numerosos estudiosos que se valen del conocido clásico para ejemplificar los temores que suscita las intromisiones incontroladas en el ámbito más reservado del ser humano.

Por nuestra parte, abandonamos esta deriva y nos centramos en una inquietud palpable en la sociedad. No perdemos, por dicho moti-

---

46 NISSENBAUM, H. (2004): «Privacy as contextual integrity», en *Washington Law Review*, vol.79, n.1, p. 107

47 ORWELL, G. (1949): *1984*. Hay múltiples ediciones en castellano, por citar una de las más recientes Orwell, G. (2009): *1984*. Barcelona: Ediciones Destino.

vo, la perspectiva que nos enseña que cualquier avance siempre vino lastrado por una serie de inconvenientes, lo que no debe empañar sus virtudes. Recordaremos esta reflexión, más adelante, para no olvidar que las tecnologías, dejando a un lado sus posibles efectos nocivos, son instrumentos imprescindibles para el desarrollo del ser humano y que, por ende, nunca debemos poner en duda sus bondades por el simple hecho de que exista una serie de desviaciones negativas.

1.3 RAZONES PARA UN ESTUDIO DE ESTA ÍNDOLE

1.3.1 **Interés académico**

Como ya hemos adelantado en el apartado precedente, son innumerables las investigaciones, ensayos, monografías y publicaciones de actualidad centradas en las distintas y complejas interacciones que se producen al entrar en juego la intimidad y vida privada en los entornos digitales. A este respecto, desde el ámbito académico se ha abordado cuantiosamente no solo el surgimiento, desarrollo y actual situación de la problemática, sino que se ha tratado de ofrecer soluciones a medida que la invasión del ámbito reservado del individuo parecía suponer una amenaza para el necesario desarrollo de la tecnología. No debe sorprender al lector, por ello, el amplio espectro de estudios a este respecto que certifican que, lejos de suponer una moda pasajera, constituye un auténtico desafío para la ciencia.

Por otra parte, la razón primordial de este interés la encontramos en la complejidad inherente a la esencia de los parámetros que entran en juego. De un lado, el objeto de estudio, esto es, la intimidad y vida privada, viene marcado por una naturaleza variable en función de condicionamientos culturales, legales y costumbres. Y, si ya de por sí resulta complicado conjugar la subjetividad humana con otros factores, encontramos que la dificultad se agrava al añadir las características de la naturaleza global, cambiante, inmaterial y difusa del entorno tecnológico digital. Nos movemos, en definitiva, en arenas movedizas en las que nada permanece estable, invariable, ni constituye una regla absoluta.

No obstante y aun cuando la incertidumbre constituye una parte innegociable de las investigaciones que analizan fenómenos de las ciencias sociales, debemos centrarnos en el hecho concreto y real: la

desprotección que amenaza la salvaguarda de las informaciones privadas de los individuos. Es por ello, que en el presente estudio trataremos de esbozar un panorama global, una instantánea que servirá para centrarnos en las circunstancias concretas, delineando la evolución del suceso y explicando qué se encuentra bajo la superficie de estas situaciones de vulnerabilidad del usuario. Si bien, cabe advertir al lector del inconveniente que lastra las investigaciones sobre hechos contemporáneos: cuando nos referimos a la situación actual hablamos, en realidad, del pasado más inmediato, por cuanto no podemos obviar que mencionar el presente es un acto inexacto, pues nada (y mucho menos en un entorno tan cambiante) se mantiene intacto.

Asimismo, otra de las innovaciones de esta investigación es la propuesta final en la que se intenta solventar una parte de la problemática. Internet nació como una red de intercambio de conocimiento, elemento que, curiosamente, se encuentra en la esencia misma del dilema, constituyendo un lugar común en el amplio abanico de intromisiones observado. A lo largo de la presente investigación, haremos hincapié en la importancia que un correcto flujo de información posee en la protección de los usuarios. Por ello, no perderemos de vista una constante: la educación, base de un buen devenir en la sociedad[48], ostenta un papel fundamental, particularmente, si tenemos en cuenta que esta nueva realidad comunicativa es cada vez más cambiante, compleja y demanda mayores competencias y recursos al ser humano. Pretendemos, de este modo, hacer valer el silogismo demostrativo según el cual si la falta de información y base crítica juegan un papel primordial en las intromisiones en el recinto reservado de la persona, la existencia de un mecanismo que proporcione dicho soporte crítico ayudaría a revertir la situación. De este modo, tras el pertinente análisis, ofreceremos una propuesta encaminada a estimular el poder de decisión del usuario, abandonando así su *role* de sujeto pasivo al vaivén de regulaciones obsoletas e intereses ajenos.

Finalmente, además de la necesidad de dar soluciones concretas a una problemática que afecta al usuario universal, otro hecho justifica la pertinencia académica de este estudio: el presente relato cuenta con

---

[48] Así lo afirmaba el filósofo griego Sócrates, para quien la educación constituía una necesidad en la sociedad: «La educación es el encendido de una llama, no el llenado de un recipiente», Sócrates, *Hem*., 1 /97, p. 96.

la integración de los postulados de Helen Nissenbaum, autora de referencia a nivel internacional en el estudio de los conflictos entre tecnologías digitales y preservación del ámbito privado del ser humano, pero cuyos escritos todavía no han sido suficientemente tratados en España.

Con dichas premisas en mente, surge esta investigación que, sin duda, no será la última de su especie. Presumiblemente, más tarde o más temprano proliferarán otros muchos trabajos volcados, a buen seguro, en esta misma realidad.

1.3.2 **Interés general**

Con todo lo indicado, puede resultar obvio explicar el alcance que este tipo de investigaciones tienen en la realidad comunicativa. El carácter cotidiano de las nuevas técnicas de comunicación avala su imbricación en la sociedad. Basta echar un vistazo a las informaciones sobre tecnología en los medios de comunicación en los últimos diez años y verificaremos cómo el estudio que nos ocupa protagoniza un amplio número de boletines informativos. Que dichas cuestiones hayan saltado a la arena pública y den qué pensar al ciudadano de a pie no es mera casualidad: El correcto uso de las tecnologías de la comunicación y la información promueve el avance de la Sociedad del Conocimiento y fomenta un entorno más igualitario.

El ciudadano que posee información puede hacer valer sus derechos y las aplicaciones digitales se configuran como herramientas de acceso a las fuentes de las que emana el conocimiento, hecho que alumbra que no estamos ante un asunto trivial. Por ende, cuando hablamos de la protección de la intimidad y vida privada, subrayamos la importancia fundamental de capacitar al ciudadano, instándole a aplicar la reflexión crítica para sacar el máximo partido del progreso tecnológico sin perjuicio para su integridad privada.

En lo que respecta al plano individual, manejarse correctamente en la Red es hoy tan necesario como saber vivir en sociedad. Lejos de parecer una exageración, lo cierto es que absolutamente todas las realidades de nuestro tiempo están empapadas del cambio tecnológico, razón por la que Cebrián Herreros afirmaba que:

> La revolución de las tecnologías de la información y las comunicaciones está generando en la sociedad, no solo una época de cambios,

> sino un cambio de época. Internet se ha venido expandiendo en todos los entornos y aspectos de nuestra sociedad. […] ni un solo rincón de nuestra historia futura va a dejar de verse afectado por el desarrollo del mundo digital.[49]

No en vano hablamos de educación 2.0, nos comunicamos a través de las redes sociales o realizamos trámites con las administraciones mediante las aplicaciones habilitadas a tal efecto. Recordamos, a este respecto, los preceptos de organismos como la UNESCO según los cuales el desarrollo de las tecnologías digitales y la correcta adopción por todos los agentes involucrados, constituyen la mejor manera de difusión de conocimiento y acceso a una sociedad igualitaria, gracias, en parte, a las posibilidades que ofrecen en la educación, ciencia y cultura a nivel internacional[50].

Es por ello que el interés de esta investigación no se agota tras su publicación. Más aún, si tenemos en cuenta que, en la actualidad, hay en todo el mundo más de tres millardos de usuarios[51] y que, aunque la cifra se mantiene dentro de unos límites en el continente europeo, Estados Unidos, Canadá y Japón, su número continua aumentando enormemente en Asia, África y América Latina, lo que dibuja un matiz que a menudo pasa desapercibido: la Era Digital no ha hecho más que empezar.

---

[49] Herreros, C. (2010): *Desarrollos del periodismo en Internet,* Zamora: Comunicación Social Ediciones y Publicaciones, p. 12

[50] En particular, según la UNESCO, los gobiernos deberán centrarse en: reforzar el derecho a la educación, fortalecer la cooperación científica e intelectual internacional, proteger el patrimonio cultural, promover la evolución de los medios de comunicación y ampliar el acceso a la información y el conocimiento de dominio público. Estas tareas son esenciales para construir las sociedades del conocimiento basadas en la equidad y la justicia social, y encaminadas a fomentar la autonomía de sus miembros. UNESCO (2005): *Hacia las sociedades del conocimiento*. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Disponible en: www.unesco.org/publications [04/02/2013].

[51] Actualmente cerca del 40% de la población mundial tiene conexión a Internet hoy en día. En 1995, esta cifra suponía menos del 1%, pero el número comenzó a aumentar exponencialmente entre 1999 y 2014. Así, en 2005 se alcanzó el millardo de interactores y, cinco años más tarde, el segundo. «Number of World Internet Users (2014)», en *Internet Live Stats*. Disponible en: www.internetlivestats.com/internet-users [12/01/15].

1.4 OBJETIVOS DE LA INVESTIGACIÓN

La presente exposición parte de una inquietud personal, en la que pretendemos averiguar el papel fundamental que juegan el conocimiento y la correcta interpretación de los contextos digitales por parte de los usuarios de las tecnologías digitales, en las intromisiones en la intimidad y vida privada. En otras palabras, este estudio nace de la necesidad de analizar la relación que se establece entre la vulneración de la esfera privada del individuo y la información, o falta de ella, que impera en los escenarios digitales.

El valor primordial que le otorgamos a la información no es casual. Recordemos, citando a Castells, que si algo evidencia que vivimos en una sociedad informacional es el hecho de que la comunicación y la información se constituyen como dos de las fuentes de poder más importantes del sistema[52], esto es, fundamentan su existencia. Pues bien, dado que operamos dentro de esta Sociedad de la Información, resulta capital comprender el peso que las mecánicas de flujos de información y trasvase de datos poseen en las situaciones de vulnerabilidad del sujeto, incidiendo en cómo la propia estructura de la Internet dificulta su entendimiento. Para desentrañar el entuerto el desarrollo de esta tesis gira en torno a unas consideraciones generales y una serie de principios específicos que desgranamos a continuación.

1.4.1 **Objetivos generales**

La extensión y complejidad del tema nos invita centrar nuestros objetivos en la obtención de una serie de concreciones destinadas a:

— Conocer si los contextos en los que se producen las intromisiones en la intimidad y vida privada de los usuarios aparecen marcados por una carencia de información que dificulte al usuario interpretar la naturaleza del escenario comunicativo.

— Evaluar en qué consiste la dificultad para entender e interpretar los entornos digitales de la Web 2.0.

— Conocer los cambios que las nuevas tecnologías han introducido en la concepción de intimidad y vida privada.

---

[52] Castells, M. (2001): *Op. cit.,* p. 51.

— Desentrañar el papel del usuario en la protección de su esfera privada.

1.4.2 Objetivos específicos

La anterior visión genérica puede disgregarse en los siguientes aspectos concretos que determinan los niveles de actuación seguidos en esta investigación:

— Realizar un elenco de las principales vías de vulneración de la intimidad y vida privada del individuo en las redes sociales.

— Conocer las interacciones de los usuarios, su nivel de conocimiento y percepción de riesgo, así como las medidas que toman para proteger sus informaciones privadas.

— Analizar a través del estudio de redes sociales si las herramientas de la Web 2.0 permiten al usuario la comprensión de la naturaleza y condiciones de los intercambios de datos.

— Reseñar en qué medida la estructura de las plataformas de redes sociales oscurece el traspaso de datos que en ellas se produce.

— Deslindar las posibilidades de negocio que entraña la obtención de los datos de los sujetos bajo su desconocimiento.

1.5 HIPÓTESIS

La hipótesis constituye el eje fundamental alrededor del cual gira cualquier investigación, un puente que enlaza el planteamiento de la cuestión que se desea abordar y su comprobación empírica. Es, por tanto, «una suposición que se propone tentativamente, para dar solución a un problema planteado, buscando la relación que existe entre las variables y los fenómenos» [53]. No obstante, no debemos caer en el error de afirmar que toda suposición debe considerarse hipótesis, ya que esta debe partir de una serie de razonamientos. En definitiva, hablamos de una formulación que se sustenta en un sistema de conoci-

---

[53] LUNA CASTILLO, A. (1996): *Metodología de la tesis*, México: Trillas, p. 73.

mientos organizados y sistematizados, y se apoya en una relación de dos o más variables para explicar y, si es posible, predecir estadísticamente, los fenómenos que nos interesan, en el caso de que se compruebe la relación establecida[54].

En el presente trabajo pretendemos averiguar si existe una relación directamente proporcional entre el conocimiento e información que recibe el interactor de las tecnologías digitales y las intromisiones en su intimidad y vida privada. Partimos, por ello, de la siguiente premisa: El usuario necesita información para interpretar los escenarios de la Web 2.0, para entender los flujos de trasvase de información que se dan en su estructura y para saber cómo serán recolectados, almacenados y gestionados sus datos. De este modo podrá decidir, de manera crítica, cuando introducir sus contenidos privados, actuando acorde a la integridad del contexto.

Para abordar dicha proposición, nos hemos decantado por una tipología de hipótesis descriptiva de dos variables en la que estas se relacionan en términos de asociación o covarianza, esto es, cuando una variable cambia también las otras se modifican, pero siempre en forma proporcional o directa. En este caso, la variable independiente es el conocimiento y la dependiente el nivel de protección de la intimidad y vida privada que pueden obtener los sujetos. Así, a mayor conocimiento, mayor protección, en una relación directamente proporcional. Es pertinente puntualizar que, en este tipo de hipótesis, la relación no es causal, ya que ambos elementos lógicos pueden ser causa y efecto a la vez[55]. La comprobación se realizará mediante el cruce de informaciones relativas a ambas variables.

Desde esta perspectiva y dado que la herramienta teórica que usaremos para verificar la existencia o no de dicha correlación será el marco de la integridad contextual enunciado por Helen Nissenbaum (y que posteriormente detallaremos) la hipótesis sustantiva que planteamos parte de la siguiente consideración:

— «El usuario no obtiene información suficiente para comprender los escenarios de la Web 2.0 (representados por las redes

---

[54] ROJAS SORIANO, R. (1977): *Guía para investigaciones sociales*. México: UNAM. pp. 21-56.

[55] LUNA CASTILLO, A. (1996): *Op. cit.,* p. 73.

sociales) en los que opera e introduce sus datos privados. Por tanto, no puede interpretar la integridad del contexto y proteger así sus contenidos privados».

Esta será la premisa que guiará nuestra investigación, en la que la cronología de los acontecimientos relatados hará las veces de hilo conductor. Como suposiciones derivadas de la anterior se plantean:

— Tras la llegada de la Web 2.0, la información y la formación del individuo constituyen su mejor defensa *a priori* para proteger su intimidad y vida privada.

— La estructura y diseño de algunas de las herramientas arquetípicas de la Web 2.0, como son las redes sociales, contravienen la integridad del contexto propiciando la aparición de escenarios potencialmente peligrosos.

— Muchas de las plataformas de la Web 2.0 sacan provecho o incluso basan su negocio en este desconocimiento del usuario, en tanto que la mayor parte de recopilación de datos se da en escenarios de desinformación. Es decir, en los que los individuos no son completamente conscientes de que se están recopilando sus datos.

1.6 METODOLOGÍA EMPLEADA

Como fenómenos simbólicos que son, las ciencias sociales deben ir más allá de una mera cuantificación de acontecimientos para poder hallar sentido al estudio de los datos. Abandonando así la fascinación, casi veneración, por las cifras de las técnicas cuantitativas cuyos resultados no siempre conducen a la comprensión global de los fenómenos, el análisis de contenido y la posterior comparación de registros son considerados dos de las técnicas de investigación más importantes para el estudio de las realidades sociales. La conjunción de ambas procura, tal y como subraya Klaus Krippendorff (Frankfurt am Main, 1932) comprender los datos no como un conjunto de acontecimientos físicos, sino como fenómenos simbólicos; reconociendo su papel social, sus efectos y su significado[56].

---

[56] KRIPPENDORFF, K. (1990): *Metodología de análisis de contenido,* Barcelona: Paidós Ibérica, pp. 28-29. Además de este autor, hemos revisado la obra

Así pues, el método seleccionado para abordar el material que conforma la extensa materia prima de nuestro estudio es primordialmente el análisis comparativo y de contenido de los artículos científicos recabados. Dicha aproximación surge determinada por la propia naturaleza de la investigación, fundamentada en la verificación de la correlación entre conocimiento e información en el entorno digital y protección de la esfera privada del sujeto.

En su tratado: *Metodología de análisis de contenido,* el autor alemán define esta técnica de investigación como aquella: «destinada a formular, a partir de ciertos datos, inferencias reproducibles y válidas que puedan aplicarse a su contexto» [57] y añade, «su finalidad consiste en proporcionar conocimientos, nuevas intelecciones, una representación de los hechos y una guía práctica para la acción. Es una herramienta» [58].

Más concretamente, son tres los argumentos de Krippendorff que nos motivan a elegir esta metodología: en primer lugar, el análisis de contenido tiene «una orientación fundamentalmente empírica, exploratoria, vinculada a fenómenos reales y de finalidad predictiva» [59]. Es, asimismo, una técnica no intromisiva, es decir, dado que no interviene en el comportamiento de los fenómenos, no crea observaciones contaminadas. Finalmente, el análisis de contenido es capaz de abordar un gran volumen de información, como la que corresponde encontrar al analizar una temática como la que protagonista nuestro estudio [60].

La idoneidad de esta técnica de análisis viene avalada no solo por las razones anteriormente argumentadas, sino por el abanico de estudios precedentes, relativos a la misma temática y en los que se ha usado este método. Es por ello que en la presente investigación hemos resuelto aplicar el análisis de contenido a una serie de estudios académicos motivados por el objeto de estudio de esta tesis, esto es, la vulneración de la intimidad y vida privada en los entornos digitales.

---

de WOLF, M. (1987): *La investigación en comunicación de masas*. Barcelona: Paidós.

57 Ibídem., pp. 28-29.

58 Ídem.

59 Ibídem., pp. 10 y 44

60 Ídem.

Asimismo, como método subsidiario abogaremos por el análisis comparativo. Inclinándonos por esta aproximación metodológica, hemos pretendido no solo descubrir las correlaciones que se producen entre los contextos de vulneración y los flujos informativos en dichos escenarios, sino también inferir las interrelaciones existentes entre esta problemática y el diseño de ciertas aplicaciones, en términos tanto de opacidad de los flujos de información, como de comprensión de la estructura de las herramientas digitales por parte de los individuos. Y, de manera complementaria, procederemos a examinar las actuaciones que los interactores llevan a cabo para preservar sus informaciones privadas. De este modo, podremos descubrir la evolución de la intimidad y vida privada en paralelo al desarrollo, expansión y popularización de las herramientas digitales más usadas, así como inferir sus relaciones con los avatares sociopolíticos del momento en que se producen, ofreciendo una contextualización completa del fenómeno.

1.6.1 **Pasos metodológicos**

Cualquier análisis de contenido ha de hacerse en relación al contexto de los datos y justificarse en función de este. Y el escenario donde surgen los datos nos habla, en este caso, de que hay una preocupación cada vez mayor desde el mundo académico por la intimidad y vida privada, por cuanto los estudios que ha motivado esta temática han aumentado, considerablemente, en los últimos años. Algo que, a su vez, constituye una cierta fuente de certidumbre respecto a la prevalencia e importancia del objetivo perseguido en esta investigación, así como de su pertinencia.

Sin embargo, y dado que la multitud de estudios nacidos en torno a las nuevas tecnologías exceden con mucho las capacidades de esta tesis, para hacer factible el análisis se decidió explorar una muestra limitada pero representativa de la documentación existente, basándonos en ciertos criterios de filtrado. Para ello, como primer paso metodológico se decidió establecer parámetros comunes que arrojasen datos capaces de ser cruzados y comparados. Así, el análisis de contenido fue aplicado a una muestra integrada por estudios e investigaciones que versaban sobre la intromisión en la intimidad y vida privada provocada por las nuevas herramientas tecnológicas. Es preciso

aclarar, no obstante, que aunque la unidad física de análisis escogida se circunscribió a artículos e informes científicos, ulteriormente la visión arrojada tras el escrutinio de estos se completó con otros estudios, entradas de *blogs* y otras fuentes documentales que, en infinitud de ocasiones, apuntalaban los trabajos de los autores.

Para encaminar el análisis de contenido de los artículos se llevó a cabo un primer escrutinio que nos ayudó a identificar si dichas investigaciones versaban sobre las preocupaciones en torno a la protección de la intimidad y vida privada, si se trataba de meras referencias o, incluso, resultados erróneos arrojados por los buscadores. Paso capital, este último que nos permitió hacer una primera criba del extenso material encontrado y contar con una cierta homogenización que permitiera su análisis. A este respecto, el análisis de contenido se aplicó, exclusivamente, a aquella muestra de artículos científicos que había pasado la primera selección, examinando la relación existente entre las unidades referenciales que citaremos en el siguiente apartado. En definitiva, nos inclinamos por una metodología cualitativa deductiva caminando, mediante el uso de la inferencia, de lo general a lo particular; explorando las categorías referentes a ciertos descriptores o términos claves para, posteriormente, analizar el contenido de los aspectos concretos que cada estudio ha priorizado con respecto a la temática analizada.

Aunque puede afirmarse que, prácticamente, todos los análisis de contenido y comparativos son diferentes entre sí y que cada disciplina usa esta técnica desde parámetros distintos, sí podemos afirmar que la generalidad de los estudios seleccionados comparte una lógica de composición, una forma de razonamiento y, por supuesto, ciertos criterios de validez[61]. Esta homogeneización se consigue gracias al cruce de variables, en tanto que es la variación, afirma Krippendorff lo que permite que los datos sean informativos[62]. En consecuencia, la correlación de dichas referencias ha sido determinante para trazar las líneas del mencionado dilema en relación no solo al desarrollo de las aplicaciones informáticas, sino al papel desempeñado por el individuo.

En una segunda vertiente más teórica, la investigación aborda los flujos de información observados tras el análisis comparativo, bajo el

---

61 KRIPPENDORFF, K. (1990): *Op. cit.,* p. 88.

62 Ídem.

prisma teorético aportado por Helen Nissenbaum basado en la protección de la vida privada en función del respeto a la integridad del contexto. A través de dicho marco, se pretende evaluar no solo el nivel de información que recibe el usuario y su capacidad de entendimiento de los entornos digitales, sino determinar los vínculos y correspondencias con las herramientas tecnológicas que más problemas suscitan, así como con ciertas prácticas no leales de las empresas de redes sociales.

1.6.2 **Criterios específicos para la selección**

Para realizar la selección de los estudios científicos a analizar delimitamos un período de estudio que abarcó desde el año 1995 hasta 2014; es decir, desde el despegue de Internet a nivel global hasta la actualidad, un ciclo suficientemente prolongado como para evaluar, con una cierta perspectiva, los efectos producidos por las interacciones de las tecnologías digitales. Si bien cabe indicar que una gran parte de los estudios finalmente analizados correspondieron al período comprendido entre los años 2004 y 2014, por cuanto el despegue de la Web 2.0 y, particularmente, de las redes sociales como herramienta arquetípica, ha disparado el número de publicaciones destinadas a solventar los dilemas asociados. Dicha primera observación nos llevó a centrar el presente texto en este período de tiempo, por considerar que era un lapso suficientemente convulso como para demandar un análisis pormenorizado.

La elección de estos estudios se acometió mediante palabras clave referidas a los conceptos «intimidad» y «vida privada», así como los descriptores basados en sus sinónimos o relacionados con su campo semántico como, por ejemplo: «ámbito íntimo», «esfera privada» o «espacio privado», entre otros. Son las unidades referenciales en la terminología del análisis de contenido funcional de Krippendorff. Posteriormente, dichas unidades se cruzaron con otras relativas a las redes sociales para obtener interacciones entre ambos campos y, subsiguientemente, un significado. Entre dichas categorías aparecían también descriptores como «tecnologías digitales», «Web 2.0» o «Internet», dado que la violación de la intimidad y vida privada en las redes sociales va más allá de los límites propios de las plataformas, pues se produce una alta interacción con otras herramientas externas.

Por otra parte, en una investigación con una material tan extenso como la presente, la necesidad de interponer elementos de filtrado se

antoja sustancial para garantizar una cierta efectividad en el desarrollo de la misma. Comentar la existencia de ese cribado inicial se torna necesario para clarificar los límites iniciales de los que parte el estudio, así como las demarcaciones que, posteriormente, reflejarán los resultados.

Respecto a dicha selección inicial debemos advertir que, si bien es cierto que en ningún momento se pretendió establecer un filtro por regiones o zonas geográficas, la realidad es que la mayoría de los estudios provienen de unos determinados países punteros en esta clase de investigaciones. El motivo lo encontramos, como veremos a lo largo de esta tesis, en la propia evolución y desarrollo de la tecnología digital, anclada, desde su origen, en una serie de Estados, lo que, a su vez, provoca que sean los únicos que posean una producción científica considerable al respecto. Por otra parte, tal y como ya indicara la UNESCO[63], el nivel de desarrollo de las tecnologías aparece ligado al nivel socioeconómico de los países, por lo que si bien los problemas sobre intimidad y vida privada resultan primordiales en los países más industrializados, no así en los países en vías de desarrollo cuyo principal problema es el acceso a las herramientas interactivas.

Del mismo modo, es preciso añadir que en dicha selección se excluyeron todos aquellos documentos sobre intimidad y vida privada que no se refirieran, explícitamente, a las tecnologías digitales; al igual que se obviaron los relativos a dichas herramientas en relación a otros dilemas éticos, pese a haber encontrado, en un gran número de estos, referencias a la temática estudiada. Por todo ello, entendemos que la necesidad de posteriores estudios queda palpable, en tanto que son innumerables los conflictos entre el sustrato digital y ciertos derechos inalienables del ser humano como, por ejemplo, el acceso a la información.

1.7 FUENTES DE LA INVESTIGACIÓN

1.7.1 **Fuentes primarias**

Dada la naturaleza de nuestra investigación, la fuente primordial de la que emana el análisis contenido se constituye de los artículos

---

[63] UNESCO (2005): *Op. cit.*

científicos analizados, que cubren el período temporal indicado y que se encuentran reseñados en el capítulo *Anexos* del presente trabajo. Dichos estudios aparecen, en su mayoría, en revistas científicas y actas de congresos, y su búsqueda documental se ha centrado, como ya hemos adelantado, en el cruce de binomios referentes a los campos semánticos: «intimidad y/o vida privada y/o informaciones privadas/personales y/o datos privados/personales» y «redes sociales y/o Internet y/o Web 2.0 y/o tecnologías de la comunicación y/o la información y/o espacios mediados», sin descartar el cruce de otras variables parejas basadas en dichos descriptores.

1.7.2 **Fuentes secundarias**

Posteriormente, dichos artículos se completaron con otras publicaciones que, a nuestro juicio, resultaban imprescindibles por cuanto se mencionaban en los trabajos analizados o, en cierta medida, los cumplimentaban. La elección de estas revistas, libros y otros materiales documentales se perpetró al comprender la gran cantidad de textos que se habían publicado en relación a la citada temática. Así, las fuentes secundarias se nutren de un amplio abanico bibliográfico y hemerográfico, paso necesario para arrojar luz en la problemática descrita y que, además, ha contribuido a trazar los contornos de esta investigación.

Para la compilación completa de este material, tanto el primario como el complementario, se ha acudido, fundamentalmente, a los centros académicos, instituciones y bibliotecas que mencionamos a continuación:

— Biblioteca de la Facultad de Ciencias de la Información. Universidad Complutense de Madrid.

— Biblioteca de la Facultad de Filosofía. Universidad Complutense de Madrid.

— Biblioteca de la Facultad de Derecho. Universidad Complutense de Madrid.

— Biblioteca de la Facultad de Sociología y Ciencias Políticas. Universidad Complutense de Madrid.

— Biblioteca Nacional.

— Bibliothek Karlsruher Institut für Technologie.

— Bibliothek Fraunhofer-Institut für Sichere Informationstechnologie (SIT).

— Bibliothek Institut für Kulturanthropologie und Europäische Ethnologie. Goethe-Universität Frankfurt am Main.

— Bibliothekzentrum Geisteswissenschaften. Goethe-Universität Frankfurt am Main.

— European Centre for Security and Privacy by Design (EC SPRIDE). Technical University Darmstadt.

— Universitätsbibliothek Johann Christian Senckenberg. (Biblioteca Central) Goethe Universität Frankfurt Am Main.

Asimismo, las principales bases de datos usadas para la recopilación del *corpus* bibliográfico y hemerográfico son las siguientes:

— ARIADNA, catálogo automatizado de la Biblioteca Nacional.

— ACM, Digital Library.

— COMPLUDOC, base de datos multidisciplinar, de artículos de revistas.

— DISSERTATION ABSTRACTS, Tesis defendidas en las universidades norteamericanas y europeas entre los años 1997 y 2000.

— ISOC, base de datos en Ciencias Sociales y Humanidades desde 1975.

— Katalog der Bibliotheken der Goethe-Universität Frankfurt am Main.

— KVK Karlsruher Virtuelle Katalog, Karlsruher Institut für Technologie.

— Suchportal Frankfurt am Main Universitätsbibliothek.

— TESEO, Tesis españolas del Consejo de Universidades.

Para completar la compilación de artículos científicos, recurrimos a algunas de las principales revistas académicas. Su consulta nos ayudó, además, a centrar el campo estudiado:

— *Ámbitos. Revista Internacional de Comunicación.*

— *Comunicar.*

— *Communication Quarterly.*
— *Comunicación y Sociedad.*
— *Communication Research Report.*
— *Communication Research Trends.*
— *Communication Theory Review.*
— *Convergence: The International Journal of Research into New Media Technologies.*
— *Cuadernos de Información y Comunicación (CIC).*
— *European Journal of Communication.*
— *Ethical Space. Internacional Journal of Communication Ethics.*
— *First Monday, Free Journal of University of Illinois.*
— *German Law Review.*
— *Harvard Law Review.*
— *Human Communication Research.*
— *Information Ethics.*
— *Journal of Broadcasting and Electronic Media.*
— *Journal of Communication.*
— *Journal of Computer-Mediated Communication.*
— *Journal of Information, Communication and Ethics in Society, JICE.*
— *Journal of Mass Media Ethics.*
— *Mass Communication on Society.*
— *Media, Culture and Society.*
— *Media Ethics.*
— *MIS Quarterly.*
— *New Media and Society.*
— *Nordicom Review. Journal from the Nordic Information Centre for Media and Communication Research.*
— *Recherches en Communication.*
— *Revista Internacional de Ciencias Sociales.*
— *Revista Latina de Comunicación Social.*

— *Tecnoscienza, Italian Journal of Science & Technology Studies*.

— *Zer, revista de Estudios en Comunicación*.

Así como a las actas de congresos que periódicamente se celebran centrados en esta problemática:

— ETHICOMP, Ethics and Computer International Congress.

— IEEE Security & Privacy.

— Proceedings of ACM Workshop on Privacy in the Electronic Society.

— PNAS.

— Proceedings of the Conference on Human Factors in Computing Systems (SIGCHI /CHI)

Además de los estudios y monografías sobre este campo, se han consultado boletines internos y actas de diversas asociaciones, los informes realizados por organismos internacionales a colación de la vulneración de la intimidad y vida privada, así como los informes publicados por los estados que se han anticipado en su regulación. Entre ellos, destacamos los elaborados por:

— Agencia Española de Protección de Datos (AEPD). España.

— Alto Comisionado Alemán.

— Americam Civil Liberties. Estados Unidos.

— Asociación de Usuarios de Internet (AUI). España.

— Comisión Europea y Grupo de Trabajo del Artículo 29[64]. Unión Europea.

— Comisión de Protección de Datos de Irlanda.

— Comisión de Privacidad de Canadá

— Deutsche Akademie der Technikwissenschaften (ACATECH). Alemania.

— Electronic Privacy Information Centre (EPIC). Estados Unidos.

---

[64] El Grupo de Trabajo del Artículo 29 es un órgano creado en virtud del artículo 29 de la Directiva 95/46/CE e integrado por representantes de las autoridades de protección de datos de los Estados Miembros. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada.

— Electronic Frontier Foundation (EFF). Estados Unidos.
— European Network and Information Security Agency (ENISA). Unión Europea.
— Federal Trade Commission (FTC). Estados Unidos.
— Grupo Europeo de Ética en Ciencia y Nuevas Tecnologías (EGE). Unión Europea.
— Instituto Nacional de Tecnologías de la Comunicación (INTECO). España.
— Information Security Agency. Unión Europea.
— Internet Society (ISOC). Spanish and English Chapter. España y Reino Unido.
— Office of Communications (OFCOM). Reino Unido.
— Pew Internet and American Life Project, Estados Unidos.
— Privacy Right Clearinghouse, Estados Unidos.
— The International Working Group on Data Protection in Telecommunications, (IWGDPT). Unión Europea.

Dichos estudios y el amplio espectro bibliográfico relacionado se han cumplimentado con informaciones periodísticas para contextualizar y tomar el pulso a la actualidad que rodea el fenómeno, lo que nos ayudará a visualizar la coyuntura que enmarca el objeto de estudio durante los eventos mencionados. Todo ello, nos ha servido para nutrir la investigación, toda vez que nos ha otorgado las líneas básicas de actuación.

1.8 PROBLEMAS DE BASE Y PRESUPUESTOS TEÓRICOS

1.8.1 **La delimitación del marco situacional o acotación geográfica**

El marco situacional establece límites de espacio y temporales del evento a estudiar, sugiriendo los alcances y dimensiones a los que se quiere llegar mediante la reflexión crítica de los resultados obtenidos. Sin embargo, delimitar una zona geográfica de influencia a la que circunscribir el estudio de los efectos de las tecnologías digitales en el ámbito reservado del ser humano resultaría un intento sesgado desde el comienzo y, por esencia, imposible, en tanto que el único linde que

encontramos en la Red es la globalidad. Sí resulta necesaria, no obstante, una aclaración: el material analizado y los estudios citados se circunscriben a documentos provenientes de Europa y Norteamérica en su mayor parte, así como de otros países industrializados que se encuentran en un estadio de desarrollo, implantación y acceso a Internet muy similar. La razón se encuentra implícita en la propia historia y evolución de la tecnología digital, así como su posterior progresión, lo que provoca que sean estos países los que posean una mayor producción científica al respecto.

No nos atrevemos a predecir, por tanto, cómo evolucionará esta problemática en otros países con un recorrido menor en el uso de estas aplicaciones informáticas, ni en países con circunstancias políticas concretas, como es el caso de China y que merecerían, sin duda, un estudio pormenorizado. Sin embargo, intuimos que dado que en Internet los patrones se reproducen a gran escala y en cualquier zona geográfica, el resto de países ofrecerá una evolución muy similar en lo que respecta a los dilemas asociados a la salvaguarda de la vida privada.

Por otra parte, si bien no podemos adelantar cuál será la situación de los países con menos investigaciones científicas sobre el tema, sabemos que cuando se produce una intromisión en la intimidad y vida privada de un usuario esta repercute a nivel global, por cuanto la propia naturaleza de las tecnologías provoca que no estén circunscritas a un ámbito territorial concreto. Por ello, y aunque en muchos casos los resultados obtenidos puedan observarse como una generalidad o, por el contrario, como complicaciones asociadas a los usos propios de una determinada sociedad, el hecho de que se trate de un fenómeno de alcance universal provoca que la acotación geográfica sea ineficiente en una investigación de estas características, motivo por la que decidimos no incluir la mencionada delimitación en el título de la misma.

1.8.2 **La acotación temporal**

En un primero momento decidimos analizar la evolución de las intromisiones en la intimidad y vida privada abarcando el período que va desde la popularización de Internet en el año 1995, hasta el presente 2014, siguiendo la línea ya iniciada en la investigación para

la obtención del Diploma de Estudios Avanzados (DEA) y que precede a esta tesis. No obstante, ulteriormente nos percatamos de que los problemas que aparecían en la Web 2.0 contenían todas aquellas situaciones que ya habían aparecido anteriormente, aumentando, eso sí, su complejidad. Por otra parte, al analizar la muestra de artículos que van desde el año 1995 en adelante, encontramos cómo entre los años 2004 y 2014, coincidiendo con la popularización de las herramientas de la Web 2.0, el número de publicaciones centradas en la problemática aumentaba exponencialmente. Dicha observación nos llevó a establecer el punto de mira del presente escrito en este período de tiempo, por considerar que los datos arrojarían una serie de conclusiones ampliamente representativas y que la enorme cantidad de estudios aparecidos entre estos años demandaba una incursión pormenorizada.

1.8.3 **Problemas de base inherentes a la propia metodología**

Mediante esta investigación pretendemos realizar la radiografía de una problemática presente en la sociedad y de creciente interés para, posteriormente, brindar soluciones eficientes aplicables en el mundo real. Sin embargo, no debemos obviar que la arbitrariedad es un ingrediente sustancial de los fenómenos simbólicos y, por ende, el contenido, tal y como indica Krippendorff, «no siempre constituye una cualidad absoluta u objetiva de las comunicaciones»[65], menos aún, conviene aclarar, si a esta ecuación le sumamos la subjetividad que conforma la propia interpretación. Empero y aunque indudablemente las metodologías no son por definición infalibles y los parámetros seguidos en cualquier investigación pueden ser mejorables, durante el desarrollo del presente estudio hemos intentado que nuestro quehacer avanzase motivado por la rigurosidad y exactitud deseables y necesarios para ofrecer unos resultados bien argumentados. Quién sabe si, indirectamente, hemos abierto la senda a futuras investigaciones que irán desentrañando la multitud de realidades que se encuentra en la maraña conformada por la relaciones entre el ser humano y las tecnologías.

---

[65] KRIPPENDORFF, K. (1990): *Op. cit.,* p. 22.

1.8.4 Concreción del objeto de estudio y justificación del título

Es posible que, a estas alturas, el lector se esté preguntando por qué en el título de esta investigación citamos Internet en vez de mencionar exclusivamente las redes sociales. Pues bien, no se trata de un error en la delimitación del campo de estudio, sino una complejidad más añadida a las atribuciones del universo digital. La razón tiene que ver con el hecho de que, dado que en la Web relacional todo está conectado, lo que sucede dentro de una red social es susceptible de obtener su correlato en la Red general, esto es, en Internet. Más aún, cuando el intercambio de datos que tiene lugar en estas herramientas de comunicación a menudo va más allá de sus confines. La indexación de los datos de los perfiles públicos por defecto, el trasvase de contenidos a terceras empresas asociadas y otras coyunturas similares que aparecen anejas a estas herramientas provocan que las informaciones privadas de los usuarios desborden, con creces, los cauces delimitados por las propias plataformas. En definitiva y como podremos comprobar en el capítulo *Análisis,* las intromisiones en el ámbito privado que se producen en estos espacios, aparentemente acotados de la Web, se traducen a la postre en injerencias acontecidas en todo el amplio espectro Internet.

2. ESTRUCTURA DE LA PRESENTE INVESTIGACIÓN

Una vez aclarados los principios que centrarán nuestro empeño en esta investigación, se impone establecer un esquema que guíe nuestro recorrido, más aún, teniendo en cuenta la complejidad del asunto que nos ocupa. Es por ello que un tema tan extenso y difuso requiere ser debidamente seccionado y dispuesto, de ahí los capítulos que lo conforman y su división interna. Asimismo, la exposición se presentará aliñada con una breve introducción a cada capítulo y un balance final donde se recoge la síntesis y principales reflexiones extraídas del mismo, con el objetivo en mente de facilitar al lector el acceso a los datos presentados y a la lectura crítica.

Antes de comenzar nuestro análisis, resulta necesario aportar un marco sólido capaz de soportar una problemática tan confusa y, en ocasiones, polifacética como es la protección de la intimidad y vida privada en este mundo interconectado en que se constituye la Era

Digital. En definitiva, el objetivo último de esta parte de la investigación es hallar un sostén conceptual inequívoco que podamos aplicar durante su desarrollo. Comenzamos, por ello, con un potente *corpus* teórico destinado a esclarecer qué realidades intervienen cuando referimos la relación entre vida privada y tecnología. Este *Marco conceptual* se conforma de tres capítulos destinados a esclarecer los pilares fundamentales que protagonizarán el posterior análisis. Así, en el *Capítulo II* se analizan a fondo los significados contenidos en los vocablos «intimidad» y «vida privada», y se aborda su protección desde el marco legislativo. Posteriormente, el *Capítulo III* surge encaminado a explicar el universo digital y las características de los entornos mediados por las tecnologías, contextualizando este fenómeno mediante el repaso de sus antecedentes y la definición de los principios en que se sustenta. Una vez detalladas dos de las constantes substanciales, esto es, la intimidad y vida privada de un lado e Internet y los escenarios digitales de otro, resulta imprescindible observar la confluencia entre ambas, una mixtura en la que observaremos propiedades específicas que no presentan dichas realidades por separado. Consecuentemente, en el *Capítulo IV* se expone el cambio de perspectiva en la protección y concepción de lo privado, transformación que comienza ligada al desarrollo de los medios de comunicación de masas tradicionales y que alcanza su máximo apogeo con el advenimiento de las herramientas relacionales digitales. Lejos de ser superfluo, este paso se torna necesario para introducir al lector en el marco teórico al que nos remitiremos en la resolución de esta tesis, esto es, la integridad contextual.

Partiendo de este soporte crítico, comenzaremos la tercera parte o *Análisis* propiamente dicho, desgranando, en distintos bloques temáticos, los diversos puntos de conflicto. En este sentido, la tesis cubrirá una serie de capítulos que tendrán como misión abordar en profundidad el objeto de estudio, desde la fecha de partida hasta la actualidad. Este apartado aparece dividido en capítulos debidamente fraccionados, contextualizados y, en ocasiones, organizados cronológicamente; de esta manera se pretende, a la vez, resumir los acontecimientos más sobresalientes en relación a la cronología que se les adscribe. Obtendremos, a este tenor, una instantánea definida de todas aquellas intromisiones en la intimidad y vida privada de los usuarios, acaecidas a raíz de la interacción con las redes sociales digitales.

Finalmente, en el capítulo *Discusión,* examinamos los flujos de información detectados durante el análisis precedente, pasándolos por el tamiz de la integridad contextual. Como colofón, tras un balance de las etapas estudiadas y comprobar las hipótesis de partida, daremos paso a la presentación de una serie de propuestas destinadas a minimizar la problemática, así como a los hallazgos finales extraídos del estudio.

En otro orden de cosas, conviene puntualizar que esta tesis se desarrolla con arreglo a la denominación de *Doctorado Europeo* o *Mención Europea,* lo que implica que, en su mayor parte, el desarrollo de la misma se realizará en castellano, salvo una serie de capítulos que se presentarán en inglés, idioma elegido para su presentación y defensa. Se ha perseguido, por ello, una cierta coherencia tanto en las notas a pie de página, como en las acotaciones y citas textuales, por lo que los textos que aparecen en los capítulos lo harán en el idioma correspondiente, ya sea bien porque la obra tiene una edición en dicha lengua o por traducción de la propia autora al idioma de dicho capítulo.

Es posible que la complejidad del fenómeno no permita analizar toda la variedad de interrelaciones en conjunto con la intensidad que nos gustaría, pero sí efectuaremos aproximaciones sobre algunos de los aspectos principales de la sociedad actual que bien merecen ser reseñados. En este escenario, marcado por el cambio y la complejidad, nacen estas páginas encaminadas a clarificar una de las controversias que más informaciones protagonizan en los medios de comunicación, más inquietudes suscitan en el ámbito científico y, por encima de todo, más lastran el satisfactorio uso y potencial de las tecnologías digitales.

El deseo no es otro que el lector disfrute tanto de la lectura de este trabajo, como la que suscribe estas líneas en su confección.

PARTE II

MARCO CONCEPTUAL Y ACLARACIÓN DE TÉRMINOS

CAPÍTULO II. LA INTIMIDAD Y LA VIDA PRIVADA

SÍNTESIS

La presente tesis doctoral aparece enmarcada bajo el título: La protección de la intimidad y vida privada en Internet: La integridad contextual y los flujos de información en las redes sociales (2004-2014). Para acotar y definir el espectro teórico en el que navegaremos en las siguientes páginas, resulta preciso realizar, antes de adentrarnos en el análisis en sí, las aclaraciones pertinentes respecto al significado de los conceptos usados. Así pues, el mejor punto de partida para situar al lector en el marco apropiado para la comprensión del estudio consiste en la demarcación semántica de las siguientes locuciones, claves en la totalidad del texto: la «intimidad y vida privada», que constituye el objeto de estudio; «Internet» y la «Web 2.0», ecosistema al que se circunscribe y, finalmente, la confluencia de ambos mediante la explicación de la perspectiva aportada por la integridad contextual.

En este primer capítulo del Marco Conceptual nos centraremos en la concreción de términos referentes al campo semántico de la vida privada, desgranando sus atribuciones y abordando, ulteriormente, tanto los diversos aspectos que la conforman, como su protección desde el ámbito jurídico.

1. INTRODUCCIÓN: LA INTIMIDAD Y VIDA PRIVADA, CONFUSIÓN ENTRE AMBOS TÉRMINOS Y AMBIGÜEDADES TERMINOLÓGICAS

Salvo contadas excepciones[66] habitualmente los términos «intimidad» y «vida privada» son usados como sinónimos de manera erró-

---

[66] Estas excepciones corresponden a José María Desantes Guanter, Miguel Urabayen y Norberto González Gaitano. DESANTES GUANTER, J. M. (1972): «Intimidad e información, derechos excluyentes», en *Nuestro tiempo*, n.º 213. Pamplona, p. 18; GONZÁLEZ GAITANO, N. (1990): *El deber de respeto de la intimidad. Información pública y relación social*, Pamplona: Eunsa, p. 16.;

nea, tanto en lenguaje cotidiano como en literatura jurídica. Esta asimilación entre dos voces que poseen semánticas distintas responde, según alude González Gaitano, a razones históricas y filológicas. Aunque la palabra «privacidad» deriva del latín *privatus*, se ha incorporado a nuestra lengua en los últimos años a través de la construcción anglosajona *privacy,* por lo que el término es tachado de anglicismo y rechazado en favor de la voz «vida privada».

Por su parte, en el caso de la voz «intimidad» el análisis terminológico, tanto de la lengua castellana como de la inglesa, verifica la procedencia latina del concepto, cuya esencia semántica se distingue de la contenida en el vocablo *privacy*. Si bien, ambas voces son usadas como sinónimos erróneamente tanto en la tradición jurídica como en el lenguaje cotidiano. Según afirma Desantes Guanter, en sentido etimológico «íntimo» procede del latino *intimus* que es una variación filológica de *intumus*, forma superlativa del verbo *intus*, «dentro»[67]. «Íntimo» e «intimidad» refieren, en consecuencia, a aquello que está lo más dentro posible, a lo más reservado y lo más profundamente sentido por el ser humano.

En el caso de la lengua inglesa, fueron los vocablos *intimity* e *intimacy* los dos términos provenientes del latín *íntimus*. Sin embargo, rara vez se usan dichas voces para referirse a «lo más íntimo» o «reservado» del sujeto y su campo semántico original fue ocupado por la palabra *privacy*:

> La lengua inglesa posee otros términos distintos para designar la intimidad —*intimity* e *intimacy*— pero también tienen un valor eufemístico para designar las relaciones sexuales ilícitas, por el que se usan menos y su campo semántico original es ocupado por el de la palabra *privacy*. […] Al pasar a otros idiomas se ha mantenido la ambigüedad y se habla indistintamente, por ejemplo en castellano, de derecho a la intimidad o derecho a la vida privada. Como la tradición jurídica anglosajona en el tratamiento del tema fue la primera, y la más abundante, ha influido notablemente en el resto de países y no solo desde el punto de vista léxico, sino también en el contenido doctrinal.[68]

URABAYEN, M. (1977): *Vida privada e información: Un conflicto permanente*, Pamplona: Eunsa, pp. 9-19.

67 DESANTES GUANTER, J. M. (1972): *Op. cit.,* p. 18.

68 GONZÁLEZ GAITANO, N. (1990): *Op. cit.,* p. 16.

El origen de esta confusión entre ambas voces proviene de la traducción de la locución inglesa que da origen al derecho y que se formula por primera vez en 1890, bajo la expresión «*the right to privacy*»[69]. Para González Gaitiano, este uso indiscriminado e imposición de la voz *privacy* ha producido «la pérdida de la dimensión más profunda de intimidad, es decir, la que designa lo más interior de la persona, en beneficio del carácter de ocultamiento *[privacy]*»[70]. En la misma línea, la socióloga Helena Béjar señala que esta confusión de conceptos se debe a la difícil correspondencia del término inglés con el castellano y que, indistintamente, es traducido con adjetivaciones como «lo privado» o nombres como, «esfera o vida privada» e «intimidad», sustantivos no sinónimos[71].

1.1 CONCEPTUALIZACIÓN DE LA INTIMIDAD

Retomando, pues, su etimología primigenia, la intimidad del ser humano correspondería a esa realidad de índole inmaterial, relativa a lo más nuclear de la persona y que, además de ser reservada, tiene el valor de algo genuino: «La intimidad en sentido más propio engloba también el conjunto de emociones, sentimientos y estados de ánimo que constituyen la vida afectiva»[72].

En este sentido, la idea de intimidad refiere a todos aquellos pensamientos, deseos, sueños, intenciones, fantasías, imaginaciones y creencias que solo una persona sabe o conoce, algo que no se comunica a nadie y que uno se lleva consigo tras su muerte. La intimidad no se opone a lo privado, pero aún compartiendo ciertas atribuciones sí se distingue de la substancialidad de esta esfera. Y si es comunicada a otra persona, aun cuando esto se produjese en el propio ámbito de

---

69 WARREN, S. y BRANDEIS, L. (1890): «The right to privacy», *Harvard Law Review*, vol. IV, n. 5. pp. 193-220. Traducción a cargo de PENDÁS, B. y BASELGA, P. (1995): *El derecho a la intimidad.* Madrid: Civitas.

70 GONZÁLEZ GAITANO, N. (1990): *Op. cit.,* p. 22.

71 BÉJAR, H. (1988): *El ámbito íntimo: privacidad, individualismo y modernidad,* Madrid: Alianza, p. 784.

72 CHOZA ARMENTA, J. (1980): *La supresión del pudor y otros ensayos*. Pamplona: Eunsa. p. 26.

lo privado, al ser conocida y volverse una realidad tangible, dejaría de ser intimidad como tal.

Por ello, dado que la intimidad se sitúa en el recinto interno de cada persona donde se forjan las decisiones más propias e intransferibles[73] y que dicha voz engloba aquellos aspectos de nosotros mismos que, por esencia, no son conocidos por los demás, se constituye como una suerte de «derecho al secreto» sobre lo que somos, pensamos o hacemos[74]. Lo íntimo se relaciona con soledad, con reserva y «se refiere a una persona en sus relaciones consigo misma»[75].

En este sentido, el principal rasgo definitorio de la intimidad es que forma parte de la esencia misma de la personalidad y, por ende, es inherente a todos los seres humanos[76], a la persona, «sustancia primera, completa e individual» según Aristóteles[77], como ser racional. La intimidad es, consiguientemente, una parte esencial de la creación de la identidad, esto es, de la consolidación del «yo».

Tanto la vida pública como la vida privada son términos relativos que se definen por contraposición uno del otro, pero la intimidad está a un lado de esta dialéctica, en un plano distinto y absoluto que no varía por cuanto aparece ligada de forma substancial al ser humano: «Se puede recortar el espacio de vida privada de una persona hasta el límite, hasta suprimirlo, sin que se destruya la persona, le queda el refugio inaccesible de su intimidad; en cambio si se destruye la intimidad la persona se volatiliza»[78]. Esta característica de la intimidad ya fue mencionada por Samuel D. Warren y Louis D. Brandeis al referirse al derecho a disfrutar de espacios de soledad, no como una extensión del derecho de propiedad, sino como una dimensión de la propia dignidad humana[79].

---

73 GARCÍA FERNÁNDEZ, D. (2010): «El derecho a la intimidad y el fenómeno de la extimidad» en *Dereito*, vol. 19, n.º 2, pp. 269-284, p. 271

74 GARCÍA SAN MIGUEL, L. (1992): *Estudios sobre el derecho a la intimidad*. Madrid: Tecnos. p. 17.

75 URABAYEN, M. (1977): *Op. cit.,* pp. 9-19.

76 GARCÍA MORENTE, M. (1972): *Ensayo sobre la vida privada*. Madrid: Universidad Complutense. p. 55.

77 ABBAGNANO, N. (1980): *Diccionario de Filosofía*, México: Fondo de Cultura Económica, p. 909.

78 GONZÁLEZ GAITANO, N. (1990): *Op. cit.,* p. 45.

79 WARREN, S. y BRANDEIS, L. (1890): *Op. cit.,* pp. 193-220.

La intimidad es, pues, un factor de individualización, un «recinto secreto del alma»[80] que hace al ser humano ser quien es y que, por tanto, no es objetivable «desde fuera» ni objeto de derecho[81]. Del mismo modo, posee otras diferencias respecto a la vida privada por cuanto el conocimiento de esta, aun cuando sea intrusivo, no la destruye, mientras que la intimidad pierde su condición cuando es conocida[82]. En consecuencia, señala Gaitano, intimidad y vida privada son realidades distintas, aunque relacionadas.

Queda patente, sin embargo, que el hecho de que la noción de intimidad posea un fuerte contenido emocional, compuesto en muchos casos de sentimientos, creencias o modos de conductas personales no tangibles, provoca dificultades a la hora de describir el concepto, cuestionándose, autores como Urabayen, si puede ser satisfactoriamente definido.

1.2 CONCEPTUALIZACIÓN DEL VOCABLO «PRIVACY» O VIDA PRIVADA

Señalaba Alan Westin que «ninguna definición de *privacy* es posible porque lo concerniente a la vida privada es, fundamentalmente, una cuestión de valores, intereses y poder»[83]. En la misma línea, Urabayen nos alerta de cómo el campo de la vida privada aparece gobernado «en parte no desdeñable por las modas y las costumbres de la sociedad de la que forma parte, sujetas a cambios considera-

---

80 LAÍN ENTRALGO, P. (1985): La intimidad del hombre. Homenaje a Antonio Maravall. Madrid: CIS, p. 379.

81 GONZÁLEZ GAITANO, N.: «¿Deber de respeto a la intimidad o derecho a la intimidad?», en Innerarity, D. y Vaz, A. (ed.) (1987): *Información y derechos humanos. Actas de las I Jornadas de Ciencias de la Información*. Pamplona: Eunsa, p. 129.

82 En este sentido se pronuncian: DESANTES GUANTER, J. M. (1972): *Op. cit.;* VIDAL MARTÍNEZ, J. (1980): «La protección de la intimidad de la persona en el ordenamiento positivo español», en *Revista de derecho privado,* julio y agosto, Madrid, pp. 755-774; y BOIX REIG, J. (1983): «Consideraciones sobre la protección penal de la intimidad y del honor e informática», en *Anales de la Universidad de Alicante,* n.º 2.

83 WESTIN, A. (1967): *Privacy and freedom.* New York: Athenaeum, p. 369.

bles, especialmente en nuestro tiempo»[84]. Razón no les faltaba a ambos[85], pues como veremos a lo largo de este escrito la noción aludida por la locución «vida privada» nos introduce de lleno en el alambicado terreno de la subjetividad humana, derivando en un concepto relativo cuya indefinición dificulta, en ocasiones, su propia protección.

Resulta certero afirmar que la ambigüedad que lastra la definición del concepto aparece ligada al desarrollo más amplio que la esfera privada del individuo experimenta con la llegada de la modernidad y que se acentuará a partir del s. XX, tras la aparición de los medios de comunicación de masas. Pero antes de valorar los cambios en la delimitación de la vida privada en los tiempos contemporáneos, tarea que emprenderemos en el siguiente capítulo, realicemos ahora una primera demarcación de las atribuciones de «lo privado».

2. DIMENSIONES DE LA VIDA PRIVADA

Señala Béjar que se pueden distinguir dos grandes dimensiones en la vida privada. De un lado, la dimensión descriptiva que establece relaciones con conceptos afines pero no sinónimos como son: «intimidad», «secreto» o «soledad». En esta dimensión se hace referencia a la naturaleza de la persona, a su «yo» (en clara alusión al campo semántico referente a la intimidad) y al ámbito sagrado del individuo (secreto, soledad y apartamiento). Por su parte, la dimensión normativa da lugar a la expresión «derecho a la vida privada» (consagrado como «derecho a la intimidad» en nuestro ordenamiento jurídico) y hace referencia al control exclusivo del individuo sobre todo lo relativo a su ámbito privado. Se trata, en este sentido, de una noción sociológica que tiene su origen en la filosofía liberal. Discurramos, con más detenimiento, por estas dos dimensiones para interpretar cumplidamente a qué nos referimos cuando hablamos de «vida privada».

---

[84] URABAYEN, M. (1977): *Op. cit.,* p. 13.

[85] Aunque no es propio de los trabajos científicos valorar, sí convendremos con los autores en el arduo empeño que conlleva la delimitación de la vida privada.

2.1 LA DIMENSIÓN DESCRIPTIVA DE LA VIDA PRIVADA

2.1.1 **Distinción entre «lo público» y «lo privado»**

Perpetuación de la herencia clásica, la distinción entre lo público y lo privado arrastra una larga historia enraizada, según Jürgen Habermas, en el pensamiento social y político occidental.[86] La distinción explícita procede de «los albores de la ley romana que separaban las leyes públicas de las privadas y de la concepción romana de la *res pública*»[87]. Poco a poco, a finales de la Edad Media y comienzos de la moderna, la distinción entre ambos conceptos comienza a tomar otros matices en relación a los cambios institucionales. Es a lo largo de esta evolución cuando aparecen, tal y como señala John Thompson, las dos acepciones o arquetipos principales que caracterizan la dicotomía entre «lo público» y «lo privado». Cabe reseñar, siendo fieles a la evolución de ambos vocablos, que estas no las únicas acepciones dado el nivel de polisemia de ambas voces, aunque sí son las mayoritarias.

La primera acepción distingue entre el dominio del poder político institucionalizado frente a aquellas actividades o esferas de la vida que quedaban excluidas de él, una distinción entre Estado o cualquier actividad asociada a este y el concepto hegeliano de «sociedad civil». Al introducir este concepto, Hegel apunta al cambio más significativo de la modernidad: la separación entre Estado y sociedad, esto es, entre «vida civil» y «vida política», entendiendo que esta se conforma de una esfera de individuos anónimos, organizaciones y clases formalmente distintas de las del Estado, regidas por la ley civil. Incluiría, por tanto, la esfera de relaciones personales que fundamentalmente se daban en la familia. En palabras del historiador francés Georges Duby:

> Se separa un ámbito claramente definido para aquella parte de la existencia para la cual todo lenguaje tiene una palabra equivalente a «privado», una zona de inmunidad a la que podemos retirarnos o en la

---

[86] HABERMAS, J. (1989): *The structural transformation of the public Sphere: an inquiry into a category of Bourgeois society,* UK: Cambridge Polity Press, cap. 1.

[87] THOMPSON, J. B. (1998): *Los media y la modernidad: una teoría de los medios de comunicación.* Barcelona: Paidós, p. 163.

> que podemos refugiarnos, un lugar en el que podemos dejar a un lado las armas o las armadura requerida en el espacio público, relajarnos, ponernos a gusto y descansar sin cobijarnos bajo el ostentoso caparazón que llevamos para protegernos del mundo exterior[88].

Este retiro deseado no implica la soledad, pues lo privado aparece asociado a lo doméstico y a todas las personas con las que se comparte esa esfera. De modo que lo privado, a pesar de coartar la intrusión externa «no es necesariamente tranquilo desde dentro» [89]. Sí alude a la privación en el sentido de negación de las «relaciones sociales genuinas» [90] que se encuentran fuera del ámbito privado, en la «esfera pública», representante en la Grecia clásica de la libertad e igualdad. Dicha distinción, no obstante, nunca fue rígida ni quedó bien definida en el desarrollo histórico de las sociedades modernas, más aun, cuando desde finales del siglo XIX las fronteras entre ambos se han ido desdibujando cada vez más.

> ACLARACIÓN:
>
> La voz «esfera pública» es de uso corriente en las ciencias sociales. Dicho término, retomado por Habermas en los años sesenta, proviene originariamente de Kant, tal y como sostiene Wolton[91]. Empero se hizo popular gracias a la obra de Habermas de 1962: *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft* y que fue traducida al inglés como: *The structural transformation of the public Sphere: an inquiry into a category of Bourgeois society.* Del mismo modo, se puso de moda el uso de la expresión «espacio público», debido a la traducción del título de esta obra al francés como: *L'espace public,* razón por la cual también nos referimos a «espacio público» en castellano. No obstante, tal y como señalan Castañares y Orellana, la traducción más precisa sería la de «esfera pública» o, en su defecto, «principio de publicidad» [92].

---

88 DUBY, G. (1987): «Preface», en Veyne, P. (ed.): *A history of Private Life*. Cambridge y Londres: Harvard University Press.

89 LYON, D. (1995): *El ojo electrónico: el auge de la sociedad de la vigilancia.* Madrid: Alianza. p. 253.

90 Ídem.

91 WOLTON, D. (2000): *Internet, ¿y después?: una teoría crítica de los nuevos medios de comunicación,* Barcelona: Gedisa, pp. 235.

92 QUÉRÉ, L. (1992): «L'espace public: de la théorie politique a la metathéorie sociologique», traducción de Castañares, W. y Orellana, R. (1992): «El espacio público: de la teoría política a la metateoría sociológica», en *Quaderni*,

Prosiguiendo con la segunda acepción de esta dicotomía, «lo público» significa «abierto» o «disponible al público». Para Thompson, lo que es público, en este sentido, es lo que resulta «visible u observable, aquello que se realiza ante espectadores, que se expone a todos o a muchos para que sea visto u oído, o para que tengan noticia de ello»[93], esto implica que se realiza en la arena pública, esto es, la «esfera pública». Lo que es privado, por oposición, es «lo que queda oculto a la mirada, lo que es dicho o realizado en la privacidad o en secreto o dentro de un círculo restringido de personas»[94], lo que corresponde a los actos ejecutados en la «esfera privada». Así enunciada, la dicotomía público-privado tiene que ver con la «apertura» *versus* «secretismo», con la «visibilidad» por contraposición a la «invisibilidad». Esta distinción entre esfera privada y esfera pública resulta relevante por cuanto revela, en palabras de Arendt, «lo que puede ser mostrado y lo que debería permanecer oculto»[95].

Es palpable que, si bien ambas acepciones de esta dicotomía no coinciden, sí es cierto que históricamente, advierte Thompson, existe una compleja y cambiante relación entre las formas de gobierno y la invisibilidad del poder.

Los ámbitos público y privado no se dan independientemente el uno del otro. En consecuencia, «no puede haber transformación de la esfera pública que no sea, al mismo tiempo, una transformación de lo privado»[96] y en esta continua reformulación, en la que ambos ámbitos configuran la naturaleza del otro, «lo público» —observa Giddens— solo se distingue plenamente de «lo privado» cuando se establece, cabalmente, lo que Simmel denomina la «sociedad de extraños»[97]. Y es con el advenimiento de la modernidad y, en la medi-

---

n. 18, pp. 1-25. Quéré realiza además un potente estudio de la naturaleza del concepto por lo que dicho artículo constituye un valioso punto de referencia.

93 THOMPSON, J. B. (1998): p. 166.

94 Ídem.

95 ARENDT, H. (1958): *The Human Condition*, Chicago: University of Chicago Press, p. 72.

96 GOULDNER, A. (1967): *The dialectic of Ideology and technology.* New York: Seabury Press, p. 99.

97 En referencia a la «sociedad de extraños» descrita por Simmel, que definía la existencia privada por la aparición de «los otros». GIDDENS, A. (1990): *Modernity and self-identity*. Cambridge, United Kingdom: Polity Press, y SIM-

da en que los ámbitos público y privado fueron reordenados, cuando la distinción se agudiza. Afirma David Lyon:

> Los estados gobernaban mediante el derecho el dominio público, definiendo legalmente lo privado como el lugar donde las intrusiones de los poderes públicos podían rechazarse legítimamente. De la misma manera, lo que era «privado» lo era porque podía ocultarse de otros. Cuanto más se desarrollan las relaciones anónimas e impersonales en las ciudades en crecimiento de la era moderna, tanto más diferenciadas se hicieron las relaciones privadas[98].

Para Helena Béjar, la historia de la vida privada corre pareja al desarrollo de la libertad del individuo. Lo público da forma al espacio de lo común frente a lo privado, reserva de la separación y diferencia, y que requiere un compromiso constante, una involucración plena del sujeto:

> El primero es un ámbito ya dado y el segundo es una construcción que requiere voluntad e intención. Mutuamente excluyentes, el espacio privado demanda toda clase de atenciones mientras que exige a sus participantes el apartamiento primero y el abandono de la arena pública. Y al hilo de esta polarización significativa de las dos esferas aparece la noción de «vida privada», lugar de la actividad cotidiana, espacio del tiempo pleno, esfera de intensidad vital[99].

Erving Goffman alude a «lo privado» como «las regiones no públicas» de la vida, áreas «fuera de escenario» en las que uno puede relajarse de la exhibición pública, de la interpretación[100]. El desarrollo de la vida privada solo es posible en condiciones de *Gesellschaft,* es decir, dejando un lado las constricciones de la vida comunitaria o *Gemeinschaft*. Una sacralización excesiva de dicha esfera, esto es, cuando el ámbito privado se convierte en refugio para eludir la responsabilidad pública, derivaría en lo que Richard Sennet denomina

---

MEL, G. (1986): *Sociología. Estudios sobre las formas de socialización*. Alianza: Madrid.

98 LYON, D. (1995): *Op. cit.,* p. 255.

99 BÉJAR, H (1988): *Op. cit.,* p. 61.

100 En su obra Erving Goffman utiliza el artificio teatral para reflexionar sobre los distintos ámbitos de la vida. GOFFMAN, E. (1997): La presentación de la persona en la vida cotidiana. Buenos Aires: Amorrortu.

destructive Gemeinschaft[101] una condición no deseable que acabaría por arruinar la arena pública.

Dejando a un lado la concepción extrema mencionada por Sennet, la esfera privada posee otras connotaciones. Todas las concepciones reseñadas, señala De la Válgoma, encierran un sentido negativo de exclusión: «Se trata de una esfera propia, privada donde los demás no tienen cabida. Hay un claro matiz individualista, de la protección de la personalidad en cuanto tal»[102]. Ahora bien, esta connotación cambia y experimenta un matiz positivo a partir de la reformulación de Alan Westin, abarcando el campo de la vida privada la facultad de control sobre nuestras propias informaciones[103]. Es en este reducto de autonomía frente a la «colonización del mundo de la vida»[104], en palabras de Jürgen Habermas, cuando advertimos que la vida privada está intrínsecamente relacionada con la libertad, una condición que discurre en una doble vertiente: frente a las intrusiones del Estado de un lado y, por otro, como facultad de control que nos capacita para revelar únicamente lo que uno desea, a quien quiere y bajo las condiciones elegidas.

Bajo esta premisa, Habermas conceptúa la esfera privada como aquella donde se sitúan las relaciones familiares y personales, por contraposición a la pública, constituida por toda la red de comunicaciones que posibilitan que los individuos anónimos tomen partida en la cultura y la formación de opinión pública[105]. Así pues, la esfera privada es aquella donde los sujetos tienen el máximo control respecto a sus actividades y sus comunicaciones.

Al hablar de potestad sobre nuestras informaciones, observamos como el concepto de autodeterminación subyace a esta nueva libertad que aparece asociada a la vida privada. En este sentido, Enrique Badía afirma:

---

[101] SENNET, R. (1977): *the fall of public man*. United Kingdom: Cambridge University Press, p. 282.

[102] DE LA VÁLGOMA, M. (1983): «Comentario a la ley orgánica de protección civil al honor, a la intimidad y a la propia imagen», en *Anuario de Derechos humanos,* p. 657.

[103] WESTIN, A. (1967): *Privacy and freedom*. New York: Athenaeum.

[104] HABERMAS, J. (1987): *The Theory of Communicative Action*, vol. 2, Boston: Beacon Press, p. 2.

[105] HABERMAS, J. (1989): *Op. cit.,* p. 319.

> Es cierto que la vida privada suele ser confundida, cuando no asimilada, la voluntad o el deseo de mantener el anonimato, permaneciendo total o parcialmente desconocido, inadvertido o no identificado por el gran público y, en la mayoría de los casos, por los diferentes estamentos del poder; sea este estatal o de otra índole, por ejemplo empresarial. Anonimato que, por extensión, se entiende comprensivo de datos, usos, costumbres, hábitos y prácticas de carácter personal. En el entendido de que el derecho individual a preservarlos niega el de otros para acceder a su conocimiento —y uso— sin mediar la voluntad —consentimiento— de su titular[106].

La autodeterminación informativa se considera un derecho fundamental derivado del derecho a la intimidad y se concreta en la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida tanto en registros públicos como privados, especialmente, aunque no exclusivamente, en aquellos almacenados en medios informáticos. La noción proviene de la jurisprudencia alemana: *Recht auf informationelle Selbstbetsimmung* y, en el plano procesal, el derecho sustantivo a la autodeterminación informativa se completa mediante el recurso de *hábeas data*. Dado que dicho concepto engloba la idea del «derecho a la libertad informativa», por cuanto se refiere a las facultades que tiene el individuo con respecto al tratamiento y existencia de sus datos de carácter personal, las nociones «consentimiento» y «conocimiento» adquieren un matiz prioritario.

En definitiva, podemos delinear dos claros aspectos de la vida privada. El primero, negativo, como una sacralización de la persona respecto a los demás, que trata de excluir del conocimiento ajeno cualquier cosa que hace referencia a la propia persona. El segundo aspecto, con un cariz positivo, como el control por su titular de los datos e informaciones relativas a la propia persona.

Esta última acepción es la que da paso, como veremos al estudiar el espectro normativo, a una colisión con el derecho a la información. En este caso, el derecho a la información podrá entrar o no en los espacios de la vida privada en función de lo que se considere interés público o interés general.

---

[106] BADÍA, E. (2012): «Marco conceptual. Derecho ¿pendiente?» en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados*. Madrid: Ariel. p. 5.

No obstante, tal y como sentencia Helena Béjar, en la actualidad «lo privado» poco o nada tiene en común «con aquella esfera de soberanía individual a la que aludían los liberales, por cuanto ya no se entiende el disfrute de la misma como una conquista o un espacio robado a la esfera pública, que remite a un derecho formalmente regulado» [107]. Tampoco se alude a ella como un límite a las intromisiones del poder o de reserva frente al otro. La privacidad moderna, que se identifica con el concepto de «vida privada» (término que usaremos a lo largo de este texto) se representa en «el ámbito dedicado al cultivo de los afectos y la propia intimidad, es algo que se da por sentado en las sociedades democráticas» [108]. Una suerte de privilegio que «para los teóricos del individualismo aparece como una segunda naturaleza [del ser humano, la primera sería la intimidad o el propio ser] como el espacio privilegiado de su cotidianeidad» [109].

2.1.2 **Dominios y límites de la vida privada**

Una vez realizada la pertinente demarcación entre lo público y lo privado, así como entre este y el ámbito íntimo, se torna necesario realizar lo propio respecto a las atribuciones de dichos espectros, esbozando sus límenes y dominios.

Tras su recorrido etimológico, observamos que la noción «intimidad» alude a un significado diferente al representado por «vida privada». Ambas son nociones afines, pero al igual que también lo son: «confidencial» o «reservado» y no se trata de sinónimos ni constituyen su sustantividad. Si bien, aunque la voz «intimidad» refiere a un significado diferente del que envuelve el término «vida privada» (con la noción de intimidad no se designa explícitamente la condición de «apartamiento» u «ocultamiento» sino de «interioridad») ambos comparten una característica común: lo íntimo está oculto al conocimiento ajeno, es decir, comparte con el ámbito privado la ausencia de difusión [110].

---

[107] BÉJAR, H. (1988): *Op. cit.,* p. 240.
[108] Ídem.
[109] Ibídem, p. 241.
[110] GONZÁLEZ GAITANO, N. (1990): *Op. cit.,* p. 18.

La condición propia de la intimidad hace que no tenga lugar tangible en el mundo, debemos remitirnos a la mera abstracción de dicha idea pues es de naturaleza espiritual y, aunque en ocasiones se haga presente en el mundo material a través de la vida privada y la pública, nada tiene que ver con esta jerarquía de conceptos. La intimidad no tiene más límite que la propia persona. Por el contrario, hablar de límites y protección de la vida privada nos situaría en el plano de la realidad palpable.

Tradicionalmente, señala Medina Guerrero[111] se ha acudido a la Teoría de las esferas de Heinrich Hubmann[112] como concepción predominante para perfilar «materialmente» la substancialidad, delimitar las atribuciones y así acometer la protección de la vida privada, tanto doctrinalmente como en el ámbito de la jurisprudencia. Dicha teoría defiende la existencia de diferentes esferas dotadas, cada una de ellas, de diversos niveles de protección, de modo que la inclusión de una determinada información en un nivel u otro resultaría decisiva para resolver las posibilidades de difusión de aquella[113].

Aunque las puntualizaciones de posteriores autores indican que no existe homogeneidad en el contenido abarcado en cada esfera, si hay unanimidad a la hora describir las dos esferas principales: la correspondiente al núcleo, esto es, la que circunda la «esfera intimidad» y la «esfera personal» (que se correspondería con la vida privada). Siguiendo la lógica de esta abstracción, «cuando más se acerque el dato revelado al centro, materialización de la más reservado, mayor relevancia deberá exigirse a la información para considerar que su difusión es constitucionalmente legítima»[114].

Así enunciada o con las modificaciones ulteriores, esta teoría fue largamente criticada ya que, de nuevo, nos topamos con la imposibilidad de objetivar la intimidad. La esfera íntima, que representa la esencia del individuo en tanto que ser físico, esto es: nacimiento, desnudez, enfermedad, muerte y sexualidad; y ser interior: mundo men-

---

111 MEDINA GUERRERO, M. (2005): *Op. cit.,* p. 15.

112 HUBMANN, H. (1957): «Der zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion», en *Juristenzeitung*, pp. 521-528.

113 HUBMANN, H. (1957): *Op. cit.,* pp. 521-528.

114 NEBEN, G. (2001): *Triviale Personenberichterstattung als Rechtsproblem.* Berlin: Duncker Humblot. p. 236.

tal y sentimental, goza de la máxima protección. Sin embargo, su sustantividad no sería definible en abstracto puesto que no es perceptible, evidente, cierta, ni objetivable, por lo que no existiría jurisprudencia o tribunal alguno con competencias para salvaguardar sus intereses. Del mismo modo, este último ámbito intangible quedaría sustraído por completo al poder público, por lo que ni los intereses más notables de la comunidad podrían justificar una injerencia en su contenido y, en resumen, el principio de proporcionalidad de relevancia de la información no tendría posibilidad de aplicación[115].

El segundo nivel de protección de la Teoría de las esferas referiría a la esfera privada, cuyo contenido transciende la interioridad del individuo para abarcar la vida familiar y los vínculos sentimentales establecidos con familiares y/o amigos. Igualmente, se contempla el ámbito espacial que brinda al ser humano la posibilidad de escapar de la observación pública, propiciando el esparcimiento o la relajación. De nuevo, la protección que ampara esta esfera es absolutamente relativa ya que, el mencionado criterio de proporcionalidad de relevancia social podría justificar una intromisión si concurre un interés público en los hechos aquí acaecidos.

Finalmente, el círculo exterior, denominado «esfera individual», «social» o «pública», permite una amplia capacidad de información, siempre y cuando no se divulguen informaciones falsas o lesivas del derecho al honor[116].

Con todo, una de las críticas cardinales a la concepción de Hubmann versa en la deficiencia para esclarecer el término «privado» o, más concretamente, las atribuciones de dicha esfera, lo que actúa en detrimento de la protección del ámbito reservado del individuo. Al partir de la premisa de que es factible delimitar un listado de situaciones, actividades o asuntos bajo el epígrafe de «privados», se condenaría al resto de supuestos a quedar desprovistos de la tutela del derecho, excluyendo determinados contenidos extramuros del derecho a la personalidad, por cuanto se decanta por una imagen de la vida privada «perfilada materialmente»[117].

---

[115] MEDINA GUERRERO, M. (2005): *Op. cit.,* p. 15.

[116] MÜNCH, H. (2002): *Freiwillige Selbstkonntrolle beu Indiskretionan der Presse*. Baden-Baden: Nomos, p. 135.

[117] MEDINA GUERRERO, M. (2005): *Op. cit.,* p. 13.

Sin embargo y a pesar de las controversias suscitadas, el uso de las esferas para delimitar tanto la difusión de hechos de las distintas manifestaciones del ser humano, como su protección constitucional ha sido recurrente para numerosos autores. Así, para Desantes Guanter, la relación entre intimidad, vida privada, vida profesional y vida pública puede comprenderse, visualmente, si pensamos en una serie de círculos concéntricos en los que la intimidad corone el núcleo y la vida privada, la profesional y la pública protagonizasen sucesivamente los círculos que se abren al exterior. Estos círculos nos dan la clave de cuando un hecho es noticiable o no:

> La esfera de la vida pública puede y debe ser siempre objeto de la información: la esfera de la vida privada puede ser siempre objeto del mensaje, pero debe serlo tan solo cuando la actuación privada trasciende a la vida pública; la vida íntima no solo no es informable, sino que ni siquiera es investigable. No puede, ni debe ser objeto de la información. Es un núcleo totalmente reservado[118].

2.2 LA DIMENSIÓN NORMATIVA DE LA VIDA PRIVADA: LOS ORÍGENES Y EVOLUCIÓN DEL DERECHO

En la actualidad, el derecho a la protección de nuestro ámbito reservado posee un tratamiento jurídico netamente norteamericano debido a su origen y en el que la confrontación entre el derecho a informar y el respeto a la vida privada aparece en su propia génesis.

La primera vez que se enuncia la necesidad de protección de la intimidad y vida privada es en 1890, con motivo de un procedimiento penal instaurado por dos jóvenes abogados, Samuel D. Warren y Louis D. Brandeis, después de que el primero fuera objeto, en diversos diarios, de notas sensacionalistas relacionadas con su vida privada. En concreto, el acontecimiento que motivó la escritura del artículo doctrinal fue la aparición detallada en la prensa de la época de una de las fiestas realizadas por la familia Warren en su casa. La celebración, un matrimonio familiar, fue ampliamente divulgada por la prensa lo-

---

[118] DESANTES GUANTER, J. M. y SORIA, C. (1991): *Los límites de la información. La información en la jurisprudencia del Tribunal Constitucional: las 100 primeras sentencias*. Madrid: APM, p. 108.

cal, especialmente por *Saturday Evening Gazette*. La esposa de Warren, hija de un famoso senador, no vio con buenos ojos dicha publicación, no en vano, la gente más acomodada de la sociedad de Boston de finales de siglo evitaba aparecer en la prensa[119]. Por ese motivo Warren, que había ejercido como abogado anteriormente, recurrió a su ex socio Brandeis (quien posteriormente se convertiría en juez del Tribunal Supremo) y redactaron el artículo. Con motivo de tal procedimiento, Warren y Brandeis publicaron en la revista *Harvard Law* un opúsculo que titularon «The Right to Privacy». Posteriormente, la tradicional influencia de las revistas legales en el derecho americano ayudó a extender el mensaje de dicho opúsculo:

> De la conveniencia —más bien de la necesidad— de tal protección, creemos que no puede haber ninguna duda. La prensa está sobrepasando en todas las direcciones los límites obvios de la propiedad y de la decencia […] y el hombre, bajo la influencia refinada de la cultura, se ha vuelto más sensible hacia la publicidad, de manera que la soledad y la intimidad se han vuelto más esenciales para el individuo[120].

Warren y Brandeis comienzan, de este modo, su denuncia explícita sobre el papel de la prensa de la época y la necesidad de establecer alguna medida de protección. Según los autores, a pesar de que la *common law* se desarrolla para satisfacer las demandas de la sociedad y garantiza a cada persona el derecho a decidir hasta qué punto pueden ser comunicados a otros sus pensamientos, sentimientos y emociones, con los avances y el paso del tiempo se hace imprescindible definir exactamente el alcance de dicha protección:

> Cambios políticos, sociales y económicos conllevan al reconocimiento de nuevos derechos, y la *common law*, en su eterna juventud, crece para satisfacer las demandas de la sociedad […] Gradualmente se ha ido ensanchando el alcance de estos derechos, y ahora el derecho a la vida ha llegado a significar el derecho a disfrutar la vida —el derecho a ser dejado en paz, el derecho a la libertad asegura el ejercicio de amplios privilegios civiles; y el término 'propiedad' abarca, en significado actual, todo tipo de derechos de dominio, tanto tangibles, como intangibles[121].

---

[119] PROSSER, W. L. (1960): «Privacy». *California Law Review*, n. 3, p. 383; ZIMMERMAN, D. L. (1983): «Requiem for a heavy weight: a farewell to Warren and Brandeis privacy Tort». *Cornell Law Review*, n. 68, p. 295.

[120] WARREN, S. y BRANDEIS, L. (1890): *Op. cit.,* p. 39.

[121] Ibídem., p. 48.

Dentro de esta perspectiva, la protección de la vida privada supondría, tal y como arguye Béjar, el derecho que permite al individuo ocultar información acerca de sí mismo, resaltando su inmunidad y la importancia de salvaguardar su integridad[122]. Poco antes de la publicación de este texto, en 1873, el Juez Cooley ya había mencionado en «*The elements of Torts»,* la expresión: *the right to be alone,* el derecho «a ser dejado en paz» o si se prefiere, según la traducción de Urubayen, «a ser dejado solo o tranquilo». Warren y Brandeis lo retoman como condición que es necesaria garantizar a la persona ante, citando a Cooley, «los recientes inventos y métodos de hacer negocios» [123]. Sin embargo, dicha alusión resulta sacada de contexto por Warren y Brandeis, por cuanto Cooley no se refería en ningún momento al respeto a la vida privada, sino a no ser víctima de ataques o agresiones físicas[124].

Prosiguiendo con los autores, Warren y Brandeis ya recalcaban en su escrito la importancia de distinguir entre el ciudadano común y aquel que, por voluntad propia, se convierte en una personalidad pública y, por tanto:

> Se expone a la crítica observación de sus conciudadanos. Estos comentarios sobre sus actuaciones —añaden— no siempre, necesariamente, deben ser favorables, sin que la crítica desfavorable pueda significar la demostración del ánimo de injuriar, o de penetrar en la vida privada de su existencia[125].

Refieren así a la delimitación de una esfera privada constitucionalmente garantizada, por oposición al área donde los medios tienen legitimada su actuación. De este modo, los autores vislumbran la mencionada división entre las distintas esferas de la vida humana que, ulteriormente, otros autores retomaran para explicar la dicotomía entre lo público y lo privado.

Sin embargo, desde que Warren y Brandeis lo formulasen por primera vez, la percepción del derecho a la intimidad y vida privada ha

---

122 BÉJAR, H. (1988): *Op. cit.,* p. 152.

123 COOLEY, T. M. (1888): *A treatise on the Law of Torts.* Chicago: Callaghan and Company, p. 24.

124 FAYOS GARDÓ, A. (2000): *Derecho a la intimidad y medios de comunicación.* Madrid. CEPC, p. 31.

125 WARREN, S. y BRANDEIS, L. (1890): *Op. cit.,* p. 43.

sufrido variaciones, añadiendo otras atribuciones. Señala Medina Guerrero, que si bien Warren y Brandeis ya aludían en su artículo a la necesidad de un control sobre la difusión de la información personal fuera de su esfera privada[126], no es hasta la década de los sesenta del s. XX cuando nace en Estados Unidos una concepción del derecho a la intimidad y vida privada como derecho de control de nuestras informaciones. Autores como Shils explicitan, ya en 1956, que la protección de la vida privada:

> Es la retención voluntaria de información. El derecho a limitar el poder de los extraños a descubrir o a forzar la revelación de cuestiones privadas. Es la antítesis de la publicidad, esto es, revelación de la información a un público más amplio[127].

Sin embargo, fue explícitamente Alan Westin quien inauguró esta línea doctrinal en 1967, al reconocer que la protección de la vida privada implica:

> La pretensión de los individuos [...] de determinar cuándo, cómo y hasta dónde se comunica a los demás información sobre ellos [...] El derecho de un individuo a decidir qué información sobre él mismo se debería comunicar a los demás y bajo que circunstancias[128].

Por otra parte, al referirse Westin a la necesidad del individuo de «mantener completamente privados algunos hechos relativos a sí mismo y de sentirse libre para decidir por sí mismo quién conocerá otros hechos en qué momento y bajo qué condiciones»[129] anunciaba, sin saberlo, las claves para la protección de la intimidad y vida privada en los entornos digitales: Una facultad para decidir la finalidad y el uso de nuestras informaciones que entronca directamente con la idea de «autodeterminación informativa», concepto que veremos así referenciado en el desarrollo de esta tesis.

En definitiva, la protección de la intimidad y vida privada presenta una línea de evolución en paralelo a los cambios acontecidos en el concepto de vida privada, que va desde una vertiente de libertad ne-

---

126 MEDINA GUERRERO, M. (2005): *Op. cit.,* p. 33.

127 SHILS, E. (1956): *The Torment of Secrecy: The Background and Consequences of American Secruity Policies.* London: William Heinemann, p. 22.

128 WESTIN, A. (1967): *Privacy and freedom.* New York: Athenaeum, pp. 7-8.

129 Ibíd., p. 368.

gativa frente a las intromisiones abusivas de los poderes públicos, hasta la concepción positiva actual de ejercer derecho de control sobre los datos referidos a la propia persona y que haría referencia no solo a los medios tradicionales, sino a los archivos o bases de datos electrónicos.

3. LA INTIMIDAD Y VIDA PRIVADA Y SU PROTECCIÓN JURÍDICA

A continuación, haremos un breve repaso del marco jurídico aplicable a la protección de la intimidad y vida privada, haciendo especial hincapié en la protección de este derecho en relación al uso de las Tecnologías de la Información y la Comunicación, así como los servicios asociados a ésta. Para contar con una visión global del actual contexto se analizará el ámbito internacional, comunitario o europeo y el nacional. Del mismo modo, se incluirá en el presente capítulo la normativa estadounidense, ya que la mayoría de empresas tecnológicas que estudiaremos se encuentran nacionalizadas en Estados Unidos y, desde los atentados del 11 de septiembre, una parte importante de la reglamentación de este país se ha centrado en las comunicaciones vía Internet. Asimismo, en este repaso plasmaremos la doble vertiente en que se manifiesta dicha protección legislativa, esto es: el derecho a la intimidad o vida privada de una parte y las leyes de protección de datos personales de otra.

3.1 EL DERECHO A LA INTIMIDAD Y VIDA PRIVADA

3.1.1 **Normativa internacional**

Actualmente, nadie discute la necesidad de este supraderecho fundamental de la persona, aunque sí son puestas en duda sus formas efectivas de protección. La mayor parte de países industrializados poseen leyes para la protección de la intimidad y vida privada, y en el ámbito internacional, la Declaración Universal de los Derechos Humanos del 10 de diciembre de 1948, establece la primitiva fuente normativa respecto a los derechos objeto de este apartado. El derecho a la intimidad queda consignado así en el artículo 12:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques[130].

3.1.2 Normativa en el ámbito comunitario

Conviene destacar, en primer lugar, el *Convenio de Roma* de 1950 (CEDH) considerado como el primer texto europeo en el que se consagra la tutela de la vida privada, derecho que regula en su artículo 8 en los siguientes términos:

> 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás[131].

Igualmente, en el ámbito comunitario debe reseñarse lo dispuesto en la *Carta de los Derechos Fundamentales de la Unión Europea*, de 7 de diciembre de 2000 (2000/C 364/01) donde se instituye que: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones» [132].

Finalmente, en la *Carta Europea de Derechos del Niño* (Resolución del Parlamento Europeo A3-0172/92 de 8 de julio de 1992) se declara que: «Todo niño tiene derecho a no ser objeto por parte de un

---

130 Asamblea General de las Naciones Unidas (1948): *Declaración Universal de Derechos Humanos (DUDH)*. París, artículo 12. Disponible en: http://www.un.org/es/documents/udhr/law.shtml

131 *Convenio de Roma para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950,* Instrumento de Ratificación de 26 de septiembre de 1979, artículo 8.

132 *Carta de los Derechos Fundamentales de la Unión Europea*, de 7 de diciembre de 2000 (2000/C 364/01). Diario Oficial de las Comunidades Europeas el 18 de diciembre de 2000.

tercero de intrusiones injustificadas en su vida privada, en la de su familia, ni a sufrir atentados ilegales contra su honor» [133].

3.1.3 **Normativa en Estados Unidos**

En Estados Unidos no existe una ley general que regule la intimidad y vida privada en relación a las tecnologías digitales, dado que, a diferencia de lo que sucede en Europa, la protección del derecho a la intimidad y, por extensión, de los propios datos personales no es percibida como un derecho fundamental, sino como una problemática relacionada con la defensa de la competencia y los derechos de los consumidores:

> A diferencia de la Unión Europea donde el derecho a la privacidad es recogido en diversos tratados, manifiestos y las constituciones de algunos Estados miembros, en Estados Unidos dichos conceptos no están presentes directamente en la constitución, sino que se ha seguido un enfoque *laissez faire*, más reactivo, con el que se ha dado prioridad al rol de los actores privados y de las fuerzas de mercado[134].

No obstante, aunque no se reconoce explícitamente, las distintas enmiendas de la Carta de Derechos de los Estados Unidos sí contemplan elementos parciales. Así, la zona privada protegida o de no injerencia del ser humano se recoge en las Tercera y Cuarta Enmiendas, definiendo los límites explícitos que coartan el acceso del gobierno a los hogares[135]. Si bien es cierto que no se ha desarrollado ninguna ley que trate de unificar los distintos criterios en los diversos contextos en los que la salvaguarda de la vida privada está en entredicho, es «la interpretación de dichos derechos [la que] ha derivado en el reconocimiento del derecho a la privacidad y a la privacidad de la información.» [136]. Son, sin embargo, menciones veladas, ya que el modelo de protección estadounidense es, por lo general, menos prescrip-

---

[133] *Carta Europea de Derechos del Niño*. Resolución del Parlamento Europeo A3-0172/92, 8 de julio, 1992.

[134] VERGARA PARDILLO, A. y MARTÍNEZ PÉREZ, J. (2012): «Modelos reguladores de protección de datos para una era global», en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados*. Madrid: Ariel, p. 31.

[135] BÉJAR, H. (1988): *Op. cit.,* p. 68.

[136] VERGARA PARDILLO, A. y MARTÍNEZ PÉREZ, J. (2012): *Op. cit.,* p. 32

tivo y más permisivo que el europeo, generando por tanto menores trabas a las empresas.

Esta realidad se refleja en el ámbito de las tecnologías digitales. Afirma Schwartz que, a diferencia de Europa, las leyes que regulan la protección de la intimidad y vida privada en relación al uso de las Tecnologías de la Comunicación y la Información constituyen un mosaico de normas yuxtapuestas que dejan muchas áreas desprovistas de normativa legal formal[137]. A este tenor, resulta pertinente destacar que en el marco estadounidense no se articula mediante leyes específicas y que la protección del ámbito reservado del individuo se ha desarrollado mediante una combinación de la actuación de los poderes judicial y legislativo, «siendo, en unos casos, los tribunales los que interpretan y definen nuevos derechos a la intimidad y vida privada, mientras que, en otros casos, la iniciativa parte del poder legislativo» [138].

A esta mezcolanza, hay que unir el hecho de que la consideración normativa se produce de un modo parcial, por cuanto se realiza en normas estatales y, sobre todo, por normas sectoriales de carácter federal, por lo que analizar legislativamente la regulación de la vida privada en Estados Unidos no es labor sencilla:

> A nivel federal, la privacidad y la protección de datos en Estados Unidos están recogidas mediante legislación sectorial. Existen diferentes estatutos que regulan las prácticas públicas y privadas sin que exista una ley específica sobre protección de datos. Mientras que, a nivel estatal, se desarrolla la regulación de protección al consumidor, segundo pilar en el que descansa la legislación sobre privacidad en Estados Unidos. Estos, al igual que el gobierno federal, tratan la problemática desde una perspectiva sectorial en lugar de mediante leyes integrales. Las disposiciones federales representan las protecciones mínimas que los Estados pueden reforzar, dando lugar a divergencias significativas entre Estados en algunos casos, así como a situaciones en las que sectores industriales han acudido al Congreso para tratar de limitar leyes estatales más restrictivas[139].

---

137 SCHAWRTZ, P. (2012): «Privacidad online: planteamientos jurídicos en Estados Unidos y la Unión Europea», en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados.* Madrid: Ariel, p. 59.

138 VERGARA PARDILLO, A. y MARTÍNEZ PÉREZ, J. (2012): *Op. cit.,* p. 31

139 Ídem.

En definitiva y dado que se basa en leyes constitucionales, leyes estatales, derecho común, agencias reguladoras, principios de autorregulación y normas sociales, no existe una definición coherente de qué debe quedar protegido por la legislación[140]. Como es de esperar, la conjunción de esta diversidad de agentes implicados (a nivel federal intervienen los poderes legislativo, judicial y ejecutivo, así como la intervención a nivel estatal) con las divergencias derivadas del modelo sectorial, dificultan la existencia de un enfoque cohesionado para las leyes sobre el derecho a la intimidad y vida privada, por lo que «se ha dado prioridad al rol de los actores privados y de las fuerzas de mercado»[141].

Esta sarta normativa aparece complementada por la actuación del organismo regulador de competencia, la Federal Trade Commission (FTC) que en la última década ha asumido un papel protagonista en la defensa de la intimidad y vida privada en entornos digitales. Tras su fundación en 1914, la Comisión Federal del Comercio ha sido una agencia estatal independiente dedicada a la protección del consumidor y velar por el establecimiento de prácticas comerciales leales. Dicha agencia responde a la Ley de Comercio del mismo año, razón por la que en el país norteamericano siempre se ha equiparado usuario a consumidor. Como órgano regulador de competencia, impulsa la autorregulación y las tecnologías de protección de la vida privada como principal vía de actuación. Su poder es limitado, no obstante, pues sus resoluciones solo vinculan a las empresas concretas que firmen los convenios resultantes, acuerdos que añaden la base jurídica para la salvaguarda de la intimidad y vida privada en los entornos digitales.

Además de las leyes estatales y federales, podemos mencionar normas específicas que tratan de velar por la protección de ciertos aspectos relacionados con la intimidad y vida privada:

- *Telecommunications Act* de 1996 (Ley de Telecomunicaciones, aprobada el 13 de junio de 1996) que normaliza, de forma explícita, lo concerniente a la publicación en Internet de contenidos susceptibles de dañar la integridad ética y la moral de las personas.

---

[140] SOLOVE, D. J. (2002): «Conceptualizing Privacy», en *California Law Review*, vol. 90, pp. 1087-1156.

[141] VERGARA PARDILLO, A. y MARTÍNEZ PÉREZ, J. (2012): *Op. cit.,* p. 31.

- *Children's Online Privacy Protection Act* de 1998 (Ley de Privacidad para la Actividad de los Menores en la Red) donde se establece la ordenación específica respecto a aquellos actos encaminados a obtener información o engañar a los menores en el entorno digital.

No podemos pasar por alto, no obstante, la existencia de la denominada *USA Patriot Act (UPA)*[142] de 24 de octubre de 2001, aprobada tras los atentados terroristas acaecidos el 11 de septiembre en la ciudad de Nueva York y que supone una considerable restricción del derecho a la intimidad personal y familiar, así como al secreto de las comunicaciones de cualquier persona que se encuentre dentro del territorio de los Estados Unidos. Creada para aumentar el grado de seguridad del Estado frente posibles actos terroristas, bajo esta normativa:

> El Gobierno Federal cuenta con plenos poderes para intervenir cualquier tipo de comunicación, interna o externa, de correo electrónico, conversación telefónica, ya sean mensajes de voz o texto, los históricos de navegación Web, así como de consultas en los principales buscadores de Internet[143].

3.1.4 La protección de la intimidad y vida privada en nuestro ordenamiento jurídico

En nuestro ordenamiento jurídico, la salvaguarda de intimidad y vida privada aparece desdoblada como bien protegido en el derecho a la intimidad y en la Ley de protección de datos. La jurisprudencia constitucional viene así a identificar las dos vías de afectación que se corresponden con las dos dimensiones anteriormente descritas. Se trata, como es palmario, de dos posibles formas de injerencia neutralizadas por la preservación de un ámbito reservado y el control sobre las propias informaciones.

---

[142] El texto se encuentra disponible en: http://www.justice.gov/archive/ll/highlights.htm

[143] AEPD e INTECO (2009): *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes,* p. 82. Disponible en: www.agpd.es [29/03/2013].

3.1.4.1 *La denominación: El derecho a la intimidad*

El respeto al ámbito más reservado del individuo es un deber moral y un derecho que, en nuestro ordenamiento jurídico, se materializa en el «derecho a la intimidad», expresión que incluye el honor, la persona, la familia y la propia imagen. Sin embargo, tal y como hemos comentado, existe una amplia confusión entre los términos «intimidad» y «vida privada» que se usan indistintamente aun cuando existe la imposibilidad de objetivar algo como la intimidad. Resulta necesario, no obstante, recalcar que la mencionada confusión entre intimidad y privacidad ha llegado hasta nuestro sistema normativo e, incluso, se refleja en la Constitución Española. Afirman por ello, Desantes Guanter y Calos Soria que, a diferencia de otros ordenamientos jurídicos, nuestra Carta Magna y las leyes que se derivan de ella reconocen y protegen el derecho a la vida privada, denominándolo, equívocamente «derecho a la intimidad»:

> Bajo el nombre de intimidad se han planteado asuntos que no afectan al campo de lo íntimo, sino al más amplio de lo privado. Se ha producido así en el juzgador una especie de inflación de lo íntimo que lo ha devaluado. La solución no ha consistido en aclarar los conceptos para aplicar debidamente la ley, sino en negar al derecho a la intimidad su carácter de derecho inseparable a la personalidad[144].

Según este razonamiento, aunque en el artículo 20 de la Constitución Española sobre la *Libertad de expresión*, en su apartado 4, se menciona que las libertades recogidas en el mismo tienen su límite, entre otros, en el respeto al derecho a la intimidad, en realidad solo el derecho a la vida privada constituye dicho linde. Recordemos que, para que la intimidad fuese difundida, primero debería ser contada o confesada a alguien y, en ese mismo instante, perdería su condición de intimidad y pasaría a llamarse vida privada.

Así, la construcción jurídica del «derecho a la intimidad», tal y como aparece formulada en nuestra Carta Magna, plantea problemas terminológicos por la esencia misma del objeto de derecho. Para González Gaitano, al ser la intimidad un factor de individualización, la esencia del hombre mismo, no es tangible y, por ende, no puede ser objetivable: «no es difícil objetivar las atribuciones jurídicas cuando

---

144 DESANTES GUANTER, J. M. y SORIA, C. (1991): *Op. cit.,* p. 107.

estas son sobre cosas [...] pero es imposible cuando el objeto es la persona misma. [...] Mi intimidad y yo mismo no son en realidad cosas distintas» [145]. Según el autor, la denominación «derecho a la intimidad» se refiere al «derecho a la vida privada», tal y como sostiene la investigadora Dora García Fernández, para quien dicho derecho «tiene campo propio en la vida privada de la persona, en su familia, en su círculo de amistades, pareja y la protege de intromisiones, injerencias, publicaciones, captación de datos personales, etc.» [146].

Sin embargo, autores como Urabayen, que distinguen entre intimidad y vida privada desde una perspectiva teórica, consideran dicha separación inoperante desde el punto de vista del derecho[147], ya que solo la protección de la vida privada puede ser objeto de esta disciplina. De manera similar respecto a la funcionalidad práctica de esta distinción se pronuncia Desantes[148] quien, aunque coincide en señalar que intimidad y vida privada son nociones afines pero no sinónimas, sí entiende que la primera estaría contenida en la segunda. Este foco de controversia no es exclusivo en nuestro ordenamiento jurídico, sino que se ha dado en otros países, optando por utilizar la expresión «derecho a la intimidad» en lo referente a la protección jurídica de la vida privada. Por dicho motivo y para identificar nuestro objeto de estudio con el derecho mencionado en la Carta Magna usaremos en esta investigación la expresión «intimidad y vida privada».

3.1.4.2 *El derecho a la intimidad: descripción*

En nuestro sistema jurídico, el derecho a la intimidad no se había desarrollado, como otros derechos de la personalidad, a partir del Código Civil, por lo que se creó prácticamente de cero al albor de la Carta Magna. El derecho a la intimidad, considerado un derecho fundamental, se plasma en la Constitución Española, en el Capítulo Segundo referido a los Derechos y Libertades, Sección Primera. Concretamente es en el artículo 18 de la Constitución Española donde se

---

145 GONZÁLEZ GAITANO, N. (1987): *Op. cit.,* p. 129.
146 GARCÍA FERNÁNDEZ, D. (2010): *Op. cit.,* p. 277.
147 URABAYEN, M. (1977): *Op. cit.,* pp. 11-12.
148 DESANTES GUANTER, J. M. (1991): *Op. cit.,* pp. 23-48.

contempla la tutela de la vida privada de modo integral y se ordena a la protección de distintos bienes de la personalidad:

> Artículo 18.1 «Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.»
>
> 18.2 «El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.»
>
> 18.3 «Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.»
>
> 18.4 «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos[149].

Herencia de la evolución anteriormente citada, este derecho garantiza la esfera de libertad individual y lo hace protegiendo de un lado la vida privada de las personas y otorgando, de otro, facultades que permiten ejercer un control efectivo sobre el tratamiento de sus informaciones privadas:

En el precepto conviven manifestaciones clásicas de los derechos de la personalidad —derechos al honor, a la intimidad personal y familiar y a la propia imagen— una esfera de protección frente a las injerencias en ámbitos específicos —inviolabilidad del domicilio y secreto de las comunicaciones— y un derecho de última generación definido por el Tribunal Constitucional como derecho fundamental a la protección de datos[150]. Según la jurisprudencia, tales garantías, aunque independientes, están profundamente relacionadas bajo un nexo común: la protección del uso de la información personal. Se trata por ello de un derecho de amplias miras, claramente orientado a ofrecer una esfera de protección en todas las manifestaciones de la personalidad y frente a los avances tecnológicos[151]. Sin embargo, aun cuando la referencia a la protección de datos supera la tradicional concepción de protección jurídica de la intimidad y vida privada, el uso de las Tecnologías de la Información «no solo se proyecta sobre el último

---

149 Artículo 18. Constitución Española de 27 de diciembre de 1978 (2013). Madrid: Editorial Civitas.

150 AEPD e INTECO (2009): *Op. cit.*, p. 74.

151 MARTÍNEZ, R. (2012): «El derecho a la vida privada en España», en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados*. Madrid: Ariel. p. 125.

derecho citado, sino que afectan también a la conformación constitucional de las dos primeras categorías» [152].

La demarcación del bien jurídico protegido en el artículo 18 recopila derechos que conforman la categoría de los denominados como «de la personalidad», por cuanto su titularidad es, salvo excepciones, atribuible únicamente a personas físicas. Es, por tanto, originario e inherente a la persona y se caracteriza por ser irrenunciable, intransmisible, absoluto, extra-patrimonial e imprescriptible [153].

La protección de la vida privada se recoge como manifestación de la personalidad del individuo ligada a la salvaguarda de la dignidad y libertad del ser humano. El Tribunal Constitucional Español estableció que este derecho a la intimidad deriva de la dignidad de la persona [154], por ello nos remite, asimismo, a lo dispuesto en el artículo 10.1: «La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento de orden político y de la paz social» [155].

La evocación del «respeto a la ley y a los derechos de los demás» nos sitúa en el conflicto permanente con el derecho a la libertad de expresión. No es coincidencia que, en la actualidad, uno de los principales puntos de fricción entre el Tribunal Constitucional y el Tribunal Supremo sean precisamente, los conflictos entre el derecho a la intimidad y la libertad de información. Si resulta sumamente complejo *per se* perfilar líneas nítidas que permitan predecir cuándo una información abandona el terreno de lo constitucionalmente lícito para invadir la esfera de la vida privada, la dificultad se extrema en aquellos ordenamientos, como el nuestro, que recurren a la técnica de la «ponderación» para la elucidación de este tipo de controversias [156]. Por ello, además de la legislación existente, hablar del derecho a la intimidad nos obliga a revisar la nutrida jurisprudencia nacida al respecto:

---

152 AEPD e INTECO (2009): *Op. cit.,* p. 74.
153 GARCÍA FERNÁNDEZ, D. (2010): *Op. cit.,* p. 279.
154 STC 53/1985.
155 Artículo 10.1. Constitución Española.
156 AEPD e INTECO (2009): *Op. cit.*

> Cuando entran en colisión derechos fundamentales o determinadas limitaciones a los mismos en interés de otros bienes y derechos constitucionalmente protegidos, la función del intérprete constitucional alcanza la máxima importancia y se ve obligado —como dice la STC 53/1985— a ponderar los bienes y derechos en función del supuesto planteado, tratando de armonizarlos si ello es posible o, en caso contrario, precisando las condiciones y requisitos en que podría admitirse la relevancia de uno de ellos[157].

Como hemos indicado, la intimidad y vida privada constituyen un límite al derecho a la información[158] mencionado en el artículo 20.4: «estas libertades tienen su límite […] especialmente en el derecho al honor, a la intimidad y vida privada y a la propia imagen»[159]. Estos principios forman parte de la Sección I, De los Derechos Fundamentales y Libertades Públicas, ubicado dentro del Capítulo II, Derechos y Libertades del Título I, De los Derechos y Deberes Fundamentales y, por tanto, cuentan con la máxima garantía de protección en nuestro ordenamiento jurídico. A tenor literal de la ley, el artículo 53 dice:

> 53.1 Los derechos y libertades reconocidos en el Capítulo Segundo del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161, 1, a).
>
> 53.2 Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección 1.ª del Capítulo Segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional[160].

En el Título IV, denominado Del Gobierno y De La Administración, el artículo 105.b de la Carta Magna dispone que: «la ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas»[161].

---

157 STC 254/1988, de 21 de diciembre.

158 El derecho a la información se reconoce en el artículo 20.1.d) de la Constitución Española.

159 Límites al derecho a la información. Artículo 20.4. Constitución Española.

160 Artículo 53. Constitución Española.

161 Artículo 105.b. Constitución Española.

La ley orgánica 10/1995 de 23 de noviembre, por la que se publica el Código Penal, recoge en su Título X, los «delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio» [162]. En su Capítulo I, El Descubrimiento y la Revelación de Secretos, afirma:

> 197.1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
>
> 197.2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en fichas o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero [163].

3.2 LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Advertimos ahora que hemos comenzado a usar la denominación datos «de carácter personal» en vez de datos o informaciones «privadas». Esta denominación común a la mayoría de países que introducen estas leyes responde al siguiente planteamiento. Si nos volcamos, por ejemplo, en nuestro ordenamiento jurídico observamos que, tal y como señala el Tribunal Constitucional, el objeto del derecho a la protección de datos no se limita únicamente a los datos privados sino que alcanza:

> A cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es solo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de

---

[162] Título X. Código Penal (2013): Madrid: Editorial Tecnos (19.º Edición).
[163] Título I. *Op. cit.*

> carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo[164].

Tal y como recuerda la LOPD, a efectos normativos se entiende que un dato de carácter personal es «cualquier información concerniente a personas físicas identificadas o identificables»[165], lo que convierte en dato de carácter personal la mayor parte de la información sobre personas físicas, «en la medida en que a través de escasos datos o informaciones sobre éstas y mediante la correcta aplicación de herramientas informáticas, es relativamente sencillo identificar a la persona concreta que se encuentra detrás de los datos de que se dispone»[166]. Los datos privados son aquellos que pertenecen al ámbito de lo privado de la persona y que por voluntad propia desea mantener en dicho ámbito. Sin embargo, la acumulación de informaciones personales en entornos digitales puede llevarnos a levantar el velo que protege la intimidad y vida privada de los usuarios, convirtiéndose, advierte la AEPD, en «auténticas "identidades digitales" que facilitan un rápido conocimiento de datos de contacto, preferencias, hábitos del usuario»[167] que combinados pueden llegar a desvelarnos su intimidad y vida privada.

Esta normativa va en línea con lo dispuesto desde el ámbito comunitario que entiende que dato de carácter personal es aquel «concerniente al individuo, tanto si se refiere a su vida privada, profesional o pública —por tanto— las normas de protección de datos europeas serán de aplicación cuando una persona pueda ser directa o indirecta-

---

164 Sentencia Tribunal Constitucional citada en AEPD (2009): *Op. Cit.,* p. 90.
165 LOPDP, artículo 3
166 AEPD e INTECO (2009): *Op. Cit.,* p. 90.
167 Ibídem, p. 94.

mente identificada por dichos datos»[168]. Cuando así fuere, estos datos personales tendrán protección con independencia de su emplazamiento público: «Todas las personas tienen el derecho a la protección de sus datos personales en cualquier aspecto de su vida: en casa, en el trabajo, mientras compran, recibiendo tratamiento médico, en la comisaría o cuando navega por Internet» [169].

Así por ejemplo, según el Grupo de Trabajo del Artículo 29 en su *Dictamen sobre el concepto de datos personales*[170] y la Agencia de Protección de Datos, entre los datos personales que en el contexto de las Nuevas Tecnologías pueden llegar a identificar a las personas se encuentra, entre otros, la dirección IP[171]. Es por ello que cuando hablamos de protección de la intimidad y vida privada no debemos referirnos solo a datos privados, sino también a datos de carácter personal.

3.2.1 **Ámbito internacional**

Recientemente, muchos países han promulgado leyes reguladoras de la protección de datos de carácter personal teniendo en cuenta los aspectos específicos derivados de la Sociedad de la Información. Igualmente, el debate sobre cómo crear modelos globales comunes de protección de datos ha sido adoptado en diferentes foros y conferencias globales, como el *European Data Protection Day* (EDPD) organizado anualmente por el Consejo de Europa. Todo ello, unido a la existencia de varias directrices emitidas por la OCDE[172] y la ONU[173].

---

168 *EU Chapter of Fundamental Rights* (2000/C 364/01) de 18 de diciembre de 2000.

169 Protection of personal data. *EU Chapter of Fundamental Rights* (2000/C 364/01) de 18 de diciembre de 2000, Capítulo II: Libertades, artículo 8.

170 Comisión Europea (2007): *Dictamen 4/2007 sobre el concepto de datos personales*. Grupo de Trabajo del artículo 29.

171 AEPD (2003): Carácter de dato personal de la dirección IP. Informe 327/2003 de la Agencia Española de Protección de Datos 327/2003.

172 Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, de 23 de septiembre de 1980.

173 Directrices para la regulación de los archivos de datos personales informatizados, Adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990.

A este tenor, resulta necesario reseñar el *Marco de Privacidad* de *Asia-Pacifi Economic Cooperation* (APEC) que configura una red de 21 países en la región de Asia-Pacífico, incluyendo a Estados Unidos, y que en 2011 logró un convenio para armonizar la transferencia de datos personales entre los miembros firmantes. Destaca, igualmente, la *International Conference of Data Protection and Privacy Commissioners* (ICDPPC) que ha alcanzado acuerdos relevantes como la *Resolución de Madrid*[174] de 2009. Del mismo modo, los procesos de revisión y reforma de la legislación en Europa y Estados Unidos constituyen una oportunidad para incluir medidas de carácter global, avanzando hacia un mayor reconocimiento de elementos comunes.

3.2.2 **Estados Unidos**

Al igual que sucede con la protección del derecho a la intimidad y vida privada, la protección de datos personales en Estados Unidos es, por lo general, «limitada e incoherente»[175], aunque aliñada con una serie de medidas coercitivas de la Federal Trade Comisión que ofrecen ciertos elementos generales de protección. A esto se le une el hecho de que la legislación estadounidense realiza una distinción importante entre los sectores público y privado, con leyes diversas que regulan el tratamiento de datos por parte del gobierno y las actividades similares del sector privado.

Desde el Congreso se han promulgado diversas leyes relativas a la recopilación, el tratamiento y la publicación de información y de datos personales. Dentro de este entramado, la norma principal es la *Privacy Act* de 1974[176], que regula la recogida, el uso y la publicación de datos personales e implementando varios de los elementos de las *Directivas de la Organización para la Cooperación y el Desarrollo Económicos (OCDE)*. En concreto, prohíbe que el gobierno cree bases de datos gubernamentales secretas con informaciones sobre los individuos, además de limitar la forma en que las diferentes agencias gubernamentales pueden compartir información.

---

174 VERGARA PARDILLO, A. y MARTÍNEZ PÉREZ, J. (2012): *Op. cit.,* p. 38.
175 SCHAWRTZ, P. (2012): *Op. cit.,* p. 59.
176 www.epic.org/privacy71974act

Asimismo, se han desarrollado leyes sectoriales relacionadas con la amparo de datos financieros, registros médicos y de las comunicaciones.

Posteriormente y en clara alusión al uso de las Tecnologías de la Información y la Comunicación, se promulgó la *Electronic Communications Privacy Act (ECPA)* vigente desde 1986 y en la que se establecen las bases normativas en lo que respecta a la protección de los datos personales en las comunicaciones electrónicas de los usuarios, así como los límites específicos a las posibilidades de acceso por parte de los organismos públicos. Dicha normativa fue actualizada en 1994 por *The Computer Fraud and Abuse Act*, más centrada en los programas informáticos que pudieran dañar potencialmente la integridad de las comunicaciones de los individuos.

Igualmente, cabe destacar las ya mencionadas *Children's Online Privacy Protection Act (COPPA)* del año 1998 y la *USA Patriot Act (UPA)* de 2001. En la primera se dispone que:

> En caso de que los menores tengan que facilitar datos personales a través del sitio Web, deberá informarse de forma clara y comprensible respecto a cuáles son las finalidades para las que son solicitados, así como la puesta a disposición, de los tutores de los menores, de procedimientos sencillos y gratuitos que permitan conocer el tipo de datos facilitados por el menor y dar de baja o actualizar dichos datos[177].

Por su parte y cumplimentando a la *Cyber Security Enhancement Act (CSEA)* la *USA Patriot Act (UPA)* vigente desde el 24 de octubre de 2001, autoriza la intervención, por parte del gobierno, de cualquier comunicación electrónica, con independencia del formato en que se encuentre. Esto incluye no solo las llamadas telefónicas, sino las búsquedas realizadas a través de los motores de Internet o la memoria con las páginas que hemos consultado en Internet, entre otros, sin que sea necesaria una autorización judicial previa o «lo que ha supuesto un claro retroceso de los derechos civiles y políticos en favor de la seguridad de los ciudadanos»[178].

---

[177] AEPD e INTECO (2009): *Op. cit.*, p. 101.
[178] Ídem.

3.2.2.1 *Propuestas legislativas*

A pesar de la escasa reglamentación desarrollada al respecto, resulta palmario que la implementación de muchas de las herramientas relacionales de la Web 2.0 ha evolucionado, de manera directamente proporcional, al aumento de reclamaciones y quejas por parte de grupos de protección de los derechos civiles y otros sectores de la sociedad. Y este clamor ha tenido su reflejo en el ámbito legislativo. Sólo en el año 2011, se llevaron a término, en las cámaras legislativas de Estados Unidos, más de diez propuestas de ley referidas a los derechos de los consumidores y a la protección de la esfera privada de los interactores, en concreto, a la seguridad de sus informaciones personales y la recolección de datos de localización.

Entre las principales iniciativas planteadas en las Cámaras destaca *Do-Not-Track Online*, propuesta por el senador del partido demócrata, Jay Rockefeller y en la que se propone la creación, por parte de la Comisión Federal del Comercio, de una normativa que establezca instrumentos homogéneos para que los usuarios de los servicios de Internet puedan indicar si aceptan o no que sus datos sean recopilados. Esta proposición, que prohíbe la mencionada recopilación si el individuo no da su asentimiento, fue gratamente acogida por la generalidad de las asociaciones defensoras de los derechos civiles[179].

Igualmente, esta propuesta de ley fue acompañada por otras muchas destinadas a regular los servicios de geolocalización, los datos recogidos en transacciones comerciales y la salvaguarda de los menores, entre las que hay que reseñar la denominada *Do Not Track Kids Act*.

3.2.3 **Ámbito comunitario**

El derecho a la protección de datos de carácter personal está considerado en Europa como una parte integral del derecho al respeto de la vida privada, aunque con soberanía propia. Así, en la *Carta Europea de Derechos Fundamentales,* el artículo 8 de reconoce el derecho

---

[179] (2011): «US privacy groups welcome 'Do Not Track'», en *Physorg.com*, 9 de mayo de 2011. Disponible en: billphysorg.com/news/2011-05-privacy-groups-track-bill.html. [14/08/2012].

a la protección de datos como una garantía autónoma del derecho a la vida privada. Este principio también se recoge en el artículo 286 del *Tratado de la Comunidad Europea*.

Asimismo, el Consejo de Europa, a través del anteriormente mencionado *Convenio núm. 108*[180], ahonda en la relación entre Tecnologías de la Información y la Comunicación y protección de las informaciones privadas, protegidas por el artículo 8.1 del Convenio Europeo de Derechos Humanos.

A diferencia de lo que sucede en Estados Unidos, la legislación en materia de protección de datos está anclada en unas leyes ómnibus que han dado origen a un reglamento sobre el uso de la información personal. El modelo legislativo de protección de datos personales en Europa se basa primordialmente en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995 (conocida como Directiva de Protección de Datos)[181]. Dicha norma, que refiere a la protección de las personas físicas en lo que respecta al tratamiento y libre circulación de sus datos personales, nació para armonizar las legislaciones nacionales en dicha materia.

Los aspectos primordiales de la normativa comunitaria en materia de protección de datos son, entre otros: la existencia del consentimiento previo por parte del titular de los datos, la conciliación entre la protección del derecho a la intimidad en el tratamiento de los datos personales y el derecho a la libertad de expresión. Asimismo, se establecen los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) que el usuario puede ejercer respecto a los propios datos personales y se incorpora la garantía de confidencialidad como principio básico. Por otra parte, se establece la obligatoriedad de implementar las medidas de seguridad necesarias capaces de garantizar la seguridad de la información y que el acceso a dichos datos se encuentre limitado y controlado. En la misma línea, se instituyen los pilares que regulan la transferencia internacional de datos personales, a la vez que se promueve la elaboración de códigos de conducta sec-

---

[180] Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado el 27 de enero de 1984.

[181] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

toriales, consignados a avalar la correcta aplicación de las disposiciones nacionales en materia de protección de datos personales. Finalmente, se enuncia los principios básicos que han de guiar la creación de las Autoridades Nacionales de Protección de Datos y se crea el Grupo de Trabajo del Artículo 29 institución de referencia en esta materia.

Este texto de carácter genérico se completa con la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, de 12 de julio de 2002, que garantiza el tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones digitales. Dicha directiva fue renovada en 2009 incluyendo aspectos como la violación de los datos personales.

Así, el conjunto de directivas dictadas que concretan el entramado legislativo para la protección de la vida privada en relación con el uso de las Tecnologías de la Información y la Comunicación es bastante extenso:

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos datos.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, referente al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- Directiva 2000/31/CE, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información.
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones. Uno de los primeros aspectos que podemos mencionar de esta directiva es que establece que: «el consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre inequívoca y fundada de la voluntad del usuario.» [182].

---

[182] Considerando 17. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

- Directiva 2006/24/CE, de 21 de febrero de 2006, del Parlamento Europeo y del Consejo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE.
- Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales por las Instituciones y los Organismos Comunitarios y a la Libre Circulación de estos Datos.

No obstante, cabe mencionar que esta amalgama de normas comunitarias ya no proporciona el nivel de armonización requerido, ni son lo suficientemente eficientes como para garantizar el derecho a la protección de los datos personales dentro del nuevo y complicado entorno digital[183]. De hecho, la Directiva de protección de datos de 1995 lleva sometida desde 2007 a un proceso de revisión y consulta. Por dicho motivo, la Comisión Europea ha propuesto una reforma fundamental del marco europeo sobre la protección más acorde con la problemática actual. Nos referimos a la reciente propuesta de Reglamento General de Protección de Datos, realizada a principios de 2012 y que constituye el inicio del proceso legislativo ordinario por el que la Comisión, el Parlamento y el Consejo avanzarán hacia la creación del nuevo marco europeo de protección de datos. La importancia de esta nueva legislación recae no solo en la protección que proporcionará a los ciudadanos europeos, sino en el impulso que ofrece a nivel internacional:

> El impacto de esta legislación no solo será sobre aquellos países que han adoptado leyes de protección de datos alineadas con la Directiva 95/46/EC, sino también en aquellos en los que los marcos de protección de datos son distintos y que desarrollan una intensa actividad comercial

---

183 REDING, V. (2012) «Protección de la privacidad en un mundo conectado. Un marco europeo de protección de datos para el siglo XXI», en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados*. Madrid: Ariel, p. XVIII.

> o de cooperación con la Unión Europea en las que se vea involucrado el intercambio de datos personales[184].

A continuación, desgranaremos las directrices básicas de la citada propuesta que, de prosperar, será de obligado cumplimiento en todos los Estados Miembros.

3.2.3.1 *Propuesta de Reglamento General de Protección de Datos*

En 2012 y ante las injerencias continuadas en la intimidad y vida privada de los usuarios producidas por ciertas aplicaciones de Internet, la Unión Europea propuso renovar la normativa de protección de datos vigente, centrando su marco de actuación en el refuerzo de las facultades del usuario. Esta propuesta de marco regulador, publicada por la Comisión Europea el 25 de enero de 2012, nace para actualizar la presente Directiva de Protección de Datos que data de 1995, tiempos previos no solo al desarrollo de las redes sociales y muchas de las actuales herramientas, sino incluso a la expansión de Internet.

Se torna, por ello, ineludible adaptar la legislación a los nuevos desarrollos de la Web, como son las citadas redes sociales o los motores de búsqueda. En otras palabras, se requiere estar a la altura de los retos que imponen las tecnologías digitales y la eliminación de las fronteras físicas. En este sentido, la Comisión Europea pretende fijar una normativa común para los Veintisiete en materia de protección de datos, partiendo de la base de que la salvaguarda del derecho a la intimidad y vida privada en Internet constituye, como ya hemos indicado, un principio fundamental que debe ser regulado de manera unánime.

La implementación de dicha reglamentación es más que necesaria. La mayor parte de los usuarios de Internet cree que no se les informa debidamente sobre lo que ocurre con su información personal, a quién se transmite o a qué fin se destinará; del mismo modo que desconocen cómo ejercer sus derechos *online* e, incluso, la existencia de las autoridades de protección de datos[185]. Para contrarrestar esta si-

---

[184] VERGARA PARDILLO, A. y MARTÍNEZ PÉREZ, J. (2012): *Op. cit.,* p. 31.

[185] European Commission (2011): Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_ en.pdf.

tuación de vulnerabilidad, la nueva normativa se presenta como la reforma que conseguirá que la información fluya a todos los ámbitos y que, consecuentemente, los derechos de los individuos sean más comprensibles y fáciles de ejercer.

En resumen, el objetivo cardinal de este texto es que los individuos tengan más control sobre sus propios datos y que la ley que les ampare sea unánime para todos los países de la UE. La información constituye, por ende, el pilar básico de la reforma; una información que genera conocimiento y que subraya dos conceptos básicos en la gestión de los datos privados: el consentimiento y la finalidad. Se trata en definitiva de: «reforzar el derecho a la información de manera que los individuos comprendan por completo cómo se manipulan sus datos personales, en especial cuando las actividades de tratamiento afecten a menores» [186].

Vivian Reding, anterior Vicepresidenta Primera de la Comisión Europea y Comisaria de Justicia, Derechos Fundamentales y Ciudadanía, explica a grandes rasgos en qué consisten los principales cambios introducidos por la reforma [187]:

— En primer lugar, el establecimiento de requisitos explícitos que obliguen a las redes sociales online y otros responsables del tratamiento de los datos a minimizar la cantidad de informaciones personales recabadas, así como un aumento de la responsabilidad de dichas compañías respecto al tratamiento de las mismas. Del mismo modo, se deberá garantizar al individuo la facilidad de acceso a sus propios datos, así como la facultad de obtener una copia de todos aquellos contenidos que han sido almacenados durante el servicio. Se instituye, igualmente, la obligación explícita de que los responsables del tratamiento eliminen los datos personales correspondientes a un usuario si este lo solicita de manera expresa y cuando no exista justificación alguna para su retención. Ya la directiva actual garantiza, en principio, que los individuos puedan solicitar la eliminación de sus datos y que estos no sean procesados durante más tiempo del necesario para los objetivos legítimos para los que se requirieran. El ejercicio de este derecho no contaba, sin embargo, con la implementación

---

186 REDING, V. (2012): *Op. cit.,* p. XX.
187 Ídem.

de herramientas como las redes sociales que complican la ejecución del mismo.

— La implantación de la denominada «privacidad por defecto» y «privacidad desde diseño» [188], en todas las empresas que operan en Internet. La primera, refiere a la exigencia de que los parámetros por defecto sean aquellos que proporcionen más protección y menor visibilidad a los datos del individuo, garantizando así que los contenidos no puedan hacerse públicos *a priori,* tal y como sucede ahora con las redes sociales. En cuanto a la «privacidad desde el diseño» nace para fomentar el uso de tecnologías respetuosas con la salvaguarda de la esfera privada del individuo, en tanto que minimizar el almacenamiento de informaciones personales y garantizar que las medidas de protección de los datos se incorporan desde la etapa de planificación y desarrollo de cada programa.

Ambas implementaciones deberán ser la norma en todas las herramientas de la Web que operen en suelo europeo. Por ejemplo, en las redes sociales se deberán simplificar los diversos controles de visibilidad, clarificando apropiadamente aquellas situaciones en las que los individuos se ven abocados a tomar decisiones referidas a la gestión de sus datos personales. Y, para suministrar dicho poder de elección a los usuarios, la información deberá ser proporcionada de forma comprensible y uniforme. La ventaja de establecer estos dos parámetros es que evita cualquier injerencia ya desde el momento en que se introducen contenidos en la Red.

— Asimismo, la nueva normativa mejorará la capacidad de control que los individuos podrán ejercer sobre sus propios datos, gracias a la obligatoriedad de establecer el requisito del consentimiento informado, garantizando que el usuario da su permiso de manera explícita y conscientemente cuando sus datos sean requeridos. Este consentimiento se otorgará a través de notificaciones o declaraciones que deberán ser claras, precisas y tener un formato homogéneo para facilitar su comprensión, facultando así a los individuos para tomar decisiones plenamente conscientes. De este modo, la Comisión aboga por un incremento de la transparencia en las prácticas de todos los agentes implicados en la comunicación digital.

---

[188] Ambas expresiones han sido traducidas del inglés incluyendo el anglicismo *privacy*, dando lugar a dos locuciones ya generalmente aceptadas.

— Otra de las medidas que se introduce es el «derecho al olvido», mediante el cual se concede a los usuarios de un derecho efectivo a que se eliminen sus contenidos si se retractan de dicho consentimiento o si no existe justificación legítima para retener dichas informaciones (no olvidemos que la finalidad a la que se destinarán nuestros datos constituye un concepto clave a la hora de entregarlos). Este derecho al olvido, que ya existe en la legislación española bajo el membrete de derecho de cancelación, reforzará el control del individuo sobre su propia identidad.

— Igualmente, la nueva legislación equiparará las autoridades nacionales de protección de datos, reforzando su independencia y capacidad de actuación a la hora de resolver las quejas de los interactores. De este modo, las dota de las facultades necesarias para acometer investigaciones, decisiones vinculantes e imponer sanciones efectivas y disuasorias. Se plantea, de este modo, mejorar los medios de que disponen los individuos para ejercer sus derechos eficazmente.

Estas medidas se completan con iniciativas en el terreno de la educación para concienciar a los usuarios sobre las prácticas comerciales de recogida y uso de datos personales, así como con un conjunto de obligaciones para las empresas y proveedores de servicios. Empero, no nos detendremos más en este proyecto, dado que aún no es posible referirlo como consolidado. No obstante, sí tendremos en cuenta algunas de las mejoras planteadas y que recogeremos, ulteriormente, en nuestra propuesta final.

3.2.4 La protección de datos de carácter personal en nuestro ordenamiento jurídico: definición y objeto del derecho

Aunque solo se trate de unos y ceros, la protección de nuestros contenidos es vital, ya que en el mundo digital nuestros datos somos nosotros y su unión es capaz de conformar nuestra identidad digital. Por eso, cuando hablamos de protección es imprescindible hablar de nuestros datos. La concepción de intimidad y vida privada como la capacidad de controlar el acceso a nuestras informaciones personales se vierte en esta normativa, dando cabida a la subjetividad humana y a la capacidad de decisión sobre nuestras informaciones personales.

El derecho fundamental a la protección de datos está regulado específicamente en el artículo 18.4 de la Constitución y comparte con el derecho a la intimidad del artículo 18.1 el objetivo de ofrecer una eficaz

protección constitucional de la vida privada de los individuos. Recordemos que la Constitución Española reconoce en el artículo 18.1: «el derecho al honor, a la intimidad personal y familiar y a la propia imagen» y en el apartado 4 de dicho artículo puntualiza: «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Sin embargo, si bien guarda una relación instrumental con los derechos aludidos en el artículo 18.1 CE, se trata de un derecho de configuración jurisdiccional[189] al que el Tribunal Constitucional ha dotado de autonomía y posee una configuración constitucional propia y definida. Esta capacidad de control de datos aparece ligada al concepto de autodeterminación informativa, clave en la protección y que en esta tesis trataremos en numerosas veces.

El derecho a la libertad informática o autodeterminación informativa adquiere en este momento su máxima expresión. Se trata de un derecho de los denominados de tercera generación que se refiere a las facultades que tiene el individuo con respecto al tratamiento y existencia de sus datos de carácter personal[190], con lo cual adquieren un sentido fundamental las nociones de consentimiento y conocimiento, que trataremos más adelante.

En España, la regulación sobre protección de datos de «carácter personal» se centra, principalmente, en dos normas: La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD)[191] y el Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD)[192]. No obstante, las siguientes normas se proyectan de modo muy particular sobre las Tecnologías de la Información y la Comunicación:

---

189 El primer caso relevante la STC 254/1993. MURILLO DE LA CUEVA, L. (2003): «la primera sentencia sobre el derecho a la autodeterminación informativa», en *Datos Personales*, revista de la AEPD, n. 1, marzo de 2003.

190 ORELLANO, W. (2008): «La transmisión y protección de los datos personales y la privacidad en los blogs», en Flores Vivar Jesús (ed.): *Blogogalaxia y periodismo en red: estudios, análisis y reflexiones*. Madrid: Fragua, pp. 261-267, p. 264.

191 Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD).

192 Real Decreto 1720/2007, de 21 de diciembre.

- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI-CE).
- Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
- Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

De conformidad con lo dispuesto en la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) el objeto de la norma es, según se cita en el artículo 1 del Título I relativo a las Disposiciones Generales: «garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas y especialmente de su honor e intimidad personal y familiar» [193].

4. REFLEXIONES SOBRE EL CAPÍTULO

La acotación terminológica que hemos llevado a cabo en el capítulo que ya toca su fin tiene como objetivo facilitar la comprensión de la realidad aludida por el objeto de estudio de esta tesis, esto es, la dimensión reservada del ser humano. Semejante punto de partida resulta crucial en cualquier estudio de estas características; no solo nos ha permitido clarificar el contenido semántico de las voces indicadas, sino que, por ende, hemos averiguado el porqué del uso de unas expresiones frente a otras. Así convenimos en que, durante el desarrollo del siguiente tratado, hablaremos de «intimidad y vida privada» por ser la entidad que, de manera más certera, representa el objeto de estudio.

De la misma forma, hemos acometido un breve repaso al derecho positivo, recordatorio que no es en absoluto arbitrario, ni resulta banal. La razón no es otra que la necesidad de señalar las asimetrías

---

[193] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Artículo 1.

normativas existentes entre los países donde se ubican las sedes de las empresas de redes sociales, Estados Unidos en su mayoría, y la jurisprudencia de otras regiones. En el caso particular de España, por ejemplo, existen claras diferencias en lo que respecta al alcance de la protección de datos y, por extensión, lo mismo sucede en Europa, entidad supranacional de donde emanan las directrices que posteriormente entran a formar parte de nuestro ordenamiento jurídico.

Estas diferencias a uno y otro lado del Atlántico se encuentran ahora en el difícil trance de la armonización, entendimiento al que obliga ese fenómeno mundial que es Internet. El camino a desbrozar, sin embargo, es arduo. Tradicionalmente, las disparidades más remarcadas son las referidas al nivel de protección que se le otorga a las informaciones privadas de los ciudadanos, una salvaguarda que peca de laxa en Estados Unidos, a diferencia de la doctrina imperante en Europa. Desajustes que, a la postre, generan matices nada desdeñables, como el hecho de que la jurisprudencia norteamericana considere lícita la difusión de datos personales, siempre que estos sean veraces, mientras que en los países comunitarios se argumenta la necesidad de apoyar esta divulgación con el consentimiento informado del usuario.

Todo este proceso tiene lugar en un entorno abierto, donde se difuminan las barreras territoriales aun cuando la normativa sobre derechos de la ciudadanía se crea para un territorio específico, ya sea este de una nación o un ente supranacional, como ocurre con las citadas directivas dictadas desde la Unión Europea. Pero los datos de los interactores dan la vuelta al mundo en cuestión de segundos y, en esta coyuntura, las redes sociales no dejan de ser empresas privadas con carta blanca para hacer las modificaciones que consideren en sus cláusulas y sin previo aviso, dejando al descubierto la Web como un terreno farragoso en cuanto a asuntos legales.

Al romperse la especialidad e intentar conjugar lo global con lo próximo, no solo se quiebra la tradicional barrera entre espacio público y privado, como veremos en el *Capítulo IV*, se produce, igualmente, una desprotección del individuo, por cuanto el amparo de su dimensión reservada no aparece ya sujeta por ley a una barrera territorial. El debate sobre si se puede legislar Internet de manera efectiva está servido; sin desdeñar, por ello, una reflexión previa acerca de

cómo regular este entorno sin caer en una diarrea legislativa capaz de entorpecer el principio de libertad que motivó la creación de la Red.

En última instancia, se torna necesario realizar una aclaración: no todos los países comparten los mismos referentes culturales en torno a qué se considera vida privada o qué debe mantenerse al margen de la mirada pública. Consecuentemente, las distintas concepciones y usos consuetudinarios contarán con protecciones normativas diversas, sin mencionar, incluso, la carencia de ellas. En este paisanaje, armonizar legislaciones pasaría por el impensable intento de una homogeneización cultural en torno a cada ideario, algo que, a todas luces, resulta un intento imposible.

En suma, todo apunta a que la protección de la intimidad y vida privada en un futuro, esperemos que cercano, vendrá de la mano de la flexibilidad y adaptación a cada contexto específico, respetando siempre la capacidad de decisión del sujeto. No es casualidad que, desde todos los ángulos, se acuda al concepto de autodeterminación informativa como un elemento vital en la protección del individuo. E íntimamente ligado a este, el consentimiento informado, libre y activo se consolida como un requerimiento necesario en aquellas transacciones en las que se soliciten nuestros datos privados. Evitaríamos, de este modo, no solo intromisiones indeseadas, sino tener que recurrir, una vez que estas se han producido, a mecanismos como el derecho al olvido en los que, al tratarse de acciones *a posteriori*, el resarcimiento nunca es pleno.

CAPÍTULO III. INTERNET, LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y LAS REDES SOCIALES

SÍNTESIS

Continuamos nuestra definición de términos encaminándonos, en esta ocasión, a la demarcación de aquellos referidos al mundo virtual, ecosistema al que se circunscribe el objeto de estudio y que es a la vez variable de análisis. Para ello, en el presente capítulo intentaremos dar respuesta a la ambigüedad conceptual de algunas de las constantes con las que construiremos nuestra investigación, trance que nos obliga a realizar un somero repaso a su evolución, antecedentes y contexto en el que estas se desarrollan. Nos centraremos, por ello, en el universo que rodea a las voces «Internet», «Tecnologías de la Comunicación y la Información» o «Web 2.0», entre otras muchas, aportando un soporte conceptual fundamental para entender el estado del arte del fenómeno cuyo estudio llevaremos a cabo. En este empeño surgen estas páginas destinadas a clarificar la compleja realidad intangible que conforma el tejido organizativo de nuestra sociedad entera.

1. INTRODUCCIÓN: IMBRICACIÓN DE LAS TECNOLOGÍAS DIGITALES EN LA SOCIEDAD CONTEMPORÁNEA

Afirmaba José Terceiro que la humanidad ha medido su progreso, históricamente, en términos de tecnología[194], con la facultad de que esta cada vez nos ha sobrepasado más velozmente que sus precursoras[195]. Y las herramientas digitales no son ajenas a este proceso. Durante los últimos años de la década de los 80 y a lo largo de los 90, fuimos testigos de la introducción, progresiva y rápida, de este entra-

---

194 Entendida esta como «la suma de todos los medios técnicos mediante los cuales el hombre modifica su ambiente y manera de proceder. BRAJNOVIC, L. (1979): *Op. cit.,* p. 21

195 TERCEIRO, J. B. (1996): *Op. cit.,* p. 29.

mado tecnológico en todos los ámbitos de la actividad humana. Estos novedosos instrumentos y la popularización de su ecosistema más difundido, Internet, han propiciado un cambio de época en todos los sentidos, transformado profundamente muchos de los aspectos que conforman nuestra sociedad y generando, en consecuencia, un contexto sociocultural y político muy diferente al de generaciones anteriores. Un paradigma emergente, en suma, que conocemos genéricamente como Sociedad de la Información (SI).

La denominación de esta coyuntura obedece a un nuevo criterio organizativo en el que el conocimiento genera poder y su moneda de cambio, la información, se convierte en la materia prima más deseada. En este sentido, dado que en esta era naciente la sustancia más valiosa es intangible, necesitamos una serie de tecnologías y soportes físicos para procesarla y que esta produzca conocimiento. Es por ello que el desarrollo y extensión en el uso de las denominadas Tecnologías de la Información y la Comunicación, conocidas por su acrónimo TIC, resulta clave para el avance de la sociedad actual; un potencial ya vislumbrado en sus inicios por la UNESCO, cuando en 1982 definió el alcance de estas herramientas:

> Un conjunto de disciplinas científicas, tecnológicas, de ingeniería y de técnicas de gestión utilizadas en el manejo y procesamiento de la información: sus aplicaciones, las computadoras y su interacción con los hombres y máquinas; y los contenidos asociados de carácter social, económico y cultural[196].

Aunque esta demarcación inicial se encuentra lejos de plasmar la revolución experimentada en las dos últimas décadas por las TIC, sí adelantaba muchas de las capacidades primordiales de este entorno, potencialidades que, posteriormente, la citada organización recalcaría para poner en valor su papel protagonista y la necesidad de su desarrollo como herramientas para alcanzar los Objetivos del Milenio[197].

---

[196] UNESCO (1982): *Repercusiones Sociales de la Revolución Científica y Tecnológica*. París.

[197] UNITED NATIONS (UN) (2000): *United Nations Millennium Declaration*. Resolution adopted by the General Assembly 55/2. Chapter III: Development and poverty eradication.

Consiguientemente, el conocimiento y manejo de estas tecnologías se torna vital para el ciudadano por cuanto implica, tal y como afirma García Jiménez:

> El acceso a enormes volúmenes de información y evidencia que las tecnologías de la información son el epicentro sobre el que pivotan y se estructuran las diferentes áreas que conforman la sociedad (política, economía, educación) [Ahora bien] Es preciso no caer en la falacia de la aldea global, puesto que […] no todo el mundo tiene acceso o porque no todo el mundo sabe manejar las nuevas tecnologías[198].

En la misma dirección apunta Román Gubern cuando advierte de que, en la práctica, un paraíso social basado en las tecnologías, solo podrá ser tal si las desigualdades sociales y culturales previas a la adopción fueran abolidas[199].

Señalada la importancia que implica el conocimiento y correcto manejo de estas tecnologías en la sociedad contemporánea, esbocemos ahora, brevemente, en qué cosiste la realidad que configuran y qué encierran los conceptos con los que jugaremos a lo largo y ancho de estas líneas.

2. LA SOCIEDAD DE LA INFORMACIÓN: NOMENCLATURA Y CARACTERIZACIÓN

> Desde la más remota antigüedad
> todas las sociedades han sido probablemente sociedades
> del conocimiento, cada una a su manera.
> *Hacia las sociedades del conocimiento.* UNESCO[200]

2.1 TERMINOLOGÍA

La Sociedad de la Información comenzó a configurarse conceptualmente con el desarrollo de los satélites artificiales que permitieron acercar, en el tiempo y el espacio, los sistemas de distribución de las

---

198 GARCÍA JIMÉNEZ, L. (2008): «Las ciencias de la comunicación a la luz de las nuevas tecnologías: retos para una disciplina de la incertidumbre», en *Global Media Journal Mexico*, vol. 5, n. 10, p. 104.

199 Román Gubern citado en: FERNÁNDEZ, S. y FUENTES J. F. (dirs.) (2008): *Diccionario político y social del siglo XX español*, Madrid: Alianza Editorial.

200 UNESCO (2005): *Op. cit.*

señales televisivas. Son por ello, los satélites de comunicaciones «los verdaderos responsables de que el mundo se haya convertido, aceleradamente, en la aldea global que preconizara McLuhan»[201]. Dicho esto, ha sido en las últimas décadas cuando el ciudadano medio ha sido capaz de protagonizar y saborear las mieles del cambio tecnológico y comunicativo, en tanto que la sociedad entera se ha impregnado, plenamente, del espíritu que conlleva la nueva realidad.

Así, las tecnologías digitales han sentado los pilares de esta nueva sociedad a la que hemos aludimos genéricamente como: «Sociedad de la Información», término acuñado por primera vez en el *Informe Bangemann*[202] y que se ha convertido en la locución más divulgada. Junto a esta expresión, no obstante, han proliferado otras afines que hacen hincapié en ciertos aspectos del nuevo sistema organizativo, por lo que también nos referimos a la «Sociedad (Global) de la Información (SI)»[203], la «Sociedad del Conocimiento (SC)»[204] o la suma de ambas: «Sociedad de la Información y el Conocimiento» (SIC)[205]. Estas apelaciones vienen a converger en un sentido común, por cuanto reseñan el protagonismo que la información y el conocimiento ostentan en esta nueva coyuntura, una estructura económica y de vida cotidiana «que integra todo tipo de información como fuente principal de riqueza, de producción de conocimiento de distribución de mensajes y, finalmente, de estrategias para tomar decisiones»[206].

No obstante, a pesar de constituir una realidad omnipresente en nuestros días, el tiempo transcurrido desde sus inicios y difusión no ha sido suficiente para solventar la falta de unanimidad terminológica, siendo rebautizada con múltiples nomenclaturas entre las que destacamos:

---

201 CEBRIÁN, J. L. (1998): *Op. cit.,* p. 73.

202 *Informe Bangemann. Europa y la Sociedad de la Información global* (1994). Disponible en: http://www.cyber-rights.org/documents/bangemann.htm

203 Directiva 2000/31/CE del Parlamento de Europa y del Consejo, de 8 de junio de 2000.

204 UNESCO (2005): *Op. cit.,*

205 *GIL LÓPEZ, E. (2014): La importancia del derecho de las TIC y su influencia en los Derechos Fundamentales: La colisión entre el Derecho a la Intimidad y el Derecho a la Tutela Judicial Efectiva en la descarga de archivos*. Tesis doctoral inédita dirigida por Rodríguez Baena, L. UPS p. 17.

206 SAPERAS, E. (1998): *Manual básico de teoría de la comunicación*. Barcelona: Editorial CIMS, p. 31.

«Tercera Ola»[207], «Era de la Información»[208], «Sociedad Digital»[209], «Sociedad de la Conmutación»[210], «Infolítico»[211] «Sociedad Red»[212], «Tercer Entorno»[213] o «Cibersociedad»[214], entre otras. Apelaciones que cuentan con una predecesora inmediata: la «Sociedad postindustrial»[215], tal y como la bautizaron Alain Touraine en 1969[216] y Daniel Bell en 1974[217], adelantándose a los cambios que poco a poco se aventuraban en las décadas inmediatamente anteriores a la explosión del fenómeno.

En el presente trabajo, referiremos en ocasiones a algunas de las nomenclaturas mencionadas, aunque nos decantamos prioritariamente por el uso Sociedad de la Información dado que, tal y como afirma Gil López es el concepto más ampliamente utilizado, tanto por algunos de los autores más fértiles al respecto, como en los distintos organismos de la Unión Europea y compendios normativos españoles. Baste citar, a este respecto, la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a Servicios de la Sociedad de la Información y la Ley 34/2000, de 11 de junio, de Servicios de la Sociedad de la Información y Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

2.2 CARACTERIZACIÓN DE LA SOCIEDAD DE LA INFORMACIÓN

Las distintas denominaciones anteriormente citadas ya nos dan una pista de las características inherentes a esta Sociedad de la Infor-

---

207 TOFFLER, A. (1980): *La tercera ola plaza*. Madrid: Plaza & Janés.
208 GATES, B. (1995): *El camino al futuro*. Madrid: Mcgraw-Hill; y Castells, M. (2001): *Op. cit.,* pp. 18-19.
209 NEGROPONTE, N. (1995): *El mundo digital*. Barcelona: Ediciones B.
210 SCHEER, L. (1994): *La Démocratie virtuelle*. París: Flammarion.
211 MATÍAS, G. (1995): «Telecomunicaciones en el umbral del infolítico», en *Situación*. Bilbao: BBV.
212 CASTELLS, M. (1997): *Op. cit.,* p. 446.
213 ECHEVERRÍA, J. (1999): *Op. cit.,* Barcelona: Destino.
214 JOYANES AGUILAR, L. (1997): *Cibersoceidad*. Madrid: McGraw-Hill.
215 BELL, D. (1974): *The coming of post-industrial society: a venture in social forecasting*. NY: Basic Books.
216 TOURAINE, A. (1969): *La societé post-industrielle*. París: Denoël-Gonthier.
217 BELL, D. (1974): *Op. cit.,*

mación. Para centrar la perspectiva, nos dejaremos guiar por el prolífico Manuel Castells, autor de obras como *La Galaxia Internet* y *La era de la información,* y quien proporciona uno de los mejores encuadres para enmarcar los atributos de esta nueva sociedad. Esboza Castells cómo antes del despliegue de las TIC la estructuración social obedecía a un criterio de territorialidad, con fronteras físicas y límites tangibles, existiendo, por tanto, un «espacio de lugares».

Por el contrario, el colectivismo, la integración de los principios explorados por las teorías del caos, de redes, la complejidad y la autoorganización son las claves sobre las que se sustenta el universo digital. Esto ha provocado, menciona Castells, que se haya reelaborado nuestra concepción del espacio y que la sociedad contemporánea quede establecida conforme a un «espacio de flujos» de información que circula a través de las redes electrónicas de Internet:

> La articulación espacial de las funciones dominantes tiene lugar, en nuestras sociedades, en la red de interacciones que han hecho posible los dispositivos tecnológicos e informáticos. Tal red no existe un lugar en sí mismo, ya que las posiciones se definen mediante flujos[218].

Todo ello, genera «el comienzo de una nueva existencia y, en efecto, de una nueva época: la era de la información, marcada por «la autonomía de la cultura frente a las bases materiales de nuestra existencia»[219]. Es por ello que el autor denomina el nuevo sistema organizativo como «sociedad red», por cuanto se define en relación a los susodichos flujos informativos y el control de la información se constituye como arma poderosa capaz de gobernar en todos los aspectos del ser humano.

La Sociedad de la Información tiene su correlato económico en la «nueva economía» o la «economía digital», contexto en el que, señala Ballesteros Moffa, las intromisiones en la intimidad y vida privada de los ciudadanos comienzan a adquirir mayor protagonismo. No en vano, para el autor «la tutela de la información personal es fruto de la llamada sociedad de la información o del conocimiento»[220]. Este

---

[218] CASTELLS, M. (1997): *Op. cit.,* p. 489

[219] Ibíd., p. 558.

[220] BALLESTEROS MOFFA, L. A. (2005): *La privacidad electrónica. Internet en el centro de protección*. AEPD. Valencia: Tirant lo Blanch, p. 33.

nuevo escenario parte de tres premisas fundamentales: la información como fuente de poder a todos los niveles, la globalización o materialización de la «aldea global» de Mcluhan y el uso de las Tecnologías de la Información y la Comunicación cuya evolución posibilita la convergencia tecnológica[221].

En la misma línea, Campuzano Tomé define la Sociedad de la Información como: «un nuevo modelo de organización industrial, cultural y social caracterizado por el acercamiento de las personas a la información a través de las nuevas tecnologías de la comunicación»[222].

Desde un punto de vista más poético, debemos reseñar la célebre novela *Telépolis* de Javier Echeverría, otro autor necesario y que definió a la perfección las bases de esta aldea global a través de esa metáfora literaria que es el «mundo telepolita»: «una nueva ciudad que está siendo construida a finales del s. xx, formada por estructuras reticulares que tienden a cubrir todo el planeta»[223].

Sea como fuera y basándonos en cualquiera de las aproximaciones citadas, lo cierto es que en este «Tercer Entorno» el manejo de las tecnologías se configura como condición indispensable para acceder al conocimiento que posibilita el desarrollo humano, generando a su vez una retroalimentación continua, un movimiento circular, en tanto que dicho conocimiento es substancial y promueve un uso más seguro de las herramientas digitales. Este hecho no es algo novedoso en sí. Para el profesor Davara, la información es un elemento clave que ya desde el principio de los tiempos da gran poder a quien la posee, aupando una nueva clase de individuos más poderosos: los poseedores de información[224]. Se crea así una línea digital divisoria entre «informados» y «desinformados» en palabras de Flores Vivar[225] o «enchufados» y «desenchufados», en la terminología de Cebrián[226].

---

221 Ibíd., p. 33.

222 CAMPUZANO TOMÉ, H. (2000): *Op cit.,* p. 20.

223 ECHEVERRÍA, J. (1994): *Op cit.*

224 DAVARA RODRÍGUEZ, M.Á. (2001): *Manual de Derecho Informático*. Madrid: Aranzadi, p. 23.

225 FLORES-VIVAR, J. (2004): «Internet ya es una realidad y la brecha digital, también. Mitos y realidades de Internet en la sociedad», en *Revista A distancia,* UNED, vol. 22, n. 1, p. 1.

226 CEBRIÁN, J. L. (1998): *Op. cit.,* p. 98.

3. CONCEPTUALIZACIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Centrémonos ahora en las herramientas tecnológicas. Dado que la acepción «Tecnologías de la Información y la Comunicación» aparece como la más ampliamente aceptada, será una de las que usaremos principalmente en este trabajo aunque sin desdeñar, por ello, otras acepciones descriptivas de la realidad que nos ocupa como «tecnologías digitales». A continuación, desgranaremos qué aparece contenido en dicha locución tan abundantemente citada. Sí bien, evitaremos incluir el adjetivo «nuevas» que habitualmente acompaña a su designación, atendiendo a razones que reseñaremos en el siguiente apartado.

3.1 LA APELACIÓN «NUEVAS» EN LA DENOMINACIÓN DE LAS TIC

La dificultad para acotar conceptualmente qué se conoce como Tecnologías de la Información y la Comunicación recae no solo en la confusión que produce la amplitud de manifestaciones que, a menudo, se engloban bajo dicho epígrafe, sino en la ambigüedad temporal que introduce el término que, en ocasiones, se intenta demarcar introduciendo el calificativo «nuevas». En este sentido, algunos autores como Parra Valcarce y Álvarez Marcos cuestionan la categorización de dichas tecnologías bajo el mencionado calificativo ya que, aunque en un primer momento podría facilitar la distinción de estas tecnologías de los medios de comunicación tradicionales, la vaguedad y falta de delimitación que conlleva el término vacía su capacidad de definición[227]. En consecuencia, si tomamos el adjetivo «nuevas» como referencia de «novedad» y en vista de la velocidad a la que se actualiza la tecnología, no podremos fijar formalmente la diferencia entre las tecnologías de reciente aparición y aquellas que han sido desplazadas y que se reconvierten en precursoras de las actuales. En este sentido Cebrián Herreros afirma:

---

[227] PARRA VALCARCE, D. y ÁLVAREZ MARCOS, J. (2004): *Ciberperiodismo*. Madrid: Síntesis, p. 13.

> No hay ni viejas ni nuevas tecnologías sino fases de expansión, de *big bang* progresivo del que van surgiendo las diversas innovaciones en tanto que antiguos y recientes cambios de unas y otras tecnologías. Por tanto, no hay cortes bruscos entre lo viejo y lo nuevo. Todo depende del subjetivismo que pongamos en uno y otro caso[228].

El carácter relativo que añade el adjetivo «nuevas» en la catalogación de las citadas herramientas comunicativas va más allá de la confrontación temporal que produce la aparición de una tecnología frente a otra ya existente. Esta temporalidad difusa empapa todo el proceso comunicativo. Así, desde la óptica del usuario individual, la nueva tecnología es aquella que acaba de descubrir o a la que tiene acceso por primera vez, mientras que otras personas las usan desde hace años, desde sus primeros desarrollos, o tras su comercialización industrial.

Por otra parte, en numerosas ocasiones sus orígenes no solo no son recientes sino que se producen o se mezclan con tecnologías tradicionales. A este respecto, autores como Cabero se preguntan si de verdad estas tecnologías son tan novedosas como creemos:

> ¿Cómo podemos hablar de Nuevas Tecnologías si el primer ordenador comercial aparece en los años cincuenta? Pese a que hay cierto consenso en considerar Nuevas Tecnologías a todos aquellos recursos y medios técnicos que giran en torno a la información y a la comunicación […] no son tan nuevas en el sentido de su utilización como recurso didáctico, sino más bien en tanto que abren nuevos canales y entornos de comunicación y expresión.[229]

Ahora bien, parte sustancial de la problemática que introduce el adjetivo «nuevas» se debe a la acrecentada tendencia a definir las TIC desde una vertiente exclusivamente técnica, con visiones conceptuales que, desde una óptica restrictiva, se centran en solo una parte de la realidad que reflejan. Desde dicho vértice, las TIC se definirían haciendo referencia al conjunto de herramientas o medios electrónicos, soportes y canales que crean, almacenan, recuperan y transmiten información a grandes velocidades y en grandes cantidades. Según este

---

228 HERREROS, C. (2000): «La información en Red», en *Sphera Pública, revista de ciencias sociales y de comunicación*, pp. 9-28, p. 19.

229 CABERO, J. (comp.) (2000): *Las nuevas Tecnologías Aplicadas a la Educación*. Madrid: Síntesis.

planteamiento, el uso del término «nuevas» como paraguas aglutinador no tendría razón de ser por cuanto cualquier actualización o versión de una herramienta tecnológica dejaría obsoleta la anterior, más aun, cuando hablamos de instrumentos que se modernizan a gran velocidad. A este respecto algunas voces[230] abogan por el uso de términos más restrictivos o, incluso defienden la no utilización del adjetivo sino, únicamente, Tecnologías de la Información y la Comunicación.

Por otra parte, es cierto que centrarnos en la novedad o no de estas aplicaciones guiándonos exclusivamente por un criterio cronológico y de renovación tecnológica nos llevarían a definir las TIC de una manera incompleta. Estaríamos, por tanto, desdeñando lo que verdaderamente resulta novedoso: los cambios que introducen en el proceso comunicativo, el tipo de comunicación que posibilitan y las capacidades de difusión de la información. Por ello, aun cuando el uso del término «tecnología» refiere indiscutiblemente tanto a los equipos o soportes físicos como a todos aquellos tratamientos lógicos, lenguajes técnicos o programáticos que hacen posible la comunicación, se nos antoja la necesidad de una definición integral en tanto que la realidad técnica, por sí sola, no deja entrever las verdaderas potencialidades de las TIC. Sin perder de vista su naturaleza tecnológica, urge ampliar el análisis del nuevo medio desde una vertiente comunicativa, señalado aspectos como la innovación en los procesos de intercambio de información, la revolución social que conlleva o su carácter aglutinador, entre otros. Se trata, como afirma Dominique Wolton, de «salir del falso debate de antiguos contra modernos medios de comunicación […] en definitiva desatar el nudo de la ideología técnica y sugerir que la comunicación en la gran cuestión»[231].

Asimismo, sin necesidad de juzgar su novedad en cuanto que temporalidad, existe un hecho que traza una frontera visible entre el nuevo medio y las tradicionales tecnologías, valor diferencial que, paradójicamente, tiende un puente entre unas y otras: la convergencia. «El principio de convergencia, la interactividad y el uso de un lenguaje digital como nexo común son características esenciales que definen

---

[230] PARRA VALCARCE, D. y ÁLVAREZ MARCOS, J. (2004): *Op. cit.,* p. 13, y HERREROS, C. (2000): *Op. cit.*

[231] WOLTON, D. (2000): *Internet, ¿y después?: una teoría crítica de los nuevos medios de comunicación,* Barcelona: Gedisa, p. 131.

las TIC»[232], algo que bien podría justificar su calificación de «nuevas». Es cierto que las TIC se encuentran en un proceso constante de actualización o innovación, mejora e implementación de sus funcionalidades, sin embargo, su especificidad recae inevitablemente en la capacidad que ofrecen de integración generalizada de las funciones de dichas tecnologías en diferentes espacios sociales, propiciando una interactividad hasta antes desconocida y fomentando un cambio en el proceso y las estructuras comunicativas, que bien suponen un antes y un después respecto a los medios tradicionales. Todo ello se resume si tenemos en cuenta que la mayor parte de estas tecnologías funcionan en un medio, Internet, que sí es nuevo y marca un salto evolutivo respecto a los anteriores. Así, estableciendo la novedad como criterio definitorio sería más correcto aplicarlo al entorno Internet, en el que habitualmente actúan las Tecnologías de la Información y la Comunicación, materializándose las características más rompedoras de la propia naturaleza del medio en dichas herramientas.

Por ese motivo, partiendo de la base de que la novedad acota el entorno digital pero no necesariamente a las tecnologías y, parafraseando a Cebrián Herreros, hemos decidido elegir una «fase de expansión» para ceñirnos a una acotación temporal (la comprendida entre los años 2004 y 2014) con el fin de enmarcar el estudio de manera más rigurosa y evitar así los vacíos y redundancias semánticas del término «nuevas». Evitamos, igualmente, que la palabra «nueva» vaya ligada a la obsolescencia que, evidentemente, imprimirá el paso del tiempo a la presente investigación.

3.2 DE LA «COMUNICACIÓN» Y LA «INFORMACIÓN»

Conviene señalar, en este punto, que las voces «información» y «comunicación» hacen referencia a dos realidades que, aunque relacionadas entre sí, representan naturalezas distintas. En su definición nominal o etimológica, «información» tiene dos sentidos que provienen del latín. El primero, refleja la etimología de *informatio*, *informationis, informare* (voz latina de 1190) que significa «dar forma, formar ordenar o dar un significado», derivando a su vez del verbo

---

[232] PARRA VALCARCE, D. y ÁLVAREZ MARCOS, J. (2004): *Op. cit.,* p. 12.

informo que significa «formar». El segundo significado, más tardío (1450) significa «poner a alguien al corriente de algo». Su semántica varía así del término «comunicación», de procedencia igualmente latina (1361): *communicatio*, *communicationis*, voces que a su vez provienen del verbo *communico*, *comunicas, comunicare* y cuyo significado hace referencia a «poner algo en común con los demás, compartir». La comunicación es, en su primera acepción, un intercambio entre un emisor y un receptor, y refleja lo que todos esperamos de dicho acto: «compartir algo con alguien». El segundo sentido, más reciente, refleja la idea de difusión y estaría en consonancia con el desarrollo de la prensa. Esta bifurcación de semánticas genera, según Dominique Wolton, dos realidades: de un lado la «comunicación normativa» que refleja la idea de compartir y de otro la «comunicación funcional» que refiere al intercambio y difusión de información en el seno de la sociedad. El vínculo que se establece entre información y acontecimiento parte, según Wolton, de este último significado, lo que revela una doble cara: «La información consiste en relatar el acontecimiento, es decir, todo lo que perturba y modifica la realidad. […] Es a la vez lo que da forma, lo que da sentido y lo que organiza lo real y, al mismo tiempo es la narración de lo que surge y perturba el orden»[233].

No obstante, aunque desde su origen ambas voces definen esencias distintas, en numerosas ocasiones ambos vocablos son confundidos o usados de manera errónea. A este respecto, podemos recurrir a la diferencia que Luka Brajnovic establece entre ambas en su tratado *El ambiente científico de la información*:

> La información es el conjunto de las formas, condiciones y actuaciones para notificar o hacer saber, individual o públicamente, los elementos de conocimiento de hechos, de sucesos, de actividades y proyectos, de datos históricos o previsibles, todo ello mediante un lenguaje adecuado y comunicable, utilizando palabras y signos, señales y símbolos, expresados directamente o a través de las conductas y sistemas aptos para este fin, como son los medios de comunicación social o cualquier otro procedimiento instrumental o especulativo. (…)La comunicación es el conducto, contacto directo, contagio o encuentro creativo que une distancias, presencias, estados de ánimo o disposiciones sugerentes y creati-

[233] WOLTON, D. (2000): *Op. cit.,* pp. 229-230.

> vas, sin el fin de suyo informativo, aunque puede ser el vehículo de la información. [234]

La Comisión Internacional de Estudios de los problemas de la Comunicación, más popularmente conocida como *Informe MacBride* se hace eco de la confusión que a menudo arrastran dichos vocablos y añade:

> Procede destacar que, en ciertas obras especializadas, se confunden o emplean sin distinción las palabras «información» y «comunicación». En el presente informe, han sido utilizadas del modo más coherente posible, refiriéndolas a dos fenómenos distintos: la comunicación es el proceso de intercambio de informaciones, hechos, opiniones y mensajes entre los individuos y los pueblos; la información es un «producto», independientemente de que se trate, por ejemplo, de noticias, datos y de los demás elementos o contenidos de los medios de información de las actividades o de las industrias culturales. […] El concepto de información se refiere a los signos o mensajes codificados, transmitidos unilateralmente por un emisor (fuente) o un receptor, mientras que la comunicación corresponde más a la complejidad de los fenómenos de intercambio, de todo tipo, que se producen por medio de signos entre los individuos y los grupos[235].

La comunicación es pues un proceso, mientras que la información constituye el producto de dicho proceso. La confluencia de ambas realidades conformaría el éter de «la comunicación social».

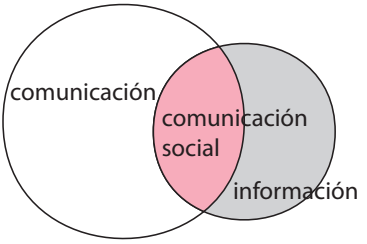

Figura 3.1 La comunicación social[236]

---

[234] BRAJNOVIC, L. (1979): *Op. cit.,* pp. 36-37 y 45

[235] MACBRIDE, S. (1980): *Un solo mundo, voces múltiples*. París: UNESCO, Fondo cultura económica, p. 491.

[236] BRAJNOVIC, L. (1979): *Op. cit.,* pp. 36-37 y 45.

Ambos conceptos, aun coincidiendo en un campo común, el referido a la comunicación social, abarcan universos distintos. La comunicación se significa en un área más extensa que la representada por la información, por cuanto, tal y como afirma Brajnovic «casi toda información es comunicada, pero no toda la comunicación es informativa»[237]. En consecuencia, «no debe confundirse información y comunicación; la primera constituye el tratamiento que recibe aquello que se va a comunicar; la comunicación es la consecuencia de ese proceso, una situación de comunicación»[238].

Por su parte, en su obra *Teoría de la información y la comunicación efectiva,* Eva Aladro contribuye con un clarificador enfoque que explicita las interrelaciones que se establecen entre «comunicación» e «información»:

> La comunicación es el proceso generador de información. No se produce jamás pérdida de información en un proceso comunicativo activo. La comunicación produce información incluso cuando no obtiene respuesta y no se produce recepción[239].

La información constituye un conjunto de datos organizados y seleccionados de tal modo que adquieren un valor adicional más allá del propio[240]. Una vez adquirida, debe ser transferida a otros miembros de la comunidad y la comunicación constituye el único medio posible para trasladar este conocimiento, que es a su vez fuente de cultura[241]. De ahí el interés del ser humano por una continua evolución de los medios de comunicación, proceso que viene de la mano de los avances tecnológicos lo que subraya su capital importancia.

---

237 Ibídem, p. 42.

238 BENITO, Á. (dir.) (1991): *Diccionario de ciencia y técnicas de la comunicación.* Madrid: Paulinas, p. 185.

239 ALADRO VICO, E. (1999): *Teoría de la información y la comunicación efectiva.* Madrid: Fragua, p. 14.

240 Esto nos traslada al concepto de «sinergia», unión de energías en las que «el todo es mayor que la suma de sus partes», y cuya substancialidad fue enunciada por Aristóteles y en su libro *Metafísica.* El axioma, recuperado por la escuela de La Gestalt (palabra alemana que quiere decir «conjunto, configuración, totalidad o forma) se referencia cuando estudiando cada elemento del sistema por separado no se explica el sistema, pero todos los elementos juntos adquieren un significado capaz de dar sentido.

241 GIL LÓPEZ, E. (2014): *Op. cit.,* p. 17.

4. EL CANAL INTERNET: NUEVO MEDIO DE COMUNICACIÓN DE LA SOCIEDAD DE LA INFORMACIÓN

La Red de redes, a la que citaremos en mayúsculas para diferenciarla de todos aquellos sistemas de nodos interconectados que no son Internet aunque operan en su seno, conforma el paradigma de la Sociedad de la Información, pues en ella se concentran las citadas tecnologías a través del lenguaje digital. Hemos convenido anteriormente en el poder sustantivo de la información en este nuevo tejido marcado por la inespecificidad y en el que navega nuestro objeto de estudio. No obstante, sus peculiaridades merecen cierta reflexión y detenimiento, razón por la que en los siguientes apartados, analizaremos más a fondo la naturaleza del sustrato en torno al que pivota la citada transformación tecnológica.

4.1. DELIMITACIÓN CONCEPTUAL

> La línea consta de un número infinito de puntos;
> el plano, de un número infinito de líneas;
> el volumen, de un número infinito de planos;
> el hipervolumen, de un número infinito de volúmenes
> Borges, *El libro de arena*[242]

La misma falta de consenso en lo denominativo que encontrábamos al referirnos a la Sociedad de la Información se aprecia en el ente que canaliza los flujos de intercambio de datos en la realidad digital. El lector se percatará por ello de que, a lo largo de esta investigación, referiremos una amplia variedad de términos que, al fin y a la postre, señalan al medio común o en el que funcionan dichas tecnologías, así como el ecosistema propio que generan. Hablaremos, a este respecto, de «entornos digitales» o «espacios mediados (digitales)», cuando no mencionaremos directamente la expresión «espacio digital». Vocablos, todos ellos, que vienen a ilustrar esa entelequia sin espacialidad que generan las tecnologías.

A este tenor, no está de más refrescar la memoria con una voz ampliamente aceptada: la denominación «ciberespacio» que refiere acer-

---

[242] BORGES, J. L. (1975): «El libro de arena», en *Ficciones,* Buenos Aires: Emecé.

tadamente al «ente abstracto que da cobertura a la Sociedad de la Información»[243]. Un conglomerado conceptual donde se intercalan relaciones humanas y datos, empleando la tecnología de la comunicación a través de las computadoras. El término, acuñado a raíz de la aparición en 1984 de la novela *Neuromante* de William Gibson[244], deriva del prefijo *cyber,* que a su vez proviene del griego *kybernetique* o arte de la navegación (de ahí que los programas de acceso reciban el nombre genérico de «navegadores»). No obstante, su definición más certera proviene de Johnson, que utiliza el término para referirse a «la red de líneas telefónicas que tienen la capacidad de entrelazar todos los ordenadores entre sí»[245].

Por su parte, lo más frecuente es que al referirnos al nuevo canal mencionemos directamente «Internet», ora como «la Red» con mayúsculas, ora como «la Web», esto es: «la infraestructura en la cual se asienta, se reproduce y extiende el ciberespacio, es decir, el espacio (o la colección de espacios) creados por la comunicación entre computadoras»[246]. La razón es sencilla: las actuales posibilidades que ofrecen las Tecnologías de la Información y la Comunicación se deben, sin duda, a la aparición, posterior desarrollo y, sobre todo, a la extraordinaria popularización de Internet. A esta también se la conoce, por generalización, como la «Red», así como por el nombre de su protocolo «World Wide Web» que al que se alude, por simplificación denominativa, como la «Web».

4.2 QUÉ ES INTERNET. BREVE HISTORIA DE LA «RED DE REDES»

Sabemos que el despegue de Internet como medio de comunicación de masas, esto es «el uso de Internet como sistema de comunica-

---

243 GIL LÓPEZ, E. (2014): *Op. cit.,* p. 20.

244 GIBSON, W. (2007): *Neuromante*, Barcelona: Minotauro. De Gibson, que escribió el relato en 1983, se ha dicho que es «uno de los primeros escritores que imaginó un mundo de redes mundiales de computadoras, piratas informáticos, virus, programas de ordenador copiados ilegalmente y dinero electrónico». LEWIS, P. H. (1995): «William Gibson: creador del término Ciberespacio», entrevista en *El País*, 4 de junio de 1995, p. 29.

245 JOHNSON, D. (2009): *Op. cit.,* p. 140.

246 TREJO DELARBRE, R. (1996): *Op. cit.,* p. 56.

ciones y como forma organizativa, hizo eclosión en los postreros años del segundo milenio» [247]. A finales de 1995, primer año del uso generalizado del *World Wide Web,* la Red había congregado unos 16 millones de usuarios en todo el mundo[248]. No obstante, se torna necesario realizar un breve repaso a su corta aunque nutrida historia para entender cómo de mera herramienta informática se ha pasado a medio de comunicación, un hecho transcendental en el estudio que tenemos ante nosotros y para cuya comprensión traeremos a colación los vericuetos que han ido dando forma a este entorno dialógico. Igualmente, conviene abordar dicha revisión ya que muchos de sus condicionamientos estructurales y que mencionaremos posteriormente estarán íntimamente ligados a su desarrollo.

4.2.1 **Apuntes sobre los antecedentes de la Red**

Decía el novelista británico Graham Greene que «una historia no tiene ni principio ni fin; arbitrariamente, uno elige un momento de la experiencia desde el cual mirar hacia el pasado o el futuro» [249]. Aunque expropiada de su contexto inicial, esta premisa adquiere, si cabe, mayor relevancia cuando hablamos de los avances tecnológicos que, muy lejos de aparecer por generación espontánea, se constituyen frecuentemente como un cúmulo de experiencias heredadas de sus predecesores. (Y lo mismo sucede con los problemas éticos referidos a la intimidad y vida privada que, como veremos en el siguiente capítulo, son herederos de lo ocurrido con los medios tradicionales). No obstante, si hemos de emplazar un referente temporal para abordar la aparición de Internet tal y como la conocemos hoy, nos decantaremos por el lugar común que señala a ARPA-Net como el embrión del movimiento revolucionario protagonizado por las nuevas tecnologías.

Ello nos impele a retrotraernos a finales de los años sesenta, concretamente a 1969, fecha en que nace la red ARPA promovida por el Gobierno de los Estados Unidos a través de la Agencia de Proyectos de Investigación Avanzados de Defensa (*Defense Advanced Research Proyects Agency,* ARPA/ DARPA) y bajo la responsabilidad de Vinton Cerf.

---

247 CASTELLS, M. (2001): *Op. cit.,* p. 16-17.
248 Ídem.
249 GREEN, G. (1951): *The End of the Affair,* Reino Unido: Heinemann.

Tejida entre dos universidades del norte de California, esta primigenia malla descentralizada nació con el propósito de facilitar el trabajo de los investigadores universitarios a cargo del Departamento de Defensa, interconectando, por medio de satélite y radio, varias redes capaces de operar en un entorno fragmentado. Se pretendía, de este modo, asegurar un sistema mediante el cual varios ordenadores fuesen capaces de «dialogar» entre sí aun cuando partes de la misma red se averiasen, permitiendo la conexión y desconexión de equipos sin perjuicio para la transmisión del mensaje: «cada nodo de la red tendría autonomía y poder para transmitir, vehicular y recibir mensajes»[250].

El acierto de este diseño recaía, por tanto, en que la red estaba descentralizada, lo que suponía múltiples caminos entre cada dos puntos y en la que se dividían los mensajes completos en fragmentos para que, al seguir tramos distintos, se asegurase su llegada. El fin último de este desarrollo no era otro que encontrar una manera de acceder y distribuir información, sorteando posibles eventualidades de interrupción súbita de las telecomunicaciones como, por ejemplo, en caso de una catástrofe, una crisis bélica o un ataque nuclear. Cruzando esta máxima con las fechas que datan su creación, dibujamos irremediablemente el paisanaje de la Guerra Fría. No obstante y a pesar de su motivación inicial, pronto fue dominada por la información que fluía hacia las universidades, laboratorios e institutos de investigación[251], en detrimento de los primigenios intereses bélicos.

Avanzando en este sentido, el 29 de octubre de 1969 se transmite el primer mensaje a través de ARPA y un mes más tarde, se establece el primer enlace entre las universidades de Stanford y UCLA. Seguidamente, se conectarían entre sí las computadoras de las ya citadas instituciones académicas con la Universidad de Utah y la Universidad de California en Santa Bárbara.

Cuesta creer que este arcaico sistema de transferencia electrónica fuese capaz de dar lugar al actual Internet. No obstante, tras al establecimiento de este primer conjunto de enlaces, instituciones académicas

---

250 ARMAÑANZAS, E., DÍAZ NOCI, J. y MESO, K. (1996): *El periodismo electrónico, información y servicios multimedia en la era del ciberespacio*. Barcelona: Ariel, p. 54.

251 KROL, E. (1995): *Conéctate al mundo de Internet. Guía y Catálogo*. Méjico: Mc Graw Hill.

de otros países se añadieron al proyecto que contó, en sus primeros pasos, con fondos federales para su expansión. Este hecho, sumado al establecimiento subsiguiente de un entramado global facilitado por un protocolo común para las transmisiones, sentará las bases que posibilitarán su posterior eclosión. Prosigamos en nuestro relato sobre el nacimiento y configuración de todas esas redes iniciales de las que, como si de afluentes se tratase, se ha nutrido la Red actual.

4.2.2 **Los primeros pasos**

ARPA-Net, cual organismo vivo, se transforma, sigue creciendo y tomando forma. Durante los años setenta, sigue añadiendo estaciones de acceso bajo un uso destinado todavía a la investigación y desarrollo. En el año 1971 se añaden 20 nodos a la red primigenia, que llegan a un total de 37 en 1972 después de que DARPA financiase la instalación de 30 terminales como parte del programa. El aumento de la cifra de usuarios, aunque testimonial, lleva a crear muchos de los servicios de los que actualmente disponemos, como el correo electrónico, creado en 1972 por Ray Tomlinson o la transferencia de archivos FTP un año más tarde. Como resultado de su adopción, su uso continúa dibujando una línea ascendente y en 1975, ARPA transfiere la dirección de la red a la Agencia de Comunicación de Defensa (*Denfence Communication Agency*, DCA).

Hasta ese momento, todos los ordenadores se conectaban al proyecto a través de un protocolo denominado NPC o «Programa de Control de Red» *(Network Control Protocol)* pero la introducción en 1977 del sistema de transmisión TCP/IP, «Protocolo de Control de Transmisión/Protocolo de Internet» *(Transmisión Control Protocol/ Internet Protocol)* permitió la creación de redes de carácter no militar. Convivían así, junto a ARPA-Net, las redes CS-Net *(Computer Science NetWork)* destinada al intercambio de documentos científicos y MIL-Net, extensión militar del proyecto ARPA.

A comienzos de los ochenta se habían registrado poco más de doscientos ordenadores servidores[252], cifra que comienza a aumentar tímidamente después de que, en 1983, estas tres grandes redes se inter-

---

[252] TERCEIRO, J. B. (1996): *Op. cit.,* p. 95.

conectaran entre sí, configurando una única malla en los Estados Unidos[253]. Dicho enlace múltiple se considera un hito clave en la prehistoria de Internet, por cuanto conseguía dar así el salto al usuario universal, aunque, por el momento, este debía disponer de una serie de conocimientos informáticos para emprender el acceso que no estaban al alcance de cualquiera.

En noviembre de 1986, el número de servidores conectados llega a 5.000, cifra que se incrementa hasta 20.000 solo un año más tarde. Es también en esta fecha, cuando la Fundación Nacional para la Ciencia *(Nacional Science Foundation*, NSF) crea su propia red ante las trabas burocráticas que encuentra para el uso de ARPA-Net. La institución, que se propone la interconexión de datos entre varias entidades científicas, lanza así la NSF-Net, alternativa que, al transcurrir los años, se convertirá en el verdadero esqueleto de Internet[254].

En 1988, ARPA-Net se convierte en la base física de conexión con toda la red que comprende la malla tejida sobre el protocolo TCP/IP. No obstante, en 1990 deja de existir sustituida por la NSF-Net que, con el paso de los años, constituiría la base fundamental de lo que hoy conocemos como Internet. Para entonces, la cifra de servidores conectados superaba los 100.000, e Internet se convertía en «la Red por antonomasia. El embrión donde nacen y se asientan todas las redes del mundo virtual. […] Sitio obligado de paso para todo el mundo» [255].

4.2.3 Los pilares del nuevo medio de comunicación de masas: El nacimiento de la World Wide Web, el lenguaje hipertextual y los navegadores

Saltamos ahora de continente. Internet es una malla gigante de redes entrelazadas e interconectadas bajo el protocolo TCP/IP, una gigante «tela de araña» [256] en la que encontrar la información requeri-

---

253 ARMAÑANZAS, E., DÍAZ NOCI, J. y MESO, K. (1996): *Op. cit.,* p. 55.

254 PARRA VALCARCE, D. y ÁLVAREZ MARCOS, J. (2004): *Op. cit.,* p. 51.

255 FLORES VIVAR, J. M. (2009): «New Models of Communication, Profiles and Trends in Social Networks», en *Comunicar,* Vol. XVII, n.º 33, 2.º semestre, 1 octubre 2009, p. 74.

256 CEBRIÁN, J. L. (1998): *La Red*, Madrid. Santillana, p. 49.

da puede convertirse en un auténtico quebradero de cabeza o, incluso, un empresa imposible a medida que aumenta el número de nodos y se extienden sus ramas. Sin la correcta organización, sería como buscar un aguja en un pajar que nunca para de crecer. Para evitar dicha situación, en 1989 el Centro Europeo de Investigación Nuclear (CERN) de Ginebra creó el lenguaje que propiciaría la posterior eclosión mundial de Internet, en tanto que lograba simplificar enormemente su uso mediante interrelaciones no lineales: hablamos del «hipertexto», el «lenguaje de marcas de hipertexto» (*Hipertext Markup Language,* HTML) o, simplemente, el «lenguaje de vínculos».

El hallazgo no fue arbitrario. El laboratorio empezó a desarrollar un sistema que facilitara a sus investigadores el uso de los archivos que manejaban en la Red y que, a la vez que, permitiera incluir unos documentos en otros a través de los adecuados enlaces. Haría así aparición la *World Wide Web*, conocida por sus siglas «www» y cuyos documentos, en formato ASCII, incluyen los comandos del citado estándar HTML. Dicho sistema hipertextual no es sino un modo de marcar partes dentro de un documento para que el ordenador identifique dónde están. Estas marcas se realizan mediante hiperenlaces (*hiperlinks*) que son líneas de código HTML que permiten a los lectores acceder a otra página Web al pulsar sobre los vínculos, obteniendo la dirección o URL (Universal Resource Locator)[257] de una nueva página. En definitiva, el hipertexto permite vincular varios documentos a través de palabras o frases, de manera no lineal, secuencial, ni jerárquica, sino imitando las relaciones y el sistema de asociaciones generadas en el cerebro humano, gracias a la creación de programas de almacenamiento y recuperación electrónica de la información[258].

Mediante esta estructuración lógica se crea el lenguaje interactivo por antonomasia, similar al de los seres vivos y que permite establecer hiperenlaces con otros documentos que no tienen por qué estar en el

---

[257] La URL es una suma de letras y cifras que identifican la dirección de la página, esto es, dónde se haya ubicada. Las primeras letras corresponden al método de acceso (http y ftp, entre otros). Posteriormente, señalado por dos puntos y una barra doble, se detalla la dirección del ordenador anfitrión del que deseamos obtener la dirección. Finalmente, aparece indicada la ruta de acceso, es decir, el directorio o archivo al que queremos acceder.

[258] CABRERA, M. A. (2000): *La prensa online. Los periódicos en la «www»,* Barcelona: CIMS, p. 248.

propio ordenador. Igualmente, posibilitará la conjugación de contenidos audiovisuales y texto mediante el *hipermedia*, lo que proporcionará el actual armazón dinámico de la Web. El sistema de hipervínculos supone, por ello, la expresión máxima de la interactividad en el universo digital, por lo que no es de extrañar que se considere a sus creadores, el británico Tim Berners-Lee y el francés Robert Caillau, como los verdaderos padres de Internet[259].

La implantación del «www» como plataforma de fácil acceso y sencilla utilización vio públicamente la luz en 1991. Tras su adopción, el ascenso de la Red fue imparable, propiciando un crecimiento gigantesco y acelerado, en tanto que reconvertida ya en una auténtica malla tupida a nivel mundial. Si en el año 1990 había 159.000 puestos conectados a Internet, en 1994 el número estaba cerca de los cuatro millones de computadoras conectadas con más de 30 millones de usuarios[260]. Trejo cita, a colación, las palabras del Ministro de Ciencia de Gran Bretaña, David Hunt, quien explica el éxito de la Red con las siguientes palabras:

> Hasta hace poco, la Red era una bestia hostil e intimidatoria, a la que solo podían controlar los expertos en computación. La *Worl Wide Web* ahora tiene las posibilidades destacadas de la Internet y el resultado es que el pasado año [1994] su uso aumento un 350 mil por ciento[261].

Lo que había empezado bajo el mando de la Guerra fría, afirma Whitaker, se había desbordado de sus confines, convirtiéndose en algo sin precedentes:

> Esta fusión tecnológica ha creado un nuevo mundo, espacio, que no existe en ninguna parte pero está en todas partes y que constituye una tabula rasa en el sentido de que se construye y reconstruye constantemente, se escribe y se rescribe mediante la acción simultánea de todos los usuarios de la Red y su consiguiente reelaboración de la misma[262].

---

259 BERNERS-LEE, T. (2008): *Tejiendo la red*. Madrid: Siglo Veintiuno de España Editores.

260 TREJO DELARBRE, R. (1996): *Op. cit.,* p. 91.

261 HULM, P. (1995): «The Worl Wide Web», *Crosslines*. Citado en TREJO DELARBRE, R. (1996): *Op. cit.,* p. 62.

262 WHITAKER, R. (1999): *El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad*. Barcelona: Paidós, p. 74.

Empero, tras la creación del hipertexto hubo todavía que esperar a la aparición del primer navegador capaz de interpretar el lenguaje de transmisión y traducirlo de forma inteligible para el receptor, ya convertido plenamente en agente activo del cambio tecnológico. De hecho, es a partir de ese momento cuando el ciudadano de a pie comienza a protagonizar, lentamente, la revolución digital. Ya no se requerían complicados procedimientos, ni destrezas específicas para establecer la comunicación, sino que bastaba con pinchar en un icono que le guiaba a través de la Red, donde la información aparecía organizada forma de «páginas Web». Dichos documentos aparecen alojados en millones de ordenadores que se reparten por todo el planeta y a los que se puede acceder desde cualquier punto geográfico a través de las palabras claves que genera el hipertexto. Asimismo, los contenidos son tan diversos como los sujetos que se conectan y la información se puede descargar en el ordenador, modificarla y volver a enviarla aumentando, exponencialmente, los volúmenes de consulta que posee esta inmensa biblioteca mundial.

El primer intento noticiable de navegador fue el programa *Gopher* de la Universidad de Minnesota, aunque la interfaz de usuario más conocida a comienzos de los años noventa fue *Mosaic*, creado en 1993 por Marc Andreessen en la universidad de Illinois. Este sistema proporcionaba una navegación lenta y engorrosa, por lo que Andreessen decidió unirse a Jim Clark para elaborar, conjuntamente, una especie de *Mosaic* implementado que daría paso al arquetipo del acceso simplificado y, por primera vez, masivo a la Red. El programa para surcar las procelosas aguas que conforman la Web se denominó *Netsacape Navigator* y ya en 1996 era utilizado por más de seis millones de usuarios[263]. Su mayor facilidad de uso favoreció así que Internet saliera del ámbito académico y se convirtiera en un fenómeno global en todo el mundo. No está de más apuntar, que son los fabricantes de programas los que, en esta época, llevan la batuta en la conquista de la Red y que tanto *Netscape* como *Explorer* de Microsoft, las dos herramientas de navegación más populares en este período, se encargan de canalizar los accesos.

---

[263] TERCEIRO, J. B. (1996): *Op. cit.,* p. 107.

4.2.4 El despegue de la WWW. La entrada de empresas comerciales en la Red y la privatización del acceso

Llegamos a la Era de Internet propiamente dicha. En 1991, consciente de su importancia económica, el entonces vicepresidente de los Estados Unidos, Albert Gore, promueve dos normativas: la *Ley Sobre Computación de Alto Rendimiento* y un año más tarde la *Ley sobre Infraestructura y Tecnologías de la Información*. Gore, que tendrá un papel primordial en la promoción inicial de Internet, comienza a potenciar en el año 1993 lo que denomina como «superautopista de la información (SAI)» [264], vislumbrando las posibilidades futuras de la Red y, en general, de las tecnologías digitales. En ellas se encuentra, según Gore: «el mercado más importante y más lucrativo del s. xx» [265]; la superautopista mejoraría la calidad de vida de los ciudadanos y la competitividad de las empresas[266].

Durante los primeros años noventa se crea la Internet Society (ISOC) entidad sin ánimo de lucro que persigue el fomento y expansión de la Web a todos los sectores de la sociedad. Por su parte, la Fundación Nacional para la Ciencia continúa financiando Internet en los Estados Unidos, responsabilizándose con unos 11 millones de dólares anuales de los aspectos técnicos, gracias a un comité de expertos (*Internet Engineering Task Force,* IETF) designados a tal efecto. Sin embargo, tras la erradicación en 1990 de la obligación de contar con apoyo gubernamental para poder conectarse, las actividades comerciales adquieren un desarrollo inusitado, en un movimiento circular en el que a la vez que aumentan los usuarios de servicios privados, se encarecen los derechos de conexión.

Las demarcaciones privadas conviven, en un primer momento, con las establecidas previamente y el usuario puede elegir conectarse a través de universidades apoyadas por fondos públicos o a través de una firma comercial a la que abona una cuota. Entre las primeras redes restringidas con acceso por suscripción destacan: Compuserve,

---

[264] La terminología usada en los discursos de Gore no es arbitraria, sino que remite al sistema de carreteras interestatales que su padre promovió en los años 50. PARRA VALCARCE, D. y ÁLVAREZ MARCOS, J. (2004): p. 36.

[265] TREJO DELARBRE, R. (1996): *Op. cit.,* p. 64.

[266] CLINTON, W. J. y GORE, A. (1993): Technology for America's economic growth. A new direction to build economic strength, 22 de febrero de 1993.

Delphi, America on line, Spin o Prodigy, y el hecho de que prioricen el entretenimiento, los negocios o las compras impulsa su campo de acción en detrimento de las redes públicas.

Esta inclinación comercial de la Red provoca que la Fundación deje de financiarla dado que esta comienza a obtener sus fondos de las cuotas de las instituciones y empresas conectadas. Finalmente en 1995, cuando la Red ya superaba los cinco millones de navegantes conectados[267], se cierra la NSF dando paso a la gestión privada de Internet. Las redes espontáneas crecieron entonces juntas dando lugar a la verdadera Red de todas las redes, Internet, que se expandió rápidamente por todo el mundo. Tanto es así que, en los cinco años siguientes, el número de interactores pasó de 40 a 500 millones y el volumen económico de las transacciones se incrementó de 100 millones a 100.000[268].

4.2.5 **Internet ya es una realidad… y el control del usuario, también**

Vastas y misteriosas colecciones de datos
tejiendo impresionantes fortalezas,
ferozmente protegidas por las mayores multinacionales.
William Gibson, *Neuromancer*[269]

Este cambio en la gestión de la Red no es baladí, ya que veremos como muchas de las intromisiones en la intimidad y vida privada de los usuarios están íntimamente ligadas a la vertiente comercial de un entorno cuyas empresas obtienen beneficio al perfilar a los usuarios, explotando el valor monetario de sus datos. Todo ello, sin contar las intromisiones en la esfera privada llevadas a cabo por los diversos programas de espionaje y control ciudadano implementados por los gobiernos, problemática que no trataremos aquí por exceder los límites del presente análisis.

Para Manuel Castells, la idea primigenia que sustenta Internet representa el «paradigma de la libertad», fundamentado en dos elementos que aparecen impregnados en su esencia desde su creación, a saber: los condicionamientos tecnológicos y el hábitat institucional. Por

---

267 TERCEIRO, J. B. (1996): *Op. cit.,* p. 95.
268 PARRA VALCARCE, D. y ÁLVAREZ MARCOS, J. (2004): *Op. cit.,* p. 37.
269 GIBSON, W. (1984): *Op. cit.*

su substancialidad, la arquitectura de Internet es abierta, es decir, se basa en la conexión informática en red sin ningún tipo de restricciones. Sus creadores le dieron este diseño intencionalmente, por lo que cualquier intento de censura es interpretado por los protocolos como un fallo técnico que sortear dentro de la red global. En este sentido, la descentralización del universo Internet impedía su control. Y como resultado, la información personal de cualquier usuario estaba protegida no solo por el anonimato, sino por la dificultad para rastrear las fuentes e identificar el contenido de los mensajes transmitidos por medio de protocolos de Internet. Institucionalmente:

> Dado que inicialmente Internet se desarrolló en Estados Unidos bajo el amparo de la protección constitucional de la libertad de expresión y es en este país donde se encontraba, principalmente, el eje central de la Red, cualquier intento de limitación o prohibición a servidores de otros países podría eludirse usando servidores estadounidenses[270].

En los primeros años de su expansión mundial, la incapacidad para dominar el flujo de información que circulaba en la Red provocó el rechazo de los dignatarios de muchos países, puesto que su supervisión resultaba demasiado costosa. Internet se configuraba, a los ojos de todos, como una colección de nodos y redes imposible de controlar y en la que es difícil determinar qué elementos forman parte del sistema.

Si bien esta es la premisa motivo su aparición, su transposición al mundo real genera algunos conflictos. Por ejemplo, no existe un propietario de la Red en el sentido clásico, pero sí parcelas en las se intercalan la propiedad pública y la privada. En esta línea, Echevarría que, al igual que Albert Gore, usa con profusión la similitud entre Internet y las vías de comunicación terrestres, compara estos primeros pasos de Internet con una calle pública de *Telépolis*:

> En 1992 tenía más de medio millón de ordenadores conectados en más de cincuenta países del mundo, y era todavía una «calle sin peaje», al menos para centros educativos y organizaciones sin ánimo de lucro. […] Está gestionada por una sociedad, la Internet Society (IS) que se ocupa de ordenar la circulación de dicha telecalle, así como de «barrerla», «decorarla» y ampliarla con el fin de que puedan «pasear» por la calle un mayor número de peatones. Los habituales de Internet están

---

270 CASTELLS, M. (2001): *Op. cit.,* p. 193.

> muy orgullosos de su calle y suelen reunirse en Asambleas Generales para decidir sobre sus «normas de circulación». Numerosas empresas y organizaciones estatales utilizan dicha calle pero solo pueden votar los miembros individuales de la IS. […] Millares de «teleencuentros» entre personas se producen a diario, y, por supuesto muchísimos negocios. Pese a ello, todavía no ha surgido una policía para mantener el orden en Internet[271].

En esta traslación metafórica que es la ciudad imaginaria *Telépolis,* lo que circula es información. A grandes rasgos, y a pesar de una mayor contribución de algunas instituciones como universidades, esta urbe funciona sola y sin un control ni gobierno concreto, no siendo por ello una anarquía. No obstante, aunque su financiación entre 1985 y 1995 era casi completamente pública, bien a través de subsidios o a través de las propias instituciones académicas, poco a poco van surgiendo una suerte de cotos reservados en la Red, gestionados por empresas comerciales. Este hecho, recreado en la polis ideada por Echevarría, tiene su correlato en el entonces presente de la Red, en la que la privatización de la superautopista no supuso un hecho menor. Así, según afirma Raúl Trejo, la comparación de Gore no es exacta ya que la supercarretera de la información estaba siendo construida fundamentalmente por el sector privado[272]. Y a este respecto, la duda que aparece es: ¿Quién controla la Web? ¿Debe ser controlada?

Si bien la filosofía de la Red no se ha distanciado de su *dictum* inicial, en tanto que la libertad y la ausencia de un poder central son preceptos que se encuentran en su propia génesis, las motivaciones de las empresas que en la actualidad la gestionan difiere mucho de poder enarbolar este ideario primigenio; más aún, cuando el control de los datos adquiere un papel esencial. No en vano, afirma Lawrence Lessig, la transformación de esta libertad primitiva, así como la concepción y el respeto a la vida privada en Internet es consecuencia directa de su comercialización[273]. Un cambio fundamental que reside en las herramientas de recolección de datos, asociadas, en un primer momento, al comercio electrónico. Todo ello, derivará en un modelo eco-

---

271 ECHEVERRÍA, J. (1994): *Op. cit.,* pp. 58-59.

272 TREJO DELARBRE, R. (1996): *Op. cit.,* p. 67.

273 LESSIG, L. (2006): *Code and other laws of Cyberspace, Version 2.0*. New York: Basic Books.

nómico en el que el perfilado y la captación de potenciales clientes moverá cifras millonarias de manos de los anunciantes.

4.3 CARACTERÍSTICAS DEL UNIVERSO DIGITAL

La substancialidad de las TIC viene inexorablemente enlazada a la naturaleza del medio Internet y a la filosofía de la Sociedad de la Información. Encontramos, por ello, que una de las mayores dificultades que presenta el estudio de las tecnologías digitales proviene de la indefinición asociada a su naturaleza intangible, así como a su carácter trasgresor y global, que no comprende limitaciones de ningún tipo, salvo las técnicas en un momento dado. Las TIC, como herramientas que las personas usan para compartir, distribuir, reunir información y comunicarse entre sí por medio de dispositivos interconectados han creado un nuevo espacio social, ese «tercer entorno» en el que los seres humanos tienen la posibilidad de relacionarse e interactuar a distancia y en el que, por primera vez, el conocimiento es una fuerza productiva directa[274]. Se trata, en definitiva, de la emergencia de un nuevo espacio público, mediado y digital.

La inmaterialidad y la deslocalización definen, por tanto, el entorno digital. Sustentando el hecho paradójico de que mientras que Internet y las TIC han creado un espacio que no tiene especialidad o tiene una especialidad virtual, «es capaz de hospedar todo, tiene vocación de totalidad, lo que es importante y lo que no lo es»[275]. Para la antropóloga Paula Sibila, la carencia de espacio físico de Internet es capaz de realizar esos imposibles cuentos de Borges, como *El Aleph* o *El Jardín de los senderos que se bifurcan,* por cuanto el nuevo ecosistema no posee fronteras, distancias, ni está gestionado por una autoridad central:

> Es accesible a cualquier usuario bajo unas condiciones técnicas determinadas y con un cierto conocimiento previo. En cierto modo, «Inter-

---

274 ECHEVERRÍA, J. (1999): *Op. cit.*

275 Entrevista a Paula Sibila, en: MARTYNIUK, C. (2008): «Antes lo íntimo era secreto, ahora se lo hace público en Internet», en *Diario Clarín,* 21 de septiembre.

> net es la Biblioteca de Babel y el manejo de las tecnologías se constituye como la herramienta necesaria para llegar a ese conocimiento[276].

Todo señala que las tecnologías digitales han cambiado, en esencia, la concepción del espacio y el tiempo de la comunicación, creando un espacio deslocalizado o atópico al que todos tienen acceso y que «se ha convertido en la nueva esfera pública, aun cuando en él se desarrolla la comunicación interpersonal. Comunicativamente hablando, ha sustituido al espacio real»[277].

Este proceso posee su epicentro en la convergencia digital y la capacidad que otorga al usuario gracias a un valor diferencial respecto a las tecnologías precedentes: la interactividad, concepto clave de la Era Digital, como ya adelantara Nicholas Negroponte[278]. Ligado desde sus inicios al desarrollo de la informática, en un primer momento el concepto «interactividad» aludía a la comunicación entre individuo y computadora[279] y a la capacidad de estas de responder a los requerimientos de los usuarios. Posteriormente, la noción ha sido reelaborada desde otras perspectivas que aluden al vínculo mediado entre individuos, en referencia a su importancia en el proceso comunicativo. De hecho, pasar de la tecnología de transmisión a la interactividad como sistema fundamental de comunicación constituye un hito esencial a la hora de analizar la nueva comunicación y relación que se establece entre la tecnología digital y los usuarios. Es por ello que la innovación tecnológica que introducen las TIC no solo desencadena cambios esenciales en los procesos productivos, sino que propicia, igualmente, la renovación en los modos de comunicar.

La convergencia tecnológica, por su parte, se apunta como la causa más importante de la globalización que experimenta la sociedad contemporánea. Tanto el acceso a la información, como la estructura

---

276 Ídem.

277 CASTAÑARES, W. (2012): «Nuevos medios, nuevas sociedades. La investigación en comunicación hoy», en MIRNA, M.; SEPÚLVEDA, L. y GARZÓN, J. A. (ed.): *Convergencia digital y medios de comunicación*. Méjico: Universidad Autónoma de Nuevo León, p. 21

278 NEGROPONTE, N. (1995): *Op. cit.*

279 HOLTZ-BONNEAU, F. (1986): *La imagen y el ordenador.* Madrid: Fundesco, y MULTIGNER, G. (1994): «¿Sociedad interactiva o sociedad programada?», en *Apuntes de la sociedad interactiva. Autopistas inteligentes y negocios multimedia.* Cuenca: Fundesco.

de la comunicación han cambiado radicalmente, extendiendo el alcance de la Red a casi todo el mundo. En esta nueva era tecnológica, la potencialidad de las TIC y la convergencia digital sitúan la información, en forma de bits, como principal materia prima que, aunque necesita de soportes físicos para su tratamiento, posee una esencia inherentemente inmaterial. En este sentido, Luis Martínez Cabiedes señala la diferencia con las tecnologías anteriores:

> Probablemente, Internet sea la más importante revolución que ha acaecido a los medios de comunicación en su ya larga historia, una revolución aún mayor que la que supuso en su momento la televisión o la radio. Y es que esta vez no se trata de que haya aparecido un nuevo medio, un nuevo soporte, sino que esta vez ha desaparecido el soporte[280].

Resulta inevitable recordar aquí las palabras de Mauro Wolf a mediados de los noventa, quien aseveraba que la comunicación mediática tiende a satisfacer, cada vez más, la utopía de la comunicación sin tecnología[281].

Otra de las características de las tecnologías digitales proviene del proceso de «mediamorfosis», término acuñado por Roger Fidler en la década de los 80 y que constituye la antesala de la convergencia digital. Para el autor debe evitarse caer en el error de estudiar los medios de comunicación por separado, pues deben analizarse todas las formas como integrantes de un sistema independiente, advirtiendo las similitudes y relaciones que existen entre las formas del pasado, del presente y las emergentes:

> Los medios no surgen por generación espontánea, ni independientemente. Aparecen gradualmente por la metamorfosis de los medios antiguos. Y cuando emergen nuevas formas de medios de comunicación, las formas antiguas no mueren, sino que continúan evolucionando y adaptándose[282].

---

[280] M. CABIEDES, L. (2002): «Prólogo», en Estévez, J. (ed.) *Periodismo en la Red*, Madrid: Anaya, p. 13.

[281] Mauro Wolf citado por Wenceslao Castañares. CASTAÑARES, W. (2012): *Op. cit.,* p. 23.

[282] FIDLER, ROGER (1998): *Mediamorfosis. Comprender los nuevos medios.* Buenos Aires: Granica.

Si bien «desde la perspectiva del medio, los modos de comunicación tienden a tomar los códigos unos de otros»[283] la convergencia digital ha propiciado que todos los medios beban de una amalgama de códigos polivalentes. Autores como Terceiro indican, además, que esta convergencia tecnológica es la causa más importante de la homogenización que vive nuestra sociedad[284]. Por ello, las Tecnologías de la Información y la Comunicación, al igual que Internet, constituyen un nuevo paradigma, fruto de la convergencia del desarrollo de las redes de comunicación y de la consolidación del lenguaje digital como «un idioma universal entre máquinas y hombres»[285]. Un ecosistema propio que fomenta una mayor fusión y retroalimentación, convirtiendo a Internet, en palabras del discípulo de McLuhan, Derrick Kerckhove, «en el medio de comunicación por excelencia, el más exhaustivo, el más innovador y el más complejo de todos» [286] y, por extensión, a las TIC en herramientas de conocimiento ineludible en las sociedades modernas.

No es de extrañar, por tanto, la atracción e interés que despiertan las tecnologías, hecho que se potencia, según Dominique Wolton, debido a que representan el profundo movimiento de individualización de la sociedad: «son el símbolo de la libertad y la capacidad para organizar nuestro tiempo y espacio.[…] Tres palabras son esenciales para entender su éxito: autonomía, organización y velocidad». Las tecnologías digitales permiten que cada individuo pueda actuar sin intermediario y cuando quiera, «sin filtros ni jerarquías y, lo más importante, en tiempo real […] esto da un sentimiento de libertad absoluta, incluso de poder, de lo cual da cuenta la expresión navegar por la Red»[287]. Premisa que pondremos en duda debido al carácter mediado de las mismas y que nos habla de la existencia de un mando superior.

Como colofón, no está de más destacar que las Tecnologías de la Comunicación y la Información no son solo una realidad técnica. Las instituciones, las empresas y la sociedad en general, transforman la

---

283 CASTELLS, M. (1997): *Op. cit.,* p. 404.
284 TERCERIRO, J. B. y MATÍAS, G. (2001): *Op. cit.,* Madrid: Taurus, p. 79.
285 PARRA VALCARCE, D. y ÁLVAREZ MARCOS, J. (2004): *Op. cit.,* p. 10.
286 KERCKHOVE, D. (1999): *Inteligencias en conexión. Hacia una sociedad de la Web.* Barcelona: Gedisa, p. 19.
287 WOLTON, D. (2000): *Op. cit.,* p. 95.

tecnología al apropiarse de ella, modificándola y experimentando con ella, algo especialmente visible en el caso de Internet, al ser esta una tecnología de la comunicación. Por consiguiente, manifiesta Dominique Wolton: «las tecnologías no bastan para crear la comunicación […] hace falta además un proyecto y un modelo cultural»[288]. Razón sustantiva por la que Wolton nos invita a salir del determinismo tecnológico y comprender que la comunicación es la combinación de tres dimensiones: la tecnológica, la cultura y la social. Ello implica que, para abordar el estudio del universo digital en su globalidad, no podemos centrarnos exclusivamente en su vertiente técnica, sino en la humana; enfoque, el de la óptica del individuo, que guiará nuestro quehacer a lo largo de esta tesis.

5. LA WEB 2.0. EL CENTRO ES EL USUARIO

El siguiente hito que marcaría la revolución digital y en el que nos encontramos inmersos actualmente es la aparición de la Web 2.0, toda una filosofía que ha modificado la manera en que se generan y comparten los flujos informativos que estructuran la sociedad entera, silenciando, en parte, los arquetipos comunicativos tradicionales. Sus consecuencias, tangibles en todos y cada uno de los aspectos que conforman la existencia humana, son manifiestas no solo en la forma en que nos relacionamos, la manera en que nos presentarnos en el nuevo espacio público o cómo disfrutamos de nuestros momentos de retiro:

> La Web 2.0 es una actitud y no precisamente una tecnología. El cambio de la Web tradicional, que venimos utilizando hace años hasta la Web 2.0, visualiza un nuevo paradigma digital. Si bien es cierto que se basa en el mismo soporte digital y funciona bajo la misma estructura reticular *(networks)* este cambio se relaciona con la filosofía que soporta el uso de Internet [...] Esta responde a la interacción de diferentes procesos tanto de orden tecnológico, económico, cultural que, indudablemente influyen en el campo social[289].

---

[288] Ibídem, p. 146.

[289] COBO, J. C. (2005): *Arquitectura de la información y su impacto en la usabilidad de las tecnologías interactivas*. Tesis Doctoral. Facultad de Ciencias de la Comunicación de la UAB.

A lo largo de la corta narración que precede la aparición de Internet y la contextualiza una vez instaurada como medio de comunicación social, hemos hecho especial hincapié en la tecnología en sí, en los desarrollos creados desde las diversas instituciones académicas y laboratorios que entran en juego, así como en los medios y agentes que posibilitan y proporcionan acceso a la información. Dicho esquema nos dibuja un panorama casi lineal, en el que el *role* del ciudadano equivale al de receptor del proceso comunicativo tradicional, en tanto que poco o nada interviene en la creación del mensaje. Sí es cierto que puede generar información: entra en foros de discusión, crea páginas Web y las primeras bitácoras, añade comentarios… pero su capacidad de interacción es todavía bastante limitada y no puede compararse a la que emana del otro vértice del proceso comunicativo.

Con la llegada de la Web 2.0, este entramado muta significativamente. Se rompe, casi definitivamente, el tradicional modelo comunicativo lineal de Harold D. Laswell[290], gracias a que aumentan las posibilidades de interacción, un atributo principal que permite que las audiencias, otrora pasivas, se conviertan también en emisores y generadores de contenido. Supone así la transformación del esquema comunicativo conocido, que ya no parte de «unos pocos a muchos», sino «de muchos a muchos». El surgimiento de la Web 2.0 o Web social ha supuesto un antes y un después para el conjunto de la sociedad en prácticamente todas las esferas de la vida. Es pertinente remarcar, no obstante, que la expresión «casi definitivamente» no es arbitraria: Si bien es cierto que el individuo tiene unas herramientas como nunca ha conocido para lanzar mensajes y hacerse ver y oír en la opinión pública, las empresas que las gestionan siguen ostentando un mayor control de la información.

La expresión Web 2.0 se hizo popular tras la celebración en San Francisco, en octubre de 2004, de la Web Conference; un encuentro en el que autoridades del sector de las tecnologías y la industria se dieron cita para discutir las posibilidades de la Red como platafor-

---

290 LASWELL, H. D. (1948): «The structure and function of communication in society», en L. Bryson (ed.): *The communication of ideas*. Nueva York: Harper, pp. 37-51.

ma[291] destinada a la innovación empresarial. En dicha reunión, se intentó discernir qué factores habían propiciado que ciertas empresas consiguieran sobrevivir a la burbuja tecnológica, mientras otras habían sucumbido. Y la respuesta fue clara: la adaptación a una realidad comunicativa más interactiva y con más innovaciones, que refiere a Internet como entidad donde se dan cita todos los contenidos, tecnologías y aportaciones de los usuarios. Una vuelta a los principios fundacionales de la Red, por los que cualquier usuario y/o plataforma es capaz de ofrecer todo lo que se encuentra en el conjunto de la Web de manera gratuita.

Para Tim O'Reilly, a quien se atribuye la adopción del término Web 2.0[292], el estallido de la burbuja de las empresas «puntocom» constituiría el referente de partida de la transición a la nueva filosofía comunicativa. De hecho, en el prólogo de su artículo referencial: «What is the Web 2.0. Design Patterns and Busines Models for the Next Generation software», sitúa la caída del índice bursátil de los valores tecnológicos, Nasdaq, en otoño de 2001, como el inicio entre la transición a la Web social. Las compañías que habían sabido aprovechar el poder de la Web para explotar la inteligencia colectiva, habían realizado la evolución de la Web 1.0 a la 2.0, evitando así la bancarrota. Dicho planteamiento había permitido a la compañía Google capear el temporal sin problemas, saliendo incluso reforzada de la crisis tecnológica.

El término se popularizó rápidamente, aunque para referenciar su uso social y no meramente empresarial. A nadie se le escapa que este nuevo esquema devuelve la voz al usuario, razón por la que también se conoce como «Web social» y las herramientas informáticas sobre las que se construye «*software* social» [293], hecho que también nos da

---

[291] Entendiendo como plataforma: «un sistema técnico-comunicativo que impulsa la integración de diversos medios y servicios con capacidad de interactividad, navegación, hipertextualidad e hipermedialidad». CEBRIÁN HERREROS, M. (2005): *Información multimedia*. Madrid: Pearson.

[292] O'REILLY, T. (2005): «What is the Web 2.0. Design Patterns and Busines Models for the Next Generation software», en *www.oreilly.com*, 30 de septiembre de 2005. (Sin embargo, según el editor californiano, fue en realidad uno de sus colaboradores, Dale Dougherty, quien usó la voz por primera vez).

[293] Este término aparecía por primera vez en el artículo: DREXLER, E. (1991): «Hipertext Publishing and the evolution of Knowledge», en *Social intelligence*, vol. 1, n. 2, pp. 87-120.

una idea del optimismo que envuelve la emergencia de la nueva realidad comunicativa.

En el citado congreso, se enunciaron los siete principios constitutivos de las aplicaciones Web 2.0. Sin embargo, para evitar entrar en consideraciones técnicas, citaremos al respecto la explicación que el periodista Dan Gillmor, considerado el padre del periodismo participativo, ofrece en el prólogo de su libro *We The media*:

> En un primer momento las páginas Web eran estáticas, creadas por unos pocos y fundamentalmente diseñadas para ser leídas [...] La primera gran transición se produjo cuando la Web se convirtió en un sistema de lectura y escritura, un gran cambio que está todavía en progreso. La gran revolución en este ámbito, tuvo lugar con los *Weblogs*, los diarios personales y los wikis. Ahora la gente no solo podía crear sus propios sitios Web, sino que podía actualizarlos fácil y rápidamente. [...] La Web que está emergiendo es una en la que las máquinas hablan entre sí de la misma manera en que antes los humanos hablaban con las máquinas o entre ellos mismos[294].

La Web se abre así a las aplicaciones de los usuarios. Es, en definitiva, la «colonización» de la Red o democratización de la Web propiciada por una tecnología que permite comunicarse a un bajo coste. La comunicación entre particulares a través de los diferentes formatos síncronos y asíncronos que estructuran la malla tecnológica es más factible que nunca, posibilitando asimismo la creación de comunidades virtuales, la transferencia fácil y casi instantánea de contenidos multimedia y la creación de inmensos repositorios de datos[295].

Si la Red es el equivalente a un sistema operativo, en esta fase el interactor aprende a programarla, en tanto que cuenta con las herramientas para hacerlo[296]. De este modo, consultar la *Enciclopedia Británica* era algo propio de la Web 1.0, mientras que visitar la *Wikipedia*, página que redactan y corrigen los propios usuarios pertenece al universo 2.0. Dicho de otra manera:

---

294 GILLMOR, D. (2004): *We the media: Grassroots Journalism By the People, For the People*. Sebastopol, CA: O'Reilly.

295 KELSEY, S. ST., y AMANT, K. (ed.). (2008): *Handbook of Research on Computer-Mediated Communication*. IGI global, pp: 447-498, p. 448.

296 SHAYNE, B. y CHRIS, W. (2003): «We Media. How audiences are shaping the future of news and information», en *The media Center*.

> En este escenario en el que interactúan lo social (cómo y dónde nos comunicamos y relacionamos) y lo tecnológico (nuevas herramientas, sistemas, plataformas, aplicaciones y servicios) provocando cambios de lo unos sobre lo otro, surge una Web caracterizada por una Web de personas (Web 2.0) frente a una de datos (1.0)[297].

Esta eclosión participativa y socialización de la Red de redes subraya un matiz distintivo definitivo para romper con el esquema precedente: La Web 2.0 evoluciona y mejora a medida que más personas la usan y más contribuciones realizan, por ello, el verdadero corazón de la nueva estructura organizativa es «su capacidad de aprovechar la inteligencia colectiva»[298].

Por consiguiente, en el epicentro de todo este tejido está el individuo, que se consolida como el principal actor y protagonista de Internet. Tal y como apunta Ismael Nafría, se ha mutado de una etapa donde lo primordial eran los contenidos a un panorama donde el papel protagonista lo desempeña el sujeto:

> A lo largo de la breve historia de Internet ha habido diferentes «reyes» de la Web. En su día la frase «el contenido es el rey» fue la dominante. Se entendía en esa etapa previa al estallido de la burbuja puntocom que quien tuviera el contenido reinaría. […] La Web 2.0 sitúa al usuario en primera línea de la nueva generación de Internet[299].

La filosofía 2.0 integra dos elementos que marcan la diferencia frente a formatos anteriores: su arquitectura tecnológica y participativa. En este sentido, tal y como señala Sara Osuna[300], la Web se apoya en conceptos enunciados previamente por distintos autores que nos dan una idea del proceso de colectivización e intercambio del nuevo escenario virtual:

---

297 O'REILLY, T. (2005): *Op. cit.*

298 PISANI, F. y PIOTET, D. (2009): *La alquimia de las multitudes. Cómo la Web está cambiando el mundo*. Barcelona: Paidos ibérica.

299 NAFRÍA, I. (2007): *El usuario el nuevo rey de internet*. Barcelona: Gestión, pp. 117-120

300 OSUNA ACEBEDO, S. (2012): «Interantes e interactuados en la Web 2.0», en Aparici, R. (ed.) *Conectados en el ciberespacio*. Madrid: UNED, pp: 135-150, p. 143.

— La inteligencia colectiva de Pierre Lévy[301].

— Las multitudes inteligentes de Howard Rheingold[302] y la sabiduría de las multitudes de James Surowiecki[303].

— La interactividad de Tim Berners-Lee[304].

— La arquitectura de la participación de Tim O'Reily[305].

Esta socialización va a adquirir diversas formas que van desde las más simples como los *blogs*, hasta las marañas de redes sociales, pasando por la facilidad para acceder a contenidos surgidos de la agregación de significados procedentes de diversas fuentes. Esta última, conforma una parte inherente a la Web 2.0 que actúa como un vehículo para añadir significados a la existencia *online*. De esta manera la Red se convierte en un instrumento más útil, más social y cargada de más significados[306], de ahí que también se la denomine «Web semántica».

Poco a poco, esta filosofía comienza a inundar todas las esferas cotidianas, desde el plano personal e íntimo hasta el profesional o académico, entrelazándolos en un mismo espacio de acceso público. El impacto en la sociedad es innegable, solo hace falta echar un vistazo a nuestro alrededor para comprobar que todo parece estar impregnado de la esencia de la Web social, lo que nos lleva a hablar de «educación 2.0», «periodismo 2.0», «política 2.0»... No sorprende, por ende, que de la Web 2.0 se hayan hablado maravillas y se haya resaltado su importancia para impulsar la Sociedad del Conocimiento. Sin embargo también surgen autores que han alzado voces críticas respecto al nuevo entorno digital, analizando no solo los aspectos positivos sino los desafíos de este nuevo espacio mediado. Por ejem-

---

301 LÉVY, P. (2004): *Inteligencia colectiva por una antropología del ciberespacio*. Washington, DC: OMS.

302 RHEINGOLD, H. (2004): *Multitudes inteligentes. La próxima revolución social.* Barcelona: Icaria Editorial.

303 SUROWIECKI, J. (2004): *Cien mejor que uno: la sabiduría de la multitud o por qué la mayoría es siempre más inteligente que la minoría.* Barcelona: Urano.

304 BERNERS-LEE, T. (2008): *Op. cit.*

305 O'REILLY, T. (2005): *Op. cit.*

306 ZIMMER, M. (2007): «Privacy and surveillance in Web 2.0. A study in Contextual Integrity, and the emergence of "Netaveillance"». p. 2.

plo, aquellos individuos que no posean una formación adecuada para seguir el ritmo de adaptación o aprendizaje son susceptibles de quedar fuera de las bondades del nuevo espacio digital. Y, en la misma línea, uno de los mayores desafíos y que influye en la protección de la intimidad y vida privada es, como veremos, la falta de conocimiento y manejo de las herramientas informáticas, hecho que provoca una barrera entre «interactuantes» e «interactuados» en la Web 2.0[307].

Dentro de esta encrucijada 2.0, dos son los puntos esenciales: las redes sociales, que se han erigido como un elemento fundamental cuyas implicaciones se extienden de manera transversal en todos los aspectos de la sociedad, y el poder omnipresente de los buscadores, capaces de realizar una agregación de significados sin precedentes. En este trabajo nos centraremos en las primeras, dejando el análisis de Google y similares para futuras aportaciones al respecto.

6. LAS REDES SOCIALES

Para saber quiénes somos tenemos
que comprender cómo estamos conectados.
Ken Robinson

Las redes sociales son tal vez el mejor ejemplo de la filosofía bajo la que se creó Internet: poder descentralizado, conexiones… Tal y como menciona Manuel Castells en su *Galaxia Internet:*

> Una red es un conjunto de nodos interconectados. Las redes son formas muy antiguas de la actividad humana pero actualmente han cobrado nueva vida al convertirse en redes de información, impulsadas por Internet. Las redes tienen enormes ventajas como herramientas organizativas debido a su flexibilidad y adaptabilidad, características fundamentales para sobrevivir y prosperar en un entorno que cambia a toda velocidad[308].

Por ello, «Internet es una red por antonomasia. Es el embrión donde nacen y se asientan todas las redes sociales del mundo virtual. La nueva forma de comunicarse viene dada por el sitio obligado de paso para todo el mundo»[309]. Las redes sociales son elementos clave de la

---

[307] OSUNA ACEBEDO, S. (2012): *Op. cit.,* p. 143.
[308] CASTELLS, M. (2001): *La galaxia Internet.* Barcelona: Plaza & Janés Editores, p. 15.
[309] FLORES VIVAR, J. (2009): *Op. cit.,* p. 74.

cultura 2.0. entorno que también aglutina *blogs*, *wikis* y *chats*, aunque estas suponen un paso más allá.

Para abordar su estudio, revisaremos algunos de los informes emitidos por la AEPD, así como los trabajos clave de las sociólogas Danah Boyd y Nicole B. Ellison. Boyd es una prolífica investigadora en el campo de las redes que, actualmente, investiga en la universidad de California-Berkeley. Ellison, por su parte, desarrolla su actividad en el Departamento de Telecomunicaciones, Tecnologías de la Información y Medios de la Universidad Michigan State.

6.1 ANTECEDENTES Y FILOSOFÍA DE LAS ACTUALES REDES SOCIALES

Cuando mencionamos la expresión «red social», nuestro imaginario colectivo lo asocia automáticamente a la instantánea de cualquiera de las redes sociales digitales que pueblan Internet, particularmente, a la imagen de su exponente más popular: Facebook. Sin embargo, el origen de las redes sociales es mucho anterior, dado que se encuentran entrelazadas a la propia esencia de la persona. No en vano, al igual que el ser humano es, por naturaleza, un ser social[310], las actividades que desempeña lo largo de su existencia son eminentemente sociales. Este dato lo verificamos echando un vistazo a la propia evolución humana: desde la aparición del correo hasta la invención de la imprenta; en el desarrollo del comercio, en la creación y expansión de los medios de transporte; en la generación de medios de comunicación de masas… El contacto con otros individuos forma parte de nuestra naturaleza constitutiva, por lo que la evolución del sujeto ha caminado simultánea a la implementación de un conglomerado de marañas que le proveen de espacios de interacción interpersonal. Dichas formas de interacción social se definen fundamentalmente por:

> Los intercambios dinámicos entre los sujetos que las forman. Las redes son sistemas abiertos y horizontales y aglutinan a conjuntos de personas que se identifican con las mismas necesidades y problemáticas. Las redes, por tanto, se erigen como una forma de organización social

[310] El hombre es un ser social, un animal cívico, un *zôon politikón* (del griego *ζῷον, zôion,* «animal» y *πολιτικόν*, *politikón*, «político» «de la polis» o «cívico»). ARISTÓTELES (1999): *Política*. Madrid: Espasa Calpe.

> que permite a un grupo de personas potenciar sus recursos y contribuir a la resolución de problemas. […] pretenden organizar esas interacciones espontáneas con un cierto grado de formalidad, en el sentido de establecer intereses, problemáticas, preguntas y fines comunes[311].

En resumen, las acciones del ser humano son substancialmente sociales o, más concretamente: las actividades sociales son un atributo propio de la persona. Desde siempre, el individuo se ha sentido llamado a relacionarse con sus iguales y con su entorno, por lo que las redes sociales constituyen, en sí mismas, una manifestación propia de la naturaleza humana.

6.1.1 ¿Qué se entiende por red social?

Fundamentada en la *Teoría de grafos* del matemático Leonhar Euler, el ámbito de las ciencias sociales equipara «red social» a «estructuras sociales»[312], entendiendo estas organizaciones como: «un grupo de individuos que, de forma agrupada o individual, se relacionan con otros con un fin específico, caracterizado por la existencia de flujos de información»[313]. Estas corrientes de datos, elemento esencial en las sociedades modernas y atributo indisoluble de la propia substancialidad de la Sociedad de la Información, constituyen el carburante que hace funcionar dichas estructuras o «representación gráfica entre actores»[314].

Junto a estos flujos de información, los nodos o actores y los vínculos o relaciones son los tres pilares básicos que conforman las redes, constituyendo estos enlaces entre actores el ser mismo de las redes sociales[315]. De hecho, según afirma la *Teoría de redes*, los nodos compiten siempre por conexiones porque, en un mundo interconectado, el establecimiento y mantenimiento de los enlaces significa la

---

311 RIZO GARCÍA, M. (2003): «Redes. Una aproximación al concepto», en *Conaculta*, Universidad Autónoma de la Ciudad de México, p. 1. G.

312 GARCÍA ESTÉVEZ, N. (2012): *Op. cit.,* p. 35.

313 VELÁZQUEZ ÁLVAREZ, O. A. y AGUILAR GALLEGOS, N. (2005): *Manual introductoria al análisis de las redes sociales Medidas de Centralidad*. México DF: UAEM.

314 REQUENA SANTOS, F. (2003): «orígenes sociales del análisis de redes», en Requena Santos F. (ed.) *Análisis de redes sociales. Orígenes, teorías y aplicaciones*, Madrid: CIS, pp. 3-12.

315 MARTÍNEZ RAVANAL, V. (2004): *El trabajo en y con las redes*. Chile: Universidad de Chile, pp. 11-12.

supervivencia»[316]. En suma, las redes sociales son las personas y las relaciones que se establecen entre ellas, más que la infraestructura o soporte técnico sobre el que se dan los procesos comunicativos. La teoría de redes no parte, pues, de una utopía irrealizable, abstracta y ajena, sino de la propia naturaleza asociativa del ser humano.

Las raíces y gestación de dicho paradigma, afirma Noelia García Estévez, pueden encontrarse en diferentes disciplinas como la antropología, la economía, la psicología social o la estadística, entre otras. Destacan, a este respecto, autores como John Barnes[317] o Clyde Mitchel[318] desde el mundo de la antropología, o los sociólogos Simmel y Radclife-Brown[319]. Este último solicitaba en 1940, desde la sociología estructural, una ciencia concreta destinada a estudiar dichos circuitos de conexiones sociales.

Por su parte, el estudio de la mecánica y generación con que se desarrollan dichas relaciones esto es, las hipótesis que sustentan la pervivencia de las redes una vez creadas, así como el acceso que unos nodos tienen a otros del sistema, encuentra su origen en la *Teoría de los seis grados de separación,* que desgranaremos, brevemente, en el siguiente apartado.

6.1.2 Presupuestos teóricos sobre la formación de estas conexiones: La teoría de los seis grados de separación

Aunque en ciencias sociales la locución «redes sociales» se usa desde 1940, la base teórica que pretende dar respuesta a cómo se crean las conexiones en dichos tejidos se fundamenta en la *Teoría de los seis grados de separación*, inicialmente expuesta por el escritor húngaro Frigyes Karinthy quien afirmó, en 1929, que todas las personas del mundo estaban interconectadas entre sí. Concretamente, y

---

316 BARABÁSI, A.-L. (2002): *Linked: How everything is connected to everything else and what it means*, en New York: Plume, p. 106.

317 BARNES, J. A. (1954): «Class and Committees in a Norwegian Island Parish», en *Human Relations,* n. 7, pp. 39-58.

318 MITCHEL, J. C. (1969): *Social networks in urban situations.* Manchester: Manchester University Press.

319 RADCLIFE-BROWN, A. R. (1977): *Social Networks: a developing paradigm*. Nueva York: Academic Press., pp. 221-232.

según el enunciado inicial de Karinthy, cualquier persona del planeta estaría vinculada a cualquier otra a través de una cadena de eslabones de no más de cinco intermediarios, esto es, un total de seis pasos entre individuo e individuo. En esta red mundial, la cifra de contactos aumentaría a medida que lo hacen los eslabones de la cadena, por lo que los sujetos de primer grado serían los más próximos y, en consecuencia, según se avanza en el grado de separación, disminuiría tanto la relación como la confianza.

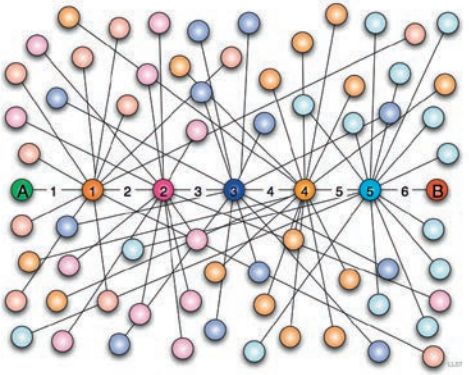

Figura 3.2 Teoría de los seis grados de separación[320]

La hipótesis de Karinthy, difícil de verificar en el terreno práctico, fue rescatada décadas más tarde por el psicólogo de la Universidad de Harvard, Stanley Milgram quien, en 1967, ideó una nueva manera de probar la teoría mediante un experimento que denominó: *El problema del pequeño mundo (Experimental Study of the Small World Problem)*[321]. Milgram resolvió seleccionar al azar varias personas del medio oeste estadounidense (concretamente, 160 granjeros de Omaha, un pueblecito de Nebraska) quienes debían hacer llegar un paquete a alguien de quien solo conocían su nombre, ocupación y localización aproximada. El destinatario en cuestión era un corredor de bolsa de Boston Massachusetts, es decir, se encontraba a cientos de kilómetros de distancia. Para llevar a cabo el experimento, cada granjero

---

[320] Fuente: LAURENS VAN LIESHOUT (2006): *Zes niveaus van shceiding*. Licencia GFDL.

[321] MILGRAM, S. (1967): «The Small World Problem», *Psychology Today*, Americam Sociological Association, vol. 1, n.1, mayo, pp. 61-67.

tendría que buscar un contacto directo y pedirle que siguiera la cadena, dándole el paquete a la persona que ellos conocieran directamente y que más posibilidades tuviera de conocer al corredor. Poco después, se comprobó que la mayoría de los envíos habían llegado en cinco o siete transacciones. Sin embargo, un dato relevante y que podría explicar el hecho es que el último grado, es decir, el círculo del corredor de bolsa era muy reducido y se ceñía exclusivamente a tres personas. A pesar de este condicionante y puesto que la entrega de cada fardo necesitó como promedio entre cinco y siete intermediarios, Milgram dio por aceptada la premisa de que cada persona está conectada a través de seis grados de separación con cualquier otra del mundo.

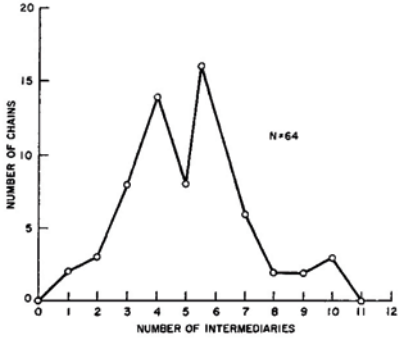

Figura 3.3 El mundo pequeño de Milgram[322]

Las dudas sobre los resultados obtenidos, especialmente ante la complejidad para demostrar dicha teoría sin elementos condicionantes que alterasen el resultado, fomentaron que, posteriormente, otros investigadores retomasen la senda iniciada por Milgram. Diez años más tarde, Pool y Kochen[323] revisaron los escritos del autor, pero sería en 1998 cuando Duncan Watts, sociólogo e investigador en Dinámica Social Humana de la Universidad de Columbia, lo repitiera. En esta ocasión, el ensayo se hizo a través del correo electrónico y, a diferencia del primer experimento, no se circunscribió exclusivamente a po-

---

322 MILGRAM, S. y TRAVERS, J. (1969): «An Experimental Study of the Small World Problem Stanley Milgram», en *Sociometry*, vol. 32, diciembre, n. 4, pp. 425-443.

323 DE SOLA POOL, I., y KOCHEN, M. (1978): «Contacs and influence», en *Social Networks,* n. 1, pp: 5-51, y KOCHEN, M. (1989): *The Small World,* Norwood, NJ: Ablex.

blaciones de Estados Unidos, sino que los participantes fueron escogidos al azar por todo el planeta. Tras observar que los resultados eran similares a los obtenidos por Milgram, Watts dictaminó que, efectivamente, era posible acceder a cualquier persona del planeta en tan solo seis eslabones, partiendo de una cadena de contactos directos[324]. De este modo, se atribuye a Watts la renombrada expresión «seis grados de separación», cuyo soporte teórico se encuentra, como veremos, en la base misma de parte del éxito de las redes sociales por Internet.

No obstante, aunque las aproximaciones al estudio de redes sociales ponen en claro que el mundo es una aldehuela en la que millones de usuarios aparecen interconectados en comunidad, su comprobación en todos los escenarios posibles resulta complicada. Tal vez por ello ha sido alabada y puesta en duda a partes iguales. Especialmente, porque dicha teoría nació para aplicarse a comunidades limitadas y no a un espacio abierto y sin límites como es Internet. Sin embargo, si sienta las bases de algunos de los principios que sustentan las redes sociales, explicando fenómenos como la influencia de los primeros grados, o cómo se contagian los comportamientos de los individuos. Así, gracias al estudio de redes y a esta teoría en concreto sabemos que una de las variables más importantes a tener en cuenta en el análisis de las herramientas sociales que habitan la Web es la proximidad e interconexión entre los individuos del universo digital[325].

6.2 LAS REDES SOCIALES DIGITALES

El todo es más que la suma de las partes
Axioma de La Gestalt

Reflejo del mundo físico, la sociabilidad innata a la naturaleza humana desde sus comienzos es también inherente a Internet. Y este es uno de los rasgos que convierte a la Red de redes en una de las

---

[324] Según Watts dicha red de contactos directos debe tener entre 100 y 200 personas. WATTS, D. J. (2004): *Six Degrees*: *The Science of a Connected Age* (Primera edición de 1971). New York: W. W. Norton & Company.

[325] ORIHUELA, J. L. (2005): «Apuntes sobre redes sociales», en el *blog ecuaderno,* 19 de julio 2005, en línea http://www.ecuaderno.com/2005/07/19/apuntes-sobre-redes-sociales/ [13/02/2013].

zonas indispensables, asevera Mayans, «para la construcción de la esfera pública contemporánea» [326]:

> El ciberespacio no es una red de ordenadores, sino el resultado de la conectividad social de los usuarios de los ordenadores conectados entre sí —desigualmente, eso sí— por todo el mundo. Por tanto el ciberespacio es sociedad y no puede ser otra cosa que sociedad [327].

En nuestro tiempo esta interconexión no es una realidad exclusiva de los espacios físicos, hecho diferencial que introducen las tecnologías digitales que, además, han dotado de un sentido global al concepto de intercomunicación, propiciando relaciones que no conocen fronteras.

> La universalidad que ofrece la Red permite ampliar el número de contactos y estrechar lazos de unión entre aquellos usuarios que tienen intereses comunes. Al centrarse en las relaciones de los individuos (o grupos de individuos) y no en las características de los mismos (raza, edad, ingresos, educación) se han utilizado para el estudio de hábitos, gustos y formas de relacionarse de los grupos sociales [328].

Las redes sociales se establecen, habitualmente, entre comunidades limitadas; pero al entrar en juego el ciberespacio nos topamos con la particularidad de que ahora deben operar en un entorno de alcance global. Esto, sumado al hecho de que los vínculos que se establecen se hallan altamente mediados, añade ciertos matices diferenciadores que influirán decisivamente en la protección de la intimidad y vida privada de los individuos. Empero, antes de entrar a analizar la cuestión, definamos claramente los atributos que acompañan a estas herramientas relacionales.

6.2.1 ¿Qué son las redes sociales digitales?

Tradicionalmente, se suele acudir al artículo referencial «Social Network Sites: Definition, History and Scholarship», escrito en 2007 por

---

326 MAYANS I PLANELLS, J. (2003): «El ciberespacio un nuevo espacio público para el desarrollo de la identidad local» conferencia inaugural del III Encuentro de Telecentros y redes de Telecentros. Peñafiel. Valladolid, octubre.

327 Ídem.

328 AEPD e INTECO (2009): *Op. cit.*

Danah Boyd y Nicolle Ellison, para abordar la caracterización de las redes sociales. En dicho texto se describen estas herramientas como:

> Servicios sustentados por la Web que permiten a los individuos (1) construir un perfil público o semipúblico dentro de un sistema delimitado, (2) articular una lista de usuarios con los que comparten una conexión y (3) ver y recorrer su lista de conexiones y aquellas hechas por otros dentro del sistema[329].

Aunque las diversas redes sociales disponibles en el universo digital presentan diferencias entre ellas, sí comparten una serie de parámetros comunes que rigen su dinámica: En primer lugar, los miembros de cada red construyen un perfil dentro de la plataforma que nutren de información personal. Esto les permite conectar ese perfil al de otros semejantes para crear una comunidad de contactos personal[330]. Igualmente, la generalidad de estos sitios permite al participante vincularse a otros enviando una petición de amistad que, previamente, debe ser autorizada por el mismo. Finalmente, tras unirse al servicio se les requiere a los nuevos usuarios proveer el sitio de información personal, incluyendo datos tales como el nombre, la edad o el correo electrónico, así como fotos y una descripción propia[331].

Dado que tras unirse a la red social los usuarios son susceptibles de ser identificados por otros participantes, se establecen entre ellos vínculos esenciales para el funcionamiento de la misma. El nombre con el que se reconocen estos contactos establecidos varía de una a otra plataforma: La terminología más popularmente usada es la de «amigos» como, por ejemplo, en Facebook, o «contactos», como en LinkedIn; servicios, todos ellos, que requieren confirmación de «amistad» bidireccional, esto es, por parte del que envía la invitación y el que la recibe. Además de las ya citadas, también se usan otras expresiones «fans» o «seguidores» en aquellas plataformas en las que la conexión no tiene por qué ser recíproca, como es el caso de Google+.

---

329 BOYD, D. y ELLISON, N. B. (2007): *Op. cit.*

330 LENHART, A. y MADDEN, M. (2007): «Teens, privacy & online social networks: how teens manage their online identities and personal information in the age of myspace», en *Pew Internet & American Life Project, Washington, DC,* p. 1.

331 Ídem.

Como vemos, la estructura primigenia de las redes sociales se sustenta en los perfiles visibles de los miembros del sistema en los que se muestran una lista de amigos que son, a su vez, integrantes de la comunidad. Además, «proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles» [332], por lo que las informaciones personales vertidas en los citados perfiles resultan cruciales para satisfacer el correcto funcionamiento y desarrollo de la red general. Recordemos que, según la *Teoría de redes*, la clave de la pervivencia y mantenimiento del sistema se encuentra en la capacidad para establecer enlaces, por lo que cuantos más nodos, esto es, a más usuarios activos, más factible será su éxito.

En consecuencia, lo importante son las conexiones o vínculos que se dan entre actores, por lo que más que una realidad técnica, la substancialidad misma de las redes sociales son las interacciones que se dan entre los sujetos, no las plataformas que las sustentan. De hecho, de las interacciones entre los individuos surgen propiedades que no pueden explicarse a partir de los elementos aislados. Para Fowler y Christakis: «Las redes pueden ayudar a que el conjunto de la humanidad sea muy superior a la suma de sus partes, y la intervención de nuevas formas de conexión parece fortalecer nuestro poder, para lograr aquello que la naturaleza nos tiene asignado» [333].

La popularidad que han alcanzado estas redes recala, según Boyd y Jenkins en «la habilidad del usuario para conversar con amigos, desarrollar una imagen personal en la Web, compartir ideas y otros ítems culturales digitales y articular las redes sociales de forma pública» [334]. Y es que además de crear y editar dichos perfiles, estas zonas semiacotadas de la Web pueden resultar muy atractivas por cuanto posibilitan que los integrantes puedan compartir fotos y vídeos, acceder a la información publicada en los perfiles de otros miembros y buscar «amigos» u otros contactos como conocidos o, incluso, personajes famosos. No en vano, aunque el objetivo primario de las redes sociales es comunicarse con individuos que ya forman

---

[332] AEPD e INTECO (2009): *Op. cit.*

[333] FOWLER, J. y CHRISTAKIS, N. (2010): *Conectados*. Madrid: Taurus, p. 294.

[334] BOYD, D. y JENKINS, H. (2006): «MySpace and Deleting Online Predators Act (DOPA)», MIT Tech Talks. Disponible en: http://www.danah.org/ papers/ MySpaceDOPA.html [29/01/2010].

parte integrante del círculo social del individuo, también permiten articular una serie de contactos más superfluos, con personas a las que no se podría acceder de otro modo; gente desconocida con la que, sin embargo, se comparten intereses comunes. No obstante, el objetivo primordial es articular una serie de contactos de una u otra manera explícitos, que sean capaces de estructurar y sustentar la red[335].

Igualmente, algunas plataformas como Facebook permiten añadir módulos denominados «aplicaciones» para mejorar las prestaciones, por lo que la participación está asegurada desde el momento en que cada participante puede comentar las páginas de otros e introducirse en grupos y comunidades virtuales. Dichos servicios resultan además muy cómodos, ya que permiten centralizar muchas de las gestiones que el interactor realiza en la Red general, pues integran servicios como la mensajería instantánea, entre otros. De este modo, a medida que las redes sociales se asientan, los sujetos comienzan a dedicarles exponencialmente más tiempo en relación con otros servicios tradicionales como los correos electrónicos[336].

Con todo lo expuesto, no resulta extraño que Duncan Watts considere las redes sociales como «cibermundos que merece la pena analizar»[337]. Para Watts las tecnologías que sustentan las nuevas redes sociales no solo revolucionan la sociedad, sino que permiten aprender sobre el propio ser humano gracias a su observación y al estudio de cómo estas comunidades se transforman y evolucionan con el tiempo.

6.2.1.1 *Tipología de las redes sociales digitales*

Según se detalla en el informe *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line*, realizado por la Agencia Española de Protección de Datos (AEPD) y

---

335 HAYTHORNTHWAITE, C. (2005): «Social networks and Internet connectivity effects», en *Information, Communication & Society*, vol. 8, n. 2, pp. 125-147, p. 135.

336 NIELSEN COMPANY (2010): *Estudio Nielsen Online*. Citado en GARCÍA ESTÉVEZ, N. (2012): *Op. cit.,* p. 42.

337 Watts citado en FLORES VIVAR, J. (2009): *Op. cit.,* p. 80.

el Instituto Nacional de Tecnologías de la Comunicación (INTECO)[338] encontramos los siguientes tipos de redes sociales:

— Generalistas o de ocio: Facebook, Google+ y su antecedente Google Buzz.

— De intercambio de contenidos e información: YouTube, Instagram, Pinterest.

— Basadas en perfiles: Facebook, Tuenti, Orkut.

— Las de servicio profesional: LinkedIn o Xing.

Existen, además, las denominadas «redes de *microblogging*» o «*nanoblogging*» como Twitter, aplicaciones que no llegan a ser consideradas redes sociales sino herramientas o plataformas de comunicación[339]. Sin embargo, si bien es cierto que no se trata de redes al uso, sí es posible crear dichas aplicaciones a partir de estas herramientas.

Cruzando las redes de ocio con las de perfiles encontramos no solo aquellas más usadas en Internet, sino las que son susceptibles de alimentar más intromisiones. En la actualidad, dentro de las redes sociales, las más populares en cuanto a número de usuarios son Facebook y LinkedIn, seguidas a mayor distancia por Google+[340]. El camino a esta popularidad, no osbtante, ha estado sembrado de intentos que, como veremos a continuación, no siempre llegaron a buen puerto.

6.2.2 Origen y evolución: de las comunidades virtuales a las redes sociales digitales

Aunque las redes sociales digitales comenzaron a popularizarse gracias al desarrollo y expansión de la Web 2.0, el concepto de red social mediada no es nuevo, sino que se encuentra en el germen mismo del ideario inicial que sustentó la creación de Internet: Conexiones entre nodos en una red descentralizada e imposible de controlar, transmisión

---

338 AEPD e INTECO (2009): *Op. cit.,* p. 45-50.

339 Así lo afirmaba su propio director ejecutivo, Jack Dorsey, en la entrevista: MUÑOZ, R. y RIVIERO, A. (2009): «Twitter no es una red social sino una herramienta de comunicación», en *El País*, 30 mayo de 2009.

340 WASSERMAN, T. (2012): «Pinterest is now the no. 3 social network in the U.S», *Mashable.com*, 6 de abril, disponible en: http://mashable.com/2012/04/06/ pinterest-number-3-social-network/ [26/09/2012].

de datos ininterrumpida gracias a la multiplicación de vínculos, aumento de las conexiones entre vínculos para asegurar el buen funcionamiento del sistema… estos principios básicos en la Red de redes se reproducen, a menor escala, en las comunidades virtuales. De hecho, si nos retrotraemos unas décadas, encontramos un precedente de Facebook concebido por las mismas mentes pensantes que sustentaron los pilares de la Web (antes incluso de la creación de Arpa-Net). En un ensayo de 1968 titulado *El ordenador como mecanismo de comunicación* (*The computer as Communication Device*)[341], Licklider y Taylor ya se preguntaban cómo serían las comunidades virtuales por ordenador. Estas se constituirían, en la mayoría de los casos, por una serie de miembros separados geográficamente y con posibilidad de actuar tanto individualmente como agrupados en nodos. El resultado es que ya no sería necesario enviar una carta o un telegrama, «simplemente se identificará a las personas cuyos archivos deberían estar conectados a los tuyos»[342].

El primer intento de crear una comunidad virtual al uso y con un número importante de usuarios se produjo en 1979 con la creación de Usenet, un espacio que permitía dejar mensajes a grupos de usuarios catalogados en función de un determinado tema. Usenet, abreviatura de «Red de Usuarios» (Users Network) fue creado por Tom Truscott y Jim Ellis, estudiantes de la Universidad de Duke. Gracias a este sistema los integrantes de la comunidad podían leer o enviar mensajes, denominados «artículos», a distintos grupos de noticias seccionados de forma jerárquica. Empezó a funcionar en 1980 y, originalmente, fue concebida como «un Arpa-Net para gente sin recursos». A pesar de su antigüedad, hoy en día sigue funcionando.

Posteriormente, en 1985, los investigadores Larry Brilliant y Stewart Brand crearon un tablón de anuncios electrónicos llamado *The Whole EarthLectronic Link*, conocido también como «*The WELL*»[343]. Tras sus experiencias en dicho foro, uno de los primeros

---

[341] LICKLIDER, J. C. R. y TAYLOR ROBERT, W. (1968): «The computer as Communication Device», en *Science and Technology,* abril. Taylor fue una pieza clave del desarrollo de la Advance Research Projects Agency del Departamento de Defensa, Arpa-Net, embrión de la actual Internet.

[342] Ídem.

[343] Juego de palabras entre su acrónimo «WELL» y la expresión «muro» en inglés «*wall*», que posteriormente se retomará en otras redes sociales como Facebook. www.thewell.com

participantes, Howard Rheingold, publicó un ensayo en el que definía la substancialidad de una comunidad virtual: «un grupo de gente que puede encontrarse o no cara a cara y que intercambia textos e ideas mediante el tablón de anuncios y las redes informáticas»[344].

Sin embargo, no será hasta el año 1995 cuando comenzaría a hablarse propiamente de redes sociales digitales tal y como las conocemos ahora. En este año, Randy Conrads crea classmates.com, un sitio Web destinado a que los estudiantes inscritos pudieran recuperar y mantener el contacto con antiguos compañeros del colegio, instituto o universidad, un concepto que ya nos es más familiar. Así, solo dos años después de que Internet empezase a desplegarse entre la gente corriente, dio comienzo oficialmente la era de las redes sociales.

Para los sociólogos Danah Boyd y Nicole Ellison, sería la aparición de Sixdegrees, en el año 1997, el acontecimiento que marcaría el verdadero comienzo de las actuales redes sociales[345]. Este servicio que contenía aspectos verdaderamente novedosos para la época, comenzó «identificando y cartografiando relaciones reales, entre personas reales y que usaban su nombre real»[346], lo que la convirtió en una red altamente exitosa. De este modo, la clave de su éxito fue solicitar que el perfil se completase con la verdadera identidad de cada participante para que otros miembros del sistema pudieran identificarle fácilmente, algo que los usuarios aceptaron sin problema. Sin embargo, no se podían añadir fotos; en ese momento resultaba muy costoso y la velocidad de conexión era muy lenta. Es más, el nivel de desarrollo técnico de la época en que se fraguó la idea provocó que el sistema no siguiera aumentando y, como sabemos, para que el negocio de las redes sociales sea factible y rentable debe alcanzar una masa crítica de participantes. Además el error de Sixdegrees fue establecer restricciones respecto a los contactos no directos: los integrantes debían entrar por invitación por lo que, a pesar de que los ya miembros podían mandar invitaciones a sus contactos, la red crecía lentamente. Por dicho motivo y a pesar de que

---

344 RHEINGOLD, H. (2008): *Op. cit.*

345 BOYD, D. y ELLISON, N. B. (2007): *Op. cit.*

346 KIRKPATRICK, D. (2011): El efecto Facebook: la verdadera historia de la empresa que está conectando el mundo. Barcelona: Planeta, p. 85.

en 1999 los habitantes de Sixdegrees ya sumaban los 3,5 millones[347], la empresa resolvió cerrar el servicio en el año 2000.

Empero, la semilla había dado su fruto y el propio creador de Sixdegrees, Andrew Weinreich, se refería a otras redes como la suya como «el sistema operativo del futuro»[348]. Y no se equivocaba, la fiebre se extendió a Silicon Valley y San Francisco entre los años 2001 y 2002. En estas fechas, tanto desde los foros universitarios, como en la industria comienza a hablarse de páginas Web que permiten crear mallas de círculos de amigos a través de Internet. En marzo de 2003, se sienta otro precedente con la aparición de Friendster, basada en la estructura de Sixdegrees, aunque siguiendo un modelo de redes en círculos. Además, añadía la posibilidad de enlazar foto a los nombres de los usuarios, lo que la hacía mucho más atractiva. No obstante, aun cuando obtuvo gran éxito y alcanzó un buen número de usuarios, de nuevo los elevados costes asociados a su mantenimiento, sumado a las restricciones técnicas[349] actuaron en detrimento de su crecimiento posterior.

También en 2003, comienzan a aparecer sitios Web que posteriormente adquirirán gran popularidad. Tal es el caso de MySpace, que rápidamente se abre mercado entre los adolescentes estadounidenses y de las redes profesionales LinkedIn y Xing. El éxito de MySpace en Estados Unidos hizo que el producto rápidamente desbordase las fronteras ya que, a diferencia de otras redes de ocio, en esta no se necesitaba invitación para ser miembro. Creada por Tom Anderson, la plataforma permitía compartir contenido audiovisual y dejar comentarios, así como conocer detalles privados de otras personas, entre otros, su orientación sexual o creencias. Sus múltiples opciones de personalización atrajeron rápidamente al usuario, por lo que, cuando en enero 2004 se pusieron en marcha Facebook y Orkut.com, MySpace ya tenía más de un millón de miembros y se había convertido rápidamente en la red social dominante en Estados Unidos.

A partir de ese momento, la popularidad de estas plataformas creció exponencialmente. Numerosas empresas y multinacionales de Internet

---

347 Ibídem, p. 87.

348 Ídem.

349 BOYD, D. (2006): «Friendster lost steam. Is myspace just a fad?», en *Apophenia Blog*, 21 de marzo de 2006. disponible en http://www.danah.org/papers/FriendsterMySpaceEssay.html.

abanderaron proyectos en el entorno de las redes sociales, entre las que destacaban la citada Orkut[350] gestionada por Google o Yahoo!360°, controlada por dicha compañía. A esto, se une la creación de otras muchas redes sociales, ora de de carácter específico, ora dedicadas a sectores concretos. Sin embargo, para hablar de revolución en la concepción de las redes sociales tenemos que esperar a la aparición, en 2004, de Facebook, considera red social *par excellance* y que marca el año cero de las herramientas relacionales a través de la Web. Dos años más tarde se crea Tuenti, destinada en un primer momento al público universitario y adolescente pero que, ulteriormente, se extendió al resto de la población siendo incluso capaz de competir con Facebook. Y aunque reseñaremos también el nacimiento de Twitter en 2006, como ya hemos indicado, técnicamente no se trata de una red social, sino de un servicio de *microblogging* o *nanoblogging*. Lo mismo sucede con portales como Youtube o Flirck que, a pesar de que comparten algunas funcionalidades, no pueden ser consideradas redes sociales por cuanto «su razón no es propiamente propiciar el contacto e interacción entre usuarios»[351].

En 2006, la red social MySpace alcanzaba la nada desdeñable cifra de 110 millones de perfiles[352], aunque es el año 2007 el que marca la eclosión de las redes en todo el planeta. A partir de este momento y gracias a la enorme cantidad de mejoras técnicas desarrolladas en tan solo un par de años, estas comunidades se propagan mundialmente. Ya en 2008, estudios de medición y análisis del tráfico en Internet informan de que dentro de los 500 sitios Web más visitados del mundo se encuentran al menos cinco redes sociales. Concretamente: Facebook, MySpace, Hi5 y Orkut se emplazan entre las veinte primeras posiciones[353]. Y según un estudio elaborado por *Pew Internet and American Life Project* publicado en enero de 2010: «la participación de los adultos usuarios de Internet que tienen un perfil en las redes

---

350 Orkut.com, una red social con buen diseño y sofisticada alimentó, en un primer momento, grandes expectativas. pero posteriormente se fue centrando en usuarios de ciertos países como Brasil o la India, donde continuó activa hasta finales de 2014.

351 GARCÍA ESTÉVEZ, N. (2012): *Op. cit.*, p. 25.

352 ANDREWS, M. (2006): «Decoding Myspace», en *U. S. News and World Report*, 18 de septiembre de 2006.

353 Alexa Internet http://www.alexa.com/site/ds/top_sites?ts_mode= global&lang=none.

sociales en línea se cuadruplica desde el 8% en 2005 hasta el 35% en 2009» [354].

Paralelamente a la expansión de las herramientas relacionales de la Web 2.0, la expansión es de Facebook es imparable y a partir de 2011, con 750 millones de usuarios en activo, se consolida como la líder indiscutible de las redes sociales de carácter generalista [355].

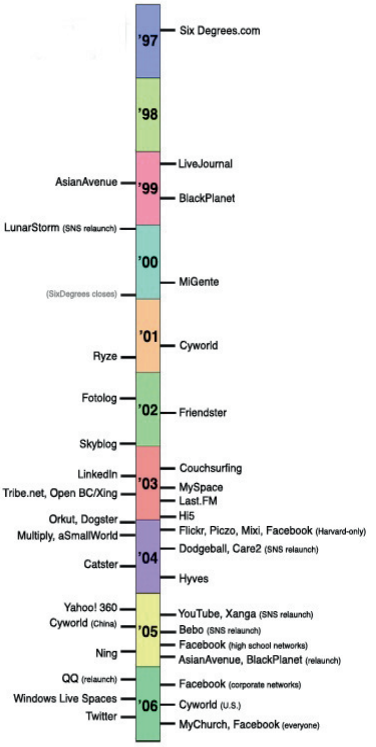

Figura 3.4 Lanzamientos de las principales redes sociales, según Boyd y Ellison 2007 [356]

---

354 LENHART, A., PURCELL, K., SMITH, A. y ZICKUHR, K. (2010): «Social media and young adults», en *Pew Internet and American Life Project*, Washington, DC.

355 Estadísticas del sitio Web: *Facebook statistics*. http://www.socialbakers.com/statistics/facebook/

356 BOYD, D. y ELLISON, N. B. (2007): *Op. cit.*, A este esquema habría que añadirle las incursiones posteriores de Google en las redes sociales (Google

7. LA VULNERACIÓN DE LA INTIMIDAD Y LA VIDA PRIVADA EN LA WEB 2.0

> Se engañaría quien pensara que la nueva ciudad
> es una panacea desde el punto de vista ético-político,
> pero también quien asegurara que es una maldición
> Javier Echevarría, *Telépolis*[357]

El tráfico de datos privados en los entornos mediados no es algo nuevo, ni exclusivo de nuestro presente más inmediato: ya era *vox populi* en los noventa. Si bien, un matiz marca la diferencia en nuestros días: se ha incrementado su frecuencia y la multiplicidad de agentes implicados. Todo ello gracias no solo a la cantidad de aplicaciones proporcionadas por la Web semántica, sino por el consecuente cambio en el modelo comunicativo que propicia un *role* más activo del usuario. En suma, cualquiera de los peligros que viésemos en esos años precedentes se ha visto magnificado gracias a la habilidad que proporcionan las herramientas de la Web 2.0 para la obtención, reproducción, correlación, agregación y etiquetado de los contenidos; un ágape de datos que, para colmo, están disponibles para todo aquel que desee consultarlos y emplearlos. Por ende, esta tecnología permite seguir la pista de la vida entera de cualquier persona con precisión y de manera instantánea; y esta capacidad ya no está solo en manos de las empresas de Internet o de los gobiernos con potencial tecnológico suficiente, sino de cualquier persona con independencia de sus intenciones. Este aumento de vulnerabilidad del usuario aparece enlazado a servicios con nombres y apellidos que crean puntos ciegos en las estrategias que los propios individuos desempeñan para proteger sus informaciones. En concreto, las redes sociales y los flujos de intercambio de datos que estas alimentan marcan la constante, especialmente cuando sus interacciones se relacionan con otros servicios como el buscador Google.

Antes de la llegada de la Web 2.0 las tecnologías digitales ya presentaban un terreno propicio para la vulneración de la dimensión reservada del ser humano. Los dos principales desafíos provenían, entonces, de dos poderosos frentes: de las empresas de Internet cuya

---

Buzz, Google +...) así como la red social Xing y la española Twenti que no aparecen citadas.

[357] ECHEVERRÍA, J. (1994): *Op. cit.,* p. 156.

búsqueda de beneficios les llevaba a hacer un seguimiento pormenorizado de los hábitos, gustos y otras peculiaridades de sus clientes, para personalizar la publicidad ofrecida y los servicios de terceras empresas[358]. Y en segundo lugar, de las bases de datos estatales mediante las cuales los gobiernos eran —y son— capaces de reunir cantidades ingentes de datos personales en sus propios servidores[359].

Es necesario sumar, a todo ello, las denominadas prácticas de «vigilancia pública» respaldadas por legislaciones laxas en el respeto a la intimidad de los individuos y que surgen en contextos histórico-políticos marcados por una carencia en la seguridad del Estado. A este respecto, las restricciones acaecidas tras los atentados del 11 de septiembre en Nueva York constituyen un punto de inflexión, en tanto que alentaron una serie de cambios normativos y mecanismos centrados en la monitorización pública, por los que el ciudadano se veía impelido a ceder en su anonimato en aras de una mayor protección nacional. En este sentido, coincidimos con Dan Gillmor quien, en su libro *We the media,* sitúa la fecha de los atentados a las Torres Gemelas como el origen de un nuevo contexto marcado no solo por la utilización masiva de las tecnologías del control, sino por un mayor uso de las herramientas de Internet por parte de los ciudadanos, para difundir y obtener información ante la incertidumbre[360]. Podemos admitir, a este tenor, que «renunciar a la intimidad en las compras por Internet parece benigno. Renunciar a ella en los vuelos puede parecer razonable; incluso pueden no ser problemáticos los circuitos cerrados de televisión que operan en lugares públicos». Sin embargo, advierte Deborah Johnson, el problema lo encontramos cuando «todo se suma, nos encontramos con que no tenemos ninguna vida privada en absoluto» [361].

En este sentido, los trabajos de Mason, aunque producidos en los años ochenta del siglo pasado, parecen no haber perdido vigencia.

---

358 Manuel Castells advertía hace años que el 92% de los sitios Web de Estados Unidos se dedicaban a recoger datos de los usuarios y los procesaban según sus intereses comerciales. CASTELLS, M. (2001): *Op. cit.,* p. 224.

359 GARTON, T. (2010): «Facebook: restablecer la privacidad», en *El País*, 11 de octubre de 2010. Disponible en: http//elpais.com/diario/2010/10/11/ opinion/12867 48 -011_ 850215.html. [04/03/2012]

360 GILLMOR, D. (2004): *Op. cit.,* p. 30.

361 JOHNSON, D. (2009): *Op. cit.,* p. 193.

Como dato curioso, cuando en 1986 el autor describió dos de los peligros más flagrantes para la integridad privada del sujeto se refería, de un lado, al avance de la tecnología de la información y su habilidad cada vez mayor para capturar, computar y comunicar datos; y de otro, al valor que podría adquirir estos contenidos para aquellos con la capacidad de usarla en beneficio propio. Sin saberlo, Mason delineaba las claves que se ocultan tras las intromisiones perpetradas en el universo Internet que dibuja la filosofía 2.0.

En el panorama actual, dichas intrusiones en nuestra intimidad y vida privada han aumentado, a la vez que nos topamos con nuevos desafíos. Las parcelas de la Web 2.0 están construidas sobre una base de datos no ya tan desestructurada como sucedía anteriormente. En sus confines, el interactor no solo utiliza Internet para mandar correos, consultar páginas, charlar o realizar compras; sino que produce contenidos y da visibilidad a ciertas informaciones a su antojo. Sin embargo, los contenidos mayoritariamente volcados por los usuarios 2.0 corresponden a información propia, relativa a su estado personal, emociones, sentimientos o actividades de su vida cotidiana, fotografías, situación geográfica… acciones que tienen por objeto que su red de contactos los conozcan, pero que, a la postre, convierten la Web 2.0 en la caja de resonancia de lo privado.

De manera paralela a esta divulgación abierta de información, resulta relativamente sencillo encontrar datos sobre iguales: muchos de los perfiles son públicos por defecto, las políticas de privacidad cambian sin aviso previo y servicios como los denominados «agregadores de datos» facilitan el trabajo de la recogida y cruce de informaciones. De este modo, una vez que se conoce el nombre de usuario o alias de una persona para un servicio concreto, se abre un número infinito de posibles combinaciones, esto es, de posibilidades de encontrar información a través de una amplia variedad de plataformas de la Web 2.0. Todo ello, aumentado por los poderosos motores de búsqueda como Google que hacen que cualquier individuo pueda perfilar a otro usuario («*amateur data mining*») buscando, rastreando y agregando detalles a la vida de cada persona, desde varios servicios de la Web. Así, un sujeto que acumule el conocimiento y las destrezas digitales pertinentes para acceder a los datos de otros y triangularlos, puede ser capaz de descifrar tanto las identidades reales que se esconden tras sus *nicks,* como un amplio abanico de informaciones personales capaz de detallar a la perfección la vida diaria

de cualquier persona. Es por ello, que muchos de los miembros de estas plataformas 2.0 asumen que tienen pocas expectativas de mantener su información privada a salvo.

No resulta sorprendente, por todo lo anteriormente expuesto, que la Red proporcione un escenario proclive al cobijo de delitos como la suplantación de identidad, el robo de datos o la erosión del derecho a la propia imagen, al honor y, cómo no, a la protección de la vida privada, entre otros muchos. A este respecto, la facilidad que proporcionan las tecnologías para acceder a estos datos encuentra un aliado en la falta de información que lastra las acciones que el sujeto emprende en Internet, en tanto que no comprende cuestiones clave como qué contenidos serán recopilados o qué tratamiento se les dará. Lo más controvertido, no obstante, es que dicho flujo de datos personales vuelve tremendamente inerme al usuario, puesto que su sustracción se produce sin apenas conocimiento, algo que parece haberse instaurado como la norma seguida por la generalidad de los agentes que operan en la Red. Y, a tenor del escrutinio realizado, esta situación no parece mejorar transcurrido el tiempo pertinente de implantación de las redes sociales, sino que se mantiene en el tiempo, toda vez que sus prácticas no merman el poder de atracción que ejercen en el usuario. Tan es así, que lejos de menguar, este festín de ideas, visiones y sentimientos personales se retroalimenta a medida que pueden ser accedidos desde más dispositivos, aumentando la capacidad de capturar texto, imágenes, vídeo o la combinación de los tres y ser publicada directamente en la red social para el consumo de la comunidad.

En consecuencia, el uso de las aplicaciones de la Web social ha aumentado exponencialmente las preocupaciones de los eruditos respecto a la complejidad que conlleva salvaguardar nuestra vida privada en este entorno difuso. Así, en el marco del *Proyecto Ética*[362], financiado por la Unión Europea para valorar la incidencia de una serie de dilemas éticos ante la aparición de las tecnologías digitales, se

---

[362] Fuente: Comisión Europea (2012): *EU FP7 ETICA project: Ethical Issues of Emerging ICT Applications*. Proyecto desarrollado dentro del 7.º Programa Marco, de abril de 2009 a mayo de 2011. Más información en: www.etica-project.eu.

observó cómo los asuntos relativos a la intimidad y vida privada habían aumentado de manera exponencial en los últimos años.

Figura 3.5 Análisis bibliométrico de los principales dilemas observados en relación a la aparición de las TIC en la sociedad[363]

Es palpable, del mismo modo, que la tensión entre el deseo de disfrutar de las capacidades que ofrece Internet y la preocupación por los peligros que esto puede acarrear genera un profundo impacto no solo en el individuo, sino que repercute en la sociedad entera, en la política e, incluso, en la propia industria. No hace falta más que observar cómo, en los últimos años, locuciones como «política de Internet» o «derechos del usuario» han comenzado a poblar los escritos científicos, al igual que, paralelamente, se han convertido en expresiones recurrentes en el discurso sociopolítico, con un efecto, eso sí, más estético que efectivo.

---

[363] Fuente: Comisión Europea (2012): *EU FP7 ETICA project: Ethical Issues of Emerging ICT Applications*. Proyecto desarrollado dentro del 7.º Programa Marco, de abril de 2009 a mayo de 2011. Más información en: www.etica-project.eu.

8. REFLEXIONES SOBRE EL CAPÍTULO

Siguiendo la tónica iniciada en el capítulo anterior, hemos realizado la demarcación conceptual que corresponde al abanico de términos referentes al entorno digital con los que operaremos a lo largo y ancho de las páginas de este trabajo. Nos serviremos, primordialmente, de las voces «Web 2.0», «Web semántica o relacional» y «Web social» por ser estas las que mejor delimitan el continente en el que se desarrolla el fenómeno a analizar. No obviaremos, sin embargo, otros referentes como «Tecnologías de la Información y la Comunicación» si queremos hacer hincapié en las herramientas en sí, o «Red» e «Internet» cuando nos refiramos al canal o medio en el que se desarrolla el fenómeno. Esta delimitación de constantes nos permite, igualmente, decantarnos por sinónimos como la locución «tecnologías digitales», que usaremos de manera rigurosa, haciendo que el lector sea capaz de seguir el hilo de la narración.

Del mismo modo, la aclaración realizada en el capítulo que ya finaliza nos permite hablar con propiedad de que dichas tecnologías navegan en «espacios o entornos digitales o virtuales», «espacios públicos mediados», «espacios públicos mediados digitales» o en el «ciberespacio»; cuando no, directamente, remitiremos a la «Red de redes» o «Internet». La adopción de estas voces nos obliga a repasar, asimismo, algunas de las características preeminentes del nuevo sustrato comunicativo, una suerte de particularidades innatas que se convierten ineludiblemente en protagonistas de la problemática que alimenta estas páginas. Se torna forzosa, pues, la referencia a esa mediación, inherente a la nueva realidad comunicativa, y que propicia no solo un entramado de escenarios mucho más complejos de los que se producen en las interacciones en el mundo físico, sino que los flujos de información no sean visibles y que encontremos dificultades para descifrar las atribuciones de los contextos. Lejos de ser esta una cuestión baladí, está íntimamente ligada a la complejidad que encuentran los usuarios para interpretar la naturaleza de los intercambios comunicativos en estos entornos; toda vez que se vuelven incapaces de valorar, en su justa medida, el alcance de los actos que ejecutan.

Cabe señalar, por el contrario, que no podemos culpar a la mediación que posibilita la comunicación de todas injerencias que se dan en estos espacios. Sería como pensar que la promoción del desarrollo

tecnológico es responsable de su mal uso. Por descontado, son muchos y de diverso calado los elementos y agentes que intervienen en este proceso, sin olvidar un detalle importante que ya adelantábamos al revisar la evolución de Internet: la entrada de empresas privadas, la comercialización de segmentos de la Web y la necesidad de obtener lucro de su uso creciente es un factor determinante que pone precio a las informaciones privadas de los sujetos.

Por todo ello, no resulta osado afirmar que muchas de las injerencias que describiremos en los capítulos pertenecientes al análisis derivan directamente de la naturaleza propia, novedosa y difusa en la que se desenvuelve el intercambio comunicativo. Y no significa esto que debamos relegar a un segundo plano los innumerables beneficios que el uso de las tecnologías digitales aporta al ser humano. Se trata únicamente de examinar aquellas atribuciones de la nueva sociedad en red que son susceptibles de redundar en aspectos potencialmente peligrosos para el individuo.

Para ilustrar dichas consecuencias adversas, en nuestro análisis nos centraremos en la observación del trasvase de datos en uno de los entramados tecnológicos que mejor representan la filosofía de la Web 2.0: las redes sociales. Del análisis de su proceder, de los flujos de contenidos que facilitan sus complejas estructuras y, en definitiva, del ideario seguido por la compañía más representativa, obtendremos la respuesta a la hipótesis planteada.

Empero, antes de sumergirnos de lleno en este apartado, revisaremos las mutaciones derivadas de la confluencia entre nuestro objeto de estudio, a saber, la intimidad y vida privada y los espacios comunicativos digitales. Esta reseña no es banal, pues la mediación, a la que tantas propiedades hemos atribuido, es asimismo capaz de modificar no solo la concepción de lo que se considera información íntima *versus* visible; sino cómo y cuándo ha de protegerse esta. Razones de peso, todas las aquí esgrimidas, para dedicar nuestro próximo capítulo a los antecedentes, gestación y explicación de la teoría de la integridad contextual.

CAPÍTULO IV. LA DEMARCACIÓN DE LA INTIMIDAD Y VIDA PRIVADA A LA LUZ DE LAS TECNOLOGÍAS DIGITALES: LA INTEGRIDAD CONTEXTUAL

SÍNTESIS

Tras la necesaria descripción que en todo texto científico ha de hacerse de las constantes que protagonizan el estudio, nos encontramos ante la ineludible tarea de situarlas en la perspectiva actual que data nuestra investigación. Para ello, en el presente capítulo plasmaremos el estado del arte mediante un sólido entramado teórico, un soporte denso pero necesario para enmarcar fielmente la problemática. Y esbozar la fase en que se encuentra la cuestión nos obligará a hablar de reconfiguraciones de los espacios público y privado, muchas de ellas, producidas antes incluso de la llegada de las tecnologías digitales. Igualmente, nos invitará a asomarnos a un escenario reciente, caracterizado por la dificultad para salvaguardar la intimidad y vida privada en los nuevos espacios públicos mediados. En esta tarea que se antoja ardua pero substancial, repasaremos algunas de las teorías más representativas surgidas para dar respuesta a las mutaciones de lo privado tras la llegada del universo digital. Semejante paso resulta necesario por cuanto nos ayudará a describir las claves del marco teórico aportado por Helen Nissenbaum y al que nos remitiremos en el capítulo Discusión de esta tesis. Nos referimos a la protección de la intimidad y la vida privada en función del respeto a la integridad del contexto. Abordemos ahora, sin más prolegómenos, las mutaciones que derivan en dicha aproximación.

1. INTRODUCCIÓN: LA DICOTOMÍA ESFERA PRIVADA *VERSUS* ESFERA PÚBLICA COMO PARÁMETRO PARA PROTEGER LA INTIMIDAD Y VIDA PRIVADA

Partíamos, al inicio de este tratado, de la primigenia distinción entre «lo público» y «lo privado» y de cómo, tradicionalmente, lo

concerniente a la intimidad y vida privada de los individuos se ha estudiado en esa relación de espacios variando, en el paso del tiempo, las competencias y atribuciones de dichos dominios. En definitiva, «lo público y lo privado son ambos —asevera Helena Béjar— objetos alternativos de interés y dedicación, compromisos mudables tal y como se ha dado en llamar a este incesante ir y venir, este movimiento pendular de una esfera a otra» [364]. Conveníamos, no obstante, en que el espacio público era aquel constituido por los asuntos que incumbían a la colectividad e incluían necesariamente una interacción cara a cara en lugares compartidos oponiéndose así a lo privado que quedaba confinado al ámbito reservado del individuo, esto es, a su esfera protegida o aquella donde se desarrollaba su intimidad y vida privada. Dicha consideración presupone que, dado que lo propio de la esfera reservada del individuo es, por esencia, su intimidad y vida privada, esta carecerá de protección en el momento que salga a la arena pública.

Sin embargo, esta dicotomía rara vez se presenta de manera aséptica, en tanto que en numerosas actividades humanas las informaciones privadas forman parte constitutiva e, incluso, necesaria de la interacción social. Es por ello que dicha demarcación entre ámbitos se antoja ineficiente como marco integral para la protección de las informaciones privadas del individuo, por cuanto no contemplaría como tales las intromisiones en la intimidad y vida privada si estas se dan en un espacio público, una coyuntura aparentemente excluyente pero que, a menudo, se da en Internet. Esto provoca que las aportaciones teoréticas tradicionales posean un alto valor descriptivo y hayan sido operativas desde el punto de vista de la filosofía del derecho, pero resulten poco apropiadas para solucionar la aquellos casos en los que las informaciones privadas aparecen fuera de su dominio.

Dicha problemática comienza a manifestarse con la llegada de los medios de comunicación colectiva tradicionales, en tanto que transforman el espacio público en «espacio público mediado» [365], fenómeno que se acentúa tras la emergencia de las tecnologías digitales y el apogeo de los denominados «espacios —en plural, pues son múlti-

---

[364] BÉJAR, H. (1988): *El ámbito de lo íntimo*. Madrid: Alianza, p. 245.

[365] Recordemos que entendemos por «espacios públicos mediados» como aquellos en los que interviene la mediación tecnológica.

ples— públicos mediados digitales» propiciados por dicho ecosistema digital.

Es por ello que la mención velada a los medios tradicionales no es casual. La adopción de las Tecnologías de la Comunicación y la Información ha acelerado los cambios que, desde mediados del siglo xx, ya lastraba la genuina distinción entre «esfera pública» y «esfera privada». En consecuencia, estas mutaciones son herencia de un proceso que aparece ligado al advenimiento de los medios de comunicación de masas y que se enfatiza con el auge de ciertos programas de televisión a mediados del pasado siglo, elevándose a su punto álgido con las tecnologías digitales.

Dichos movimientos paralelos han propiciado la necesidad de un replanteamiento teórico sobre que nos ayude a clarificar qué es legítimo proteger y en qué momento, en la interacción entre los individuos a través y con la tecnología digital, debate que afrontaremos a continuación. Para ilustrar este punto, empezaremos reseñando brevemente los antecedentes de este cambio para situarnos con más solidez en el panorama actual. Con este propósito, convergerán aquí visiones de la sociología clásica (Goffman) y la contemporánea (Béjar, Sennet, Bauman) que enlazaremos, finalmente, con autores clave de los estudios digitales en comunicación (Boyd, Ellison o Nissenbaum).

1.1 LA REDEFINICIÓN DE «LO PÚBLICO» Y «LO PRIVADO»: LOS ANTECEDENTES Y ARTICULACIÓN DE UN ESPACIO INTERMEDIO

Es un dato constatable que el uso de las tecnologías digitales ha mudado significativamente las aproximaciones a la protección de la intimidad y vida privada, especialmente en relación a qué se considera espacio público o de libre acceso y qué constituye el espacio privado o de no injerencia. Sin embargo, como ya hemos adelantado, este proceso no es novedoso ni exclusivo de los entornos digitales sino que surge enlazado a la proliferación de los medios de masas. De hecho y, aunque sin duda ahora este fenómeno ha experimentado una dimensión mayor, los estudios a este respecto florecen tras el auge de

las llamadas emisiones de la intimidad y vida privada[366] en los programas de telerrealidad televisivos durante décadas de los sesenta y setenta, describiendo dichas investigaciones cómo se desdibujan las fronteras entre lo privado y lo publicitable, toda vez que se empieza a mostrar el contenido, otrora íntimo, en el espacio público. En esta redefinición de estadios en la que ambos ya «no están determinados por la naturaleza de sus temáticas sino por la visibilidad que confieren a los acontecimientos en los medios de comunicación»[367], el espacio público, señala García Jiménez, se vuelve «espacio público mediado» estructurando muchos de sus contenidos con asuntos pertenecientes a la esfera reservada del individuo[368]. Como consecuencia directa, «los asuntos pertenecientes a la esfera reservada del individuo pasan a formar parte del espacio público e, incluso, llegan a vertebrar los contenidos mediáticos»[369], por lo que todo contenido, independientemente de su naturaleza, merece ostentar el rango de «lo público».

Este nuevo «espacio público mediado» que Thompson denomina «propiedad pública mediática»[370] es pues una consecuencia de los medios de comunicación colectiva por cuanto han creado un espacio deslocalizado y disociado de la copresencia física, en el que el modelo de interacción tradicional ha sido desplazado. Así pues antes del desarrollo de los *media*, «la propiedad de los individuos y de los acontecimientos estaba vinculada a la idea de compartir físicamente un espacio común. […] Un acontecimiento se convertía en acto público al presentarse ante una multitud de individuos físicamente en el momento que acontecía»[371]. Pero con el desarrollo de los medios de masas, el fenómeno del espacio público se ha desvinculado progresivamente de la idea de una conversión dialógica en cierto lugar compartido. El espacio público tradicional que Thompson bautiza como

---

366 MEHL, D. (1994): «La «vie publique privée», en *Hermès, la revue,* vol. 1, n. 13-14, pp. 95-113, p. 95.

367 GARCÍA JIMÉNEZ, L. (2008): «Las ciencias de la comunicación a la luz de las nuevas tecnologías: retos para una disciplina de la incertidumbre», *Global Media Journal Mexico*, vol. 5, n. 10. p. 105

368 Ibídem.

369 Ibíd., p. 105

370 THOMPSON, J. B. (1998): *Op. cit.,* p. 169.

371 Ibídem., pp. 168-169.

«propiedad pública tradicional de la copresencia» e implicaba interacción cara a cara, así como la reunión de individuos en un lugar común, ha sido sustituida por una presencia mediada, un nuevo espacio visible que introduce «lo público sin lugar».

Por otra parte, la nueva propiedad pública mediática posee otras atribuciones en tanto que proporciona una mayor visibilidad, es decir:

> Un campo de visión distinto del que tienen los individuos en sus encuentros cotidianos con los otros. Los medios colectivos cambian la intencionalidad de la visión o la forma de mirar, focalizando la atención en actos o aspectos concretos. Igualmente, los individuos ahora pueden ser vistos por telespectadores a los que no pueden ver[372].

Consiguientemente, además de producir una fusión entre lo personal y lo colectivo, los cambios introducidos conducen al fenómeno de la *hipervisibilidad*[373]. En este sentido, Dominique Wolton señala que el «principio de publicidad»[374] provoca que «el espacio público se haya convertido en el patrón y símbolo de la sociedad lo que, paralelamente, desvaloriza el espacio privado»[375], haciendo que las cuestiones vinculadas a la esfera privada se aborden en la esfera pública.

Este contexto de cambios recíprocos nos aboca a un replanteamiento integral por cuanto los ámbitos público y privado no se dan independientemente el uno del otro sino que toda transformación de la esfera pública conlleva, al mismo tiempo, una transformación de lo privado, (fenómeno que ya adelantábamos al citar a Gouldner en la *Aclaración de Términos* del *Capítulo II*. Veamos ahora, con más detenimiento, cuáles son las implicaciones de este proceso.

---

372 Ídem.

373 VERDÚ, V. (2003): *El estilo del mundo. La vida en el capitalismo de ficción*, Barcelona: Anagrama, p. 163.

374 La expresión era usada por Habermas como sinónimo de «esfera pública». Thompson recoge así el pensamiento de Habermas para quien la concepción de la propiedad pública tiene un carácter esencialmente espacial y presencial. Así, bajo las lentes de esta consideración, Habermas no contemplaría las nuevas formas de propiedad pública creadas por los medios de comunicación colectiva. Se puede hacer una crítica similar del trabajo de otros teóricos sociales cuyas razones sobre el carácter cambiante de la esfera pública convergen en ciertos aspectos en el punto de vista de Habermas.

375 WOLTON, D. (1991): «Les contradictions de l'espace public médiatisé» en *Hermès* n. 10.

1.1.1 El espacio público mediado y la intimidad y vida privada como elemento constitutivo: los procesos de personalización y de subjetivación del espacio público

> Más en general, las cosas visibles no
> concluyen en la oscuridad y el silencio,
> se desvanecen en lo más visible
> que lo visible: la obscenidad
>
> J. Baudrillard, *Las estrategias fatales*[376]

En esta continua reformulación de espacios, el hecho de que los individuos salgan de sus hogares e incluyan sus conflictos en un proceso de comunicación de masas es visto por Chambat y Ehrenberg como el germen por el cual «el espacio privado modela el espacio público»[377]. Asistimos, consecuentemente, a la desvirtuación del espacio público defendida por Sennet, para quien cuando la vida privada se erige como único ámbito de significación, el hombre, como persona, deja paso al sujeto íntimo, lo que concluye en una decadencia de la arena pública además de la consiguiente mudanza del sentido de vida privada[378]. Se produciría, a la vez, un proceso de desnaturalización de la esfera privada del sujeto que, en tanto que difundida, perdería su esencia. El espacio privado modela entonces al espacio público que se «personaliza», en una desvirtuación inducida por la aparición de la *sociedad intimista*[379] y que acaba por amenazar la vida colectiva.

Observa este mismo patrón Dominique Mehl al verificar que «las transmisiones de lo íntimo —igualmente en referencia al éxito de los *reality shows* en las cadenas de televisión francesas— ponen en escena una nueva articulación entre el espacio público y privado»[380]. Según Mehl estas emisiones representan un elemento central de doble movimiento, de publicitación de lo privado y privatización de lo público, creando una suerte de «vida pública privada» (*vie publique privée*) nacida de la hibridación de ambas esferas. Sin embargo, mientras Sennet ve una desaparición del espacio público que termina siendo devorado por lo privativo, Mehl avisa del peligro que entraña el movimiento contrario:

---

376 BAUDRILLARD, J. (1983): *Las estrategias fatales,* Barcelona: Anagrama, p. 58.
377 CHAMBAT, P. y EHRENBERG, A. (1993): «Les reality shows, nouvel âge télévisuel? », *Espirit*, n. 1, enero, p. 45.
378 BÉJAR, H. (1988): *Op. cit.,* p. 161.
379 SENNET, R. (1979): *Op. cit.,* p. 30.
380 MEHL, D. (1994): *Op. cit.,* p. 97.

> La auscultación de la realidad actual a través de sus medios no se caracteriza por la destrucción del espacio público, anulado por la invasión de las temáticas privadas. La sociedad intimista de Sennet mostraría una reformulación de las expresiones privadas y una captación, por parte de la escena pública, de nuevas temáticas […] La articulación entre las dos esferas es fluctuante, pero, con el correr del tiempo, tiende a enriquecer el espacio público con nuevas problemáticas y con nuevas cuestiones en juego, y tiende también a remodelar el espacio privado[381].

A este respecto, Mehl menciona la aparición de dos escenarios intermedios que coexisten: el proceso de personalización descrito por Sennet genera los contornos de una «vida pública privada» (*vie publique privée)* que cohabita con una «vida privada pública» (*vie privée publique*) creada por un dispositivo de subjetivización «en el que se da una representación lo más realista posible de lo privado en el espacio público»[382]. Para el autor, la convivencia de estos dos ámbitos intermedios incita dejar de concebir estas esferas como terrenos radicalmente separados entre sí o como comportamientos estancos. Consideración similar a la que realiza Alain Cottereau, para quien la articulación entre ambas de un «espacio intermedio» de atribuciones comunes, nos alienta a indagar sobre sus articulaciones y su interpenetración, a visitar los lugares en los que se tocan y se modelan recíprocamente, es decir, dónde se hace visible el enlace entre el hombre privado y el hombre público[383].

1.1.2 La debilitación del ámbito introspectivo y el fenómeno de la «extimidad»

> Orgullosos de ser telepolitas,
> los nuevos ciudadanos celebran sus fiestas
> y sus ceremonias para las cámaras,
> nueva expresión de la existencia social
>
> *Telépolis,* Javier Echeverría[384]

La aparición de ese espacio intermedio nos obliga a retomar un concepto precedente en el tiempo que proviene de la psicología social y que, recientemente, se ha trasferido a las ciencias de la comunica-

---

[381] Ibídem., pp. 97-101.

[382] Ibíd., pp. 94-95 y 116.

[383] COTTEREAU, A. (1992) «Esprit public et capacité de juger. La stabilisation d'un espace public en France aux lendemains de la Révolution». *Raisons Pratiques*, n. 3.

[384] ECHEVERRÍA, J. (1994): *Telépolis*. Barcelona: Destino, p. 30.

ción y la sociología para justificar esta apropiación perpetrada por lo privado en detrimento del espacio público. Se trata del fenómeno de la «extimidad» o ese puente donde, supuestamente, se materializan las articulaciones entre espacio privado y público. La «extimidad», vocablo acuñado por el psicoanalista francés Jacques Lacan en 1958, se ha reutilizado frecuentemente en la actualidad para referirse a la tendencia de las personas a hacer pública su intimidad y vida privada. Al hacer gala de esta extimidad, los sujetos desvirtúan su propia esfera privada y, de manera intencional, arrojan su intimidad y vida privada a la arena pública, algo que enlaza con lo que Sennet describiría al esbozar su «sociedad intimista» y con la hibridación de esferas definida por Mehl.

ACLARACIÓN:

Curiosamente, el concepto primigenio de extimidad elaborado por Lacan dentro de los vértices de la psicología partía de la visión contraria. Al construir el concepto «extimidad» mediante el prefijo «ex» de *exterieur* y la palabra *intimité,* pretendía definir la existencia de un «cuerpo extraño» dentro del «yo»[385], del ámbito íntimo del ser humano, describiendo aquello que es externo al individuo pero con lo que se identifica: «lo más íntimo —afirma Lacan— es justamente lo que estoy constreñido a no poder reconocer más que fuera»[386]. Rompe, por tanto, el binario entre «lo interior» y «lo exterior», designando una referencia exterior a lo simbólico, hasta el punto de que esa referencia llega a ser necesaria para generar la propia identidad. La extimidad por tanto no se opone, como erróneamente se cree, a la conservación y reserva de la intimidad y vida privada, sino que afirma que lo íntimo es «Otro»[387]. Echando por tierra la lógica de la «sociedad de extraños» [388] descrita

---

385 MILLAR, J-A. (1994): *Extimité in lacanian theory of discurse*. París: Paidós, p. 76

386 LACAN, J. (2008): *Seminario 16. De un Otro al otro*, Barcelona: Paidós, p. 246.

387 En contraste con la corriente defendida por los «ego-psicólogos» angloamericanos de la época, Lacan considera al yo como algo constituido en el campo del «Otro», es decir, gracias al lazo social o vínculo. Escribimos «Otro» con mayúsculas para diferenciarlo del «otro», con minúsculas, que es lisa y llanamente, un semejante. El «otro», decía Freud, es siempre un modelo identificativo, un amigo o enemigo a nuestro nivel, mientras que «el Otro» es siempre un referente significativo y de él parten las demandas para el sujeto.

388 SIMMEL, G. (1986): *Sociología. Estudios sobre las formas de socialización*. Alianza: Madrid.

> por Simmel y que definía la existencia privada por la aparición de «los otros», en la extimidad el «Otro» se torna necesario para definir nuestra propia substancialidad, para la creación del propio sujeto. Nuestra identidad, el «yo» mismo y, en definitiva, nuestra intimidad se define por lo que hay fuera.
>
> Con el paso del tiempo, será el psiquiatra Serge Tisseron quien, ignorando la aportación lacaniana, propondrá la redefinición de extimidad como «el movimiento que empuja a cada cual a mostrar una parte de su vida íntima, tanto física como psíquica» [389].
>
> Por otra parte no resulta extraño que este término haya sido reutilizado si tenemos en cuenta que una de las dimensiones de lo privado, en concreto, la intimidad, alude a lo más interno y personal del individuo, a su «yo», por lo que representa, señala Béjar, «una categoría psicológica» [390].

Aunque desvirtuada de su significado inicial, esta expresión ha conocido un renacimiento tras el auge de las tecnologías digitales por cuanto se ha rescatado para explicar la exposición voluntaria del ámbito reservado a través de las tecnologías digitales. Una exhibición inusitada de retales personales aun cuando estos no poseen ningún *role* en la interacción social, ni justificación para su aparición en el ámbito público.

La extimidad parte de la base de que el auge de la interconexión mediada supone la perversión de la substancialidad propia de la esfera privada por parte de los individuos, quienes, en este contexto, tienden a valoran su publicidad por encima de su salvaguarda. En consecuencia, refiere no solo a la modificación esencial del espacio público, ya que al hacerlo también construye o modela lo que está dentro, lo introspectivo, tornándose en definitoria del entorno privado. En esta paradójica fusión de lo interno y lo externo, las esferas privada y pública, antes separadas y opuestas, se revelan cada vez más interdependientes y complementarias [391]. Es por ello que para la antropóloga Paula Sibilia la extimidad ejemplifica el lugar en el que se articula ese espacio intermedio entre esfera privada y pública [392].

Como paso intermedio entre el binomio esfera pública *versus* esfera privada, esta vida privada condicionada en que se constituye y representa la extimidad tiene, al igual que sucede con todo comporta-

---

389 TISSERON, S. (2001): *L'intimité surexposée*, París: Hachette, p. 52

390 BÉJAR, H. (1987): *Op. cit.*, p. 785.

391 TISSERON, S. (2001) *Op. cit.*, p. 49

392 SIBILA, P. (2008): *La intimidad como espectáculo*. Fondo de Cultura Económica: Argentina.

miento público, muy en cuenta a su audiencia. Por ello, es escenificada o fabricada para ser vista, una suerte de vida privada ensayada y premeditada de cara a los otros a modo de presentación pública, en clara simetría a los «rituales de presentación» aludidos por Goffman[393]. Enlaza igualmente con los planteamientos de Bauman, por cuanto nuestra propia substancialidad se vuelve adaptable reconstruyéndose y reinventándose según las circunstancias externas[394].

1.1.3 Críticas al espacio intermedio e ineficiencia del concepto para solventar la problemática de las intromisiones en la intimidad y vida privada

El espacio intermedio creado por la hibridación entre esfera pública y privada, bien sea impulsado exclusivamente por los medios de comunicación colectivos[395] o por la intencionalidad del sujeto[396] ha sido retomado para ilustrar la inexistencia de barreras nítidas entre espacio privado y público. Sin embargo, si bien analizan el tema de la extensión de lo privado a lo público y las transformaciones que, en consecuencia, sufre el espectro reservado del individuo, no resultan un punto de partida apropiado para aproximarnos y dar respuesta a qué es legítimo proteger cuando nuestras informaciones privadas aparecen en los entornos digitales y cómo hacerlo.

La pertinencia estas aproximaciones recala en que ejemplifica esa interdependencia de lo privado y lo público, a la vez que, acertadamente, deja patente cómo ambas esferas se condicionan y modifican mutuamente. No obstante, esta extensión de la esfera privada a la pública o, mejor dicho, esta revelación de informaciones privadas se hace de manera intencional: la intimidad extimada lo es por un carácter intencional de sujeto, al igual que sucede en la sociedad intimista de Sennet. Por el contrario, no todas las injerencias en el ámbito privado del individuo se producen bajo este condicionante. En consecuencia, en tanto que se trata de una apertura de la esfera íntima premeditada, es decir, perpetrada por el propio individuo, el concepto

---

393 GOFFMAN, E. (1997): *Op. cit.,* p. 50.
394 BAUMAN, Z. (2007): *Op. cit.,* p. 127.
395 MEHL, D. (1994): *Op. cit.,* pp. 95-113.
396 SENNET, R. (1979): *Les tyrannies de l'intimité*, París: Seuil.

por sí solo no es suficiente para explicar las situaciones que, en los entornos digitales, dejan al descubierto todo aquello que el individuo desea proteger. Destacaremos, sin embargo, que sí resulta útil para evaluar los comportamientos en los que es el individuo quien, *motu proprio*, decide dar a conocer su intimidad y vida privada, y, aún en este escenario, sería cuestionable, como veremos más adelante, si el sujeto está provisto o no de la información necesaria para tomar esa decisión de revelar su intimidad de manera consciente.

Por otra parte, al intentar negar la existencia de una demarcación clara entre esferas los autores reseñan la existencia de un espacio intermedio, un área de atribuciones indefinidas en la que se fusionan elementos de la esfera privada y la pública y que se encontraría a medio camino entre el espacio público puro y la esfera privada que, por naturaleza, le es propia al ser humano. Como es palpable, este espacio intermedio no clarifica nada y dicha idea sería reducible a afirmar que hay datos privados que se emplazan en el espacio público ya sea por un carácter intencional del sujeto o por obra de los medios colectivos, posean o no justificación alguna en el contexto en el que se despliegan. Por ello, desde este escrito proponemos abandonar esa representación intermedia e indefinida y constatar que, además de esfera privada y esfera pública, es factible que los datos privados puedan transgredir el ámbito reservado por cuanto son necesarios para interaccionar en el espacio público, una visión más cercana a la cotidianeidad pero no exenta de dificultades conceptuales.

2. NUEVAS APROXIMACIONES A LA PROTECCIÓN DE LA INTIMIDAD Y VIDA PRIVADA EN ENTORNOS DIGITALES

2.1 LA SUPERACIÓN DEL MODELO DICOTÓMICO ESFERA PRIVADA-ESFERA PÚBLICA Y LAS APORTACIONES DE HELEN NISSENBAUM

Una de las aportaciones más importantes a la protección de la intimidad y vida privada en los espacios públicos mediados por las tecnologías es la realizada por la autora estadounidense Helen Nissenbaum, cuyos textos han sido usados como base de las nuevas regulaciones digitales. Nissenbaum parte del estudio de la vigilancia masiva en las sociedades actuales, práctica que no constituye un fenó-

meno novedoso por cuanto surgió como un aspecto vital de las sociedades modernas, pero que con la llegada de las tecnologías se ha visto incrementada. La autora parte de casos reales, y observa que la tradicional dicotomía público *versus* privado se revela insuficiente para solventar dilemas éticos como los provocados por la denominada «vigilancia pública»[397], término que usa para etiquetar prácticas como la grabación con cámaras de circuito cerrado en sitios públicos, la vigilancia en el trabajo o, posteriormente, el uso de las informaciones recabadas tras los atentados terroristas del 11 de septiembre en la ciudad de Nueva York, así como mediante la aplicación *Street View* de Google Maps. En todos estos casos, la distinción tradicional usada por el derecho o la filosofía se pierde en delimitaciones contextuales acerca de lo que incumbe a cada esfera, pero no es capaz de dar soluciones.

Para verificar la ineficiencia del modelo bipolar privado *versus* público, Nissenbaum parte del análisis[398] de tres principios que han guiado las políticas de protección de este derecho en la tradición jurídica anglosajona, tres formas de conceptuar la vida privada mediante oposiciones entre los siguientes binomios: 1) competencias gubernamentales para vigilancia y control de datos *versus* espacio reservado del individuo, 2) designación de lugares públicos frente a lugares privados o espacios de no intromisión y 3) distinción entre «información sensible» e «información no sensible». Dichas oposiciones, aunque útiles desde perspectivas teóricas en campos como la política o el derecho, conllevan carencias por cuanto la aplicación de estos principios no es siempre obvia y, en numerosas ocasiones, la línea divisoria entre los términos de cada binomio no es ni estática, ni universal. Es decir, se tornan ineficientes fuera de los contornos doctrinales pues en los en contextos reales esta demarcación difícilmente se presenta aséptica.

Las dos primeras oposiciones que definirían el área en la cual el individuo no es molestado ni sufre intromisión alguna por parte de los poderes estatales, asimila dicha área a un espacio de naturaleza física, por lo que desembocarían en una protección exclusiva de la

---

397 NISSENBAUM, H. (1998): *Op. cit.*,

398 NISSENBAUM, H. (2004): *Op. cit.,* p. 107.

esfera privada en cuanto a propiedad, recalando en el citado error de equiparar vida privada con espacio privado.

Por su parte, el tercer binomio que distingue entre «datos o informaciones de carácter sensibles» o «no sensibles» no queda exento de incertidumbre. Para abordar su validez Nissenbaum recupera las aproximaciones filosóficas que sostienen que el grado de sensibilidad de la información debe ser un factor determinante para discernir si se ha producido o no una intromisión en la esfera privada. Estos estudios se basan en la existencia de una categoría llamada «información sensible» que resultaría clave a la hora de defender qué contenidos privados deben protegerse y cuáles no. La autora toma el término de la tradición jurídica y, tras una revisión de los escritos de Charles Fried: *Privacy*[399], Tom Gerety: *Redifining privacy*[400] y William Parent: *Privacy morality and the law*[401], se centra en Raymond Wacks, adoptando la definición que dicho autor aporta sobre «informaciones de carácter sensible» en *Personal Information: privacy and the law*[402]. Distingue así entre información o datos personales «de carácter no sensible» en el sentido general de datos personales, esto es información identificativa y referente a personas, mientras que se reserva los términos «sensible» o «confidencial» para las informaciones de carácter privado. Se percata Nissenbaum, no obstante, de que el propio funcionamiento de los entornos digitales permite a menudo que los datos personales, esto es, de carácter no sensible, puedan llevarnos a obtener informaciones de carácter privado mediante triangulación de datos. En este sentido, la autora arguye que, incluso cuando la información proporcionada no es sensible, si se encuentra emplazada en los espacios públicos de la Red y se utiliza para realizar el perfilado de usuarios, es susceptible de derivar en intromisiones indeseadas e, incluso, llevar a la identificación del sujeto[403]. De este modo, al analizar la tradición jurídica anglosajona, la autora se hace eco de que de

---

399 FRIED, C. (1968): «Privacy», en *The Yale Journal*, vol. 77, pp. 475-493.

400 GERETY, T. (1977): «Redefining privacy», en *Harvard Civil Rights-Civil Liberties Law Review,* vol. 12, n. 2, pp. 233-296.

401 PARENT, W. (1983): «Privacy morality and the law», en *Philosophy & Public Affairs*, vol. 12, n. 4, pp. 269-288.

402 WACKS, R. (1989) *Personal information: Privacy and the law.* New York: Oxford University Press.

403 NISSENBAUM, H. (2004): *Op. cit.*, p. 116.

un problema similar al que ya mencionábamos en el *Capítulo II* al abordar la diferencia entre «datos de carácter personal» y «datos privados».

Así, esta disparidad de situaciones en las que se mezclan informaciones privadas en espacios públicos torna necesario cuestionar el marco ofrecido por estos tres principios como estándar universal para deliberar sobre la vida privada. Para ello, Nissenbaum sustenta su ideario en dos parámetros: En primer lugar, la autora rechaza enunciar sus planteamientos en términos de dicotomía entre «público» *vs.* «privado», «sensible» *vs.* «no sensible» o «gobierno» *vs.* «privado». La segunda es que la protección de la intimidad y vida privada estaría condicionada por dimensiones temporales, de localización y otras múltiples variables, esto es, vendría determinada por el contexto y, en este sentido, admite la variabilidad que se puede dar en la categorización de informaciones a través de diferentes culturas, períodos históricos y lugares.

2.2 LA DIFERENCIA ENTRE ESFERA PRIVADA Y DATOS PRIVADOS

En nuestro día a día, las informaciones privadas saltan al espacio público ya que resultan necesarias para facultar y asegurar la interacción social, dotar de significado nuestras relaciones y posibilitar el desarrollo de las dinámicas propias del ámbito social del sujeto. Este proceso en sí mismo no priva de su sentido primigenio y protección absoluta al ámbito reservado del individuo que continúa siendo un espacio inviolable, pero sí ofrece una cierta ambigüedad en lo que respecta a la salvaguarda de esa información privada emplazada en la arena pública. De hecho, es aquí donde vislumbramos una contradicción: ¿estamos preservando nuestra esfera privada si necesitamos revelar datos privados para posibilitar la interacción social?

Esta aparente paradoja nace de lo que autores como Rafael Capurro ha calificado como la identificación errónea entre los términos «esfera privada» e «informaciones (o datos) privados», locuciones que no son sinónimas, ni intercambiables[404]. La substancialidad

---

[404] BUCHMANN, J. (ed.) (2013): *Op. cit.,* p. 14.

de la esfera privada evocaría al espacio protegido donde uno puede ocultar completamente su persona del mundo exterior. Por el contrario, cuando hablamos de informaciones relativas a la intimidad y vida privada hacemos referencia a una dimensión mucho más amplia ya que, aunque su ecosistema natural es la esfera privada, estos contenidos pueden saltar a la arena pública convirtiéndose en una parte importante de la interacción social. Dicha información puede emplazarse en lugares públicos a voluntad, mientras que la esfera privada es inamovible. Su pertinencia o no dependerá no solo de la intención del propio sujeto, tal y como sugieren las alusiones a la extimidad, sino de que su emplazamiento en el espacio público sea pertinente y esté justificado por el contexto. De no ser así, podemos entender que se ha producido una violación en nuestra intimidad y vida privada.

Todo ello nos lleva a la apreciación de un aspecto en la preservación de nuestros datos privados: su relatividad en función de la coyuntura, esto es, de las atribuciones concretas del contexto. Asumimos, por tanto, que en estas interacciones el individuo decide y controla qué cantidad y qué tipo de información privada desea desplegar en cada escenario o situación particular. De este modo, la protección de la intimidad y vida privada se traduce como «la habilidad de las personas para elegir la información qué enseñan y la qué esconden»[405], una reformulación íntimamente ligada al concepto de autodeterminación informativa, por cuanto el respecto a la intención del sujeto se consolida como requerimiento capital.

2.3 LA PROTECCIÓN DE LAS INFORMACIONES PRIVADAS EN LOS ESPACIOS PÚBLICOS MEDIADOS CREADOS POR LAS TECNOLOGÍAS DIGITALES

El despliegue de información sobre la vida privada en espacios públicos no es consecuencia de la proliferación de los entornos digitales ya que, como sabemos, en numerosas ocasiones, los datos privados son necesarios para completar acciones de la vida cotidiana tales como ir al médico, realizar gestiones bancarias o mantener una con-

[405] Ídem.

versación entre amigos. Reflejo de la realidad física, esta dinámica se reproduce en los espacios públicos digitales, sin embargo, las características inherentes a las tecnologías añaden ciertos matices. En el pasado, la mayoría de los individuos asumían que en el desempeño de sus actividades y movimientos del día a día no eran ni vigilados, ni catalogados, por lo que enlazaban sus quehaceres cotidianos de manera anónima. En la sociedad actual, por el contrario, la tecnología es capaz de obtener, procesar, analizar y agregar cantidades ingentes de información sobre una persona concreta, siguiendo su huella a través de las acciones que ejecuta en la Red. Para Zimmer esto significa que, virtualmente:

> No hay límite en la cantidad de información que puede ser recogida, en el nivel de análisis de datos que puede ser realizado y que la información puede ser compartida con facilidad y digitalmente almacenada para siempre [la consecuencia es] el incremento en la magnitud, detalle, meticulosidad, y rango de la habilidad para vigilar el día a día de los ciudadanos, mientras realizan sus actividades públicas[406].

Cuando realizamos una compra en el supermercado nuestra acción es anónima en la vida real, salvo para las personas que en ese momento están en la tienda con nosotros, pero si llevamos a cabo esta acción a través de las tecnologías digitales, el poder de agregación de información de Internet permite que se nos pueda perfilar hasta límites insospechados e, incluso, identificarnos. La diferencia recae, por tanto, en que estos espacios públicos digitales representan, por sus características inherentes, una esfera social única y novedosa en la que grandes cantidades de información son susceptibles de ser almacenadas y agregadas[407] y los datos proporcionados pueden ser fácilmente copiados, utilizados y sacados de contexto[408].

Los ordenadores, por tanto, «no han creado la situación en la que los ciudadanos de las sociedades avanzadas se encuentran actualmente —afirma David Lyon— Éramos súbditos de los datos mucho antes de que se produjera ninguna supuesta revolución

---

406 ZIMMER, M. (2007): *Op. cit.,* pp. 8-9.
407 GOVANI, T. y PASHLEY, H. (2005): *Op. cit.*
408 BOYD, D. (2006): *Op. cit.*

tecnológica»[409]. Lo que sí es novedoso, sostiene el autor, es la escala y la ubicuidad de la vigilancia contemporánea que «sería imposible en ausencia del poder de los ordenadores»[410]. Para llegar a esta conclusión, Lyon parte, al igual que Nissenbaum, Allen y Slobogin, del estudio de la vigilancia masiva en las sociedades actuales. Estos autores empezaron a identificar la complejidad que conlleva la protección de esos datos privados cuando aparecen en escenarios públicos[411], denunciando, a la postre, que la mayoría de las teorías normativas y filosóficas fracasan al subestimar dicho problema obviándolo, incluso, en su totalidad[412]. Dichas teorías parten la mencionada equiparación entre informaciones y esfera privada, lo que, en palabras de Zimmer provoca que:

> Conceptualmente, la idea de que la vida privada pueda ser violada de alguna manera en un espacio público sea considerada, a menudo, paradójica. Para la mayoría, el valor de la privacidad se aplica exclusiva y únicamente a la esfera de la privacidad del individuo [413].

Igualmente, dichos planteamientos se sustentan en la tradicional dicotomía entre esferas, nociones con un alto poder descriptivo en el papel, pero que se tornan poco eficientes por cuanto las tecnologías digitales son capaces de almacenar, recolectar y analizar los datos, independientemente de nuestra situación geográfica, e, incluso, en el más privado de los lugares como es el hogar[414].

---

409 LYON, D. (1995): *El ojo electrónico,* Alianza, Madrid, p. 66.

410 Ibídem.

411 El estudio de la privacidad en público defendido por Nissenbaum en 1997 y 1998 como punto de partida para sustentar la teoría de la integridad contextual, fue anticipado por Allen en 1988 y retomado posteriormente por Slobogin en 2002.

412 NISSENBAUM, H. (1998): *Op. cit.,* p. 7.

413 ZIMMER, M. (2005): *Op. cit.,* p. 107.

414 WESTER, M. y SANDIS, P. (2010): «Privacy and the public», en ARIAS-OLIVIA, M., WARD BYNUM, T., ROGERSON, S., TORRES-CORONAS, T. (eds): *The «backwards, forwards and sideways» changes of ICT, 11th International conference on the Social and Ethical Impacts of Information and Communication Technology* (ETHICOMP 2010) 14 al 16 de abril, 2010, Tarragona, España: Universitat Rovira i Virgili, pp. 580-586, p. 580.

2.3.1 ¿Una teoría sobre la protección de los datos privados en el espacio público?

El derecho a la intimidad y vida privada no solo incluye el respeto a nuestra esfera privada, sino el control efectivo sobre nuestras informaciones y datos personales. No obstante, el aspecto normativo reconoce que la protección de la vida privada debe ser medida respecto a otros valores y en función del contexto, existiendo, por tanto, una competencia de intereses. Un simple ejemplo de tal juicio valorativo es nuestra disposición a desplegar información privada en los aeropuertos y permitir que nuestra maleta sea inspeccionada y rastreada: la seguridad ciudadana se sopesa en estas situaciones y se considera un aspecto vital frente a la reserva de nuestras informaciones privadas[415]. En el caso de la información recolectada por las tecnologías digitales sucede lo mismo y, aunque su aparición pueda ser considerada inocua en ciertos escenarios, ocurre que, para otros contextos, deseamos mantenerla en privado.

A esta arbitrariedad hay que sumarle que el rango de dimensiones del aspecto privado del sujeto es extenso y va desde la información, a las actividades, decisiones, pensamientos y comunicación, entre otros, por lo que una teoría global sobre protección de la vida privada debería tener en cuenta todas estas dimensiones lo que se antoja imposible[416]. Así por tanto, aunque el emplazamiento de informaciones privadas en lugares públicos se ha convertido en parte de la vida diaria de los ciudadanos, la dificultad en la actualidad recae en cómo conjugar la capacidad de agregación, distribución y descontextualización de esas informaciones que acompaña al uso de las TIC con la protección de la intimidad y vida privada de los individuos. Nos preguntamos entonces ¿Cómo podemos proteger a voluntad estos datos privados en la arena pública? ¿Es posible sin impedir u obstaculizar los procesos comunicativos? Para resolver este punto hemos de acudir a las teorías contextuales que enlazan el amparo de lo privado a la justificación de dichas informaciones en el espacio público, sopesando su pertinencia en función de una serie de normas compartidas.

---

415 ZIMMER, M. (2007): *Op. cit.,* p. 7.
416 NISSENBAUM, H. (2004): *Op. cit.,* p. 105.

2.3.2 La protección de la intimidad y vida privada en función de los contextos: Los primeros intentos y el contrato social

Las teorías contextuales evalúan la conveniencia de la introducción de datos privados en el espacio público en función de una serie de parámetros determinados por el contexto. Esto significa que la protección dichos contenidos se mide respecto a otros intereses gracias a la correcta interpretación de la información que recibimos de cada escenario. Y cuando la introducción de esos datos privados no se hace de acuerdo al respeto de las citadas normas, se entiende que se ha vulnerado la intimidad y vida privada del individuo.

La existencia de unos principios compartidos supone que todos los miembros de la comunidad[417] entienden un mismo lenguaje, lo que permite la correcta interpretación de dichos preceptos respecto a los cuales el individuo decidirá desplegar o no información privada. En otras palabras, la lógica del contexto va a clarificar a todos los miembros de esa comunidad lo que puede constituir o no una vulneración de la vida privada y cuándo es lícito o no mostrar dicha información. Por tanto, de la existencia de estos datos privados en el espacio público no se deriva que toda la esfera reservada del individuo deba ser conocida, sino solo aquellos datos que el usuario quiere enseñar y cuya justificación viene dada por su pertinencia en la interacción social. Por consiguiente, el carácter público del lugar donde se emplacen los instrumentos técnicos no es un elemento determinante para excluir, *per se*, un supuesto de intrusión ilegítima en la intimidad[418].

Estas aproximaciones recogen los postulados de Mason para quien la armonización de derechos en el mundo digital se daría gracias a la formulación de un nuevo «contrato social»[419] capaz de satis-

---

[417] Donalson y Dunfee definen comunidad como: «un grupo de gente auto definido y auto circunscrito que interactúan en el contexto de actividades valores o metas compartidas y que son capaces de establecer normas éticas de comportamiento por sí mismos.» DONALSON, T., y DUNFEE, T. (1994): «Towards a unified conception of bussiness ethics: integrative social contracts theory», en *The Academy of management Review*, vol. 19, n. 2, pp. 252-284, p. 262.

[418] MEDINA GUERRERO, M. (2005): *Op. cit.,* pp. 84-85

[419] MASON, R. O. (1986): «Four ethical issues of the information age», en *MIS Quarterly*, n. 10, vol. 1, pp. 5-12, p. 11.

facer todas las partes implicadas y en cuya traslación al panorama actual habría de ser suscrito por a usuarios, empresas de Internet, proveedores del servicio y administraciones. Estos acuerdos normativos aparecen redefinidos por Dunfee como aquellos «contactos sociales existentes, que dan cuerpo a las normas de comportamiento que derivan en metas compartidas, creencias y actitudes de grupos o comunidades de grupos» [420]. Dichas convenciones, creadas por una determinada comunidad, son, por lo general, acuerdos informales en los que los participantes, por sí mismos, no están guiados por un conjunto de normas explícitas sino que, de algún modo, las aceptan cuando entran a formar parte de ese grupo o realizan transacciones con dicha comunidad[421]. Esta afirmación que pone las bases de las teorías contextuales, supone un primer intento de enlazar la protección del sujeto a las normas particulares que rigen en un determinado escenario, planteamiento que, posteriormente, recogerá Nissenbaum.

Así, lo novedoso del enfoque desarrollado por nuestra autora de referencia es que no acomete una simple enumeración de atribuciones de cada esfera o una redefinición de «lo público» frente a «lo privado»; ni siquiera realiza una descripción pormenorizada de todos los escenarios en los que los datos reservados entran en juego. Rechaza, igualmente, esgrimir una teoría global sobre los contenidos privados en el espacio público. Nissenbaum, que construye sus argumentos en la filosófica política y teoría legal, aporta un marco teórico acorde con el mantenimiento del flujo coherente de datos en los contextos en los que se emplaza la información, es decir, enlaza la lógica de la pertinencia o no de informaciones privadas al dictado de las normas que imperan en cada escenario determinado, resistiendo, acertadamente, la tentación de enmarcar su crítica en el marco de la retórica «faucaldiana» de la vigilancia y control. Es por ello que su enfoque revolucionario la sitúa entre los autores más nombrados a la hora de afrontar la problemática referida a la protección de lo privado en entornos digitales, constituyéndose en pilar teorético ineludible en el abordaje y elaboración de futuras legislaciones de protección de datos. Veamos ahora, con el necesario detenimiento, en qué consisten los postulados de la autora.

---

[420] DUNFEE, T. (1991): «Business ethics and extant social contracts», en *Business Ethics Quaterly*, n. 1, vol. 1, pp. 23-51, p. 32.

[421] DONALSON, T., y DUNFEE, T. (1994): *Op. cit.,* p. 262.

3. LA PROTECCIÓN DE LAS INFORMACIONES PRIVADAS MEDIANTE EL RESPETO DE LA INTEGRIDAD CONTEXTUAL

Nissenbaum sienta en 1997 las bases para abordar la salvaguarda efectiva de las informaciones privadas en entornos digitales y lo hace al enunciar su teoría *Privacy as contextual integrity*. La idea primigenia, no obstante, fue posteriormente reformulada por la autora bajo la influencia de académicos como Solove[422], Benkler[423] o Kerr[424], y teniendo en consideración muchos de los posteriores desarrollos de las Tecnologías de la Información y Comunicación.

Como es de esperar, en este punto se torna menester delimitar a qué nos referimos exactamente cuando hablamos de integridad contextual, un apunte ineludible y que sería de fácil resolución mediante la simple transposición de los postulados de la autora, de no ser por una salvedad: Nissenbaum nunca ha aportado una definición al uso. Ello nos obliga, llegados a esta tesitura, a intentar delinear las claves que se encierran en esta locución en parte críptica.

De manera concisa, cuando citamos el respeto a la integridad del contexto nos referimos al mantenimiento de la coherencia de los flujos informativos que conforman dicho escenario, así como a la pertinencia del despliegue de ciertos datos en el mismo, estando estos dos factores determinados por la coyuntura concreta, esto es, las coordenadas que dan forma a esa situación específica.

Vayamos poco a poco. Entendemos que por «contexto» o «escenario que rodea al hecho comunicativo» nos referimos a un momento concreto de la interacción, que viene determinado por una serie de condicionantes (tiempo, espacio… etc.) y actores implicados. Las propiedades de dicho contexto se mantendrán en la medida en que no exista ninguna mutación en los elementos que lo definen, ya que, si cambia una de las coordenadas o los agentes involucrados, haría aparición otro escenario distinto.

---

422 SOLOVE, D. J. (2008): *Op. cit.*

423 BENKLER, Y. (2006): *Op. cit.*

424 KERR, I.; STEEVES, V. y LUCOCK, C. (eds) (2009): *Lessons from the identity tail: anonymity, privacy and identity in a networked society*. Oxford: Oxford University Press.

Observemos, a este tenor, el siguiente ejemplo ilustrativo: imaginemos que plasmamos en una instantánea la visión correspondiente una conversación entre amigos íntimos en un bar. En esta imagen veríamos a dos personas dialogando de manera cercana sobre una amplia gama de temáticas posibles: asuntos banales o no, privados o no, profesionales… o no y un largo etcétera. Es decir, podríamos entender que el flujo de información en coherencia con dicho escenario puede conformarse de una serie de contenidos correspondientes a un abanico de temas más o menos amplio, flexible y sin restricciones.

Pero cambiemos ahora las variables, mutemos el contexto. Los dos amigos trabajan juntos, así que salen del bar y caminan hacia el lugar donde desarrollan su vida profesional. Los seguimos y observamos cómo en este nuevo escenario la variedad de asuntos que ambos tratan ha cambiado: existe menos amplitud de temáticas y, por descontado, si hace aparición otro compañero con el que no mantengan una relación cercana limitaran el flujo de contenidos reservados. La razón por la que actúan de esta manera es porque así lo requiere la lógica del contexto o, mejor dicho, el respeto o mantenimiento a la integridad del mismo. Y este proceso se repite con los contenidos privados desplegados en la Web: atienden a una determinada lógica de usos y convenciones que, ante todo, subrayan los deseos y necesidades comunicativas del sujeto en cada momento.

Así pues, cuando hablamos de integridad contextual nos referimos a la lógica en los flujos de información desplegados en un determinado escenario, contenidos adecuados y pertinentes que permiten que la comunicación se lleve a cabo sin que se produzcan contradicciones con la naturaleza del mismo, ni restricciones en el proceso comunicativo. En cada momento concreto, en cada cruce de coordenadas particular, los intercambios de información vienen delimitados por una serie de convenciones que cambian en función de los factores que configuran el escenario, como, por ejemplo, los agentes implicados, los usos culturales correspondientes, las necesidades del sujeto… etc. Es por ello que diferentes personas, pertenecientes a culturas diversas desplegarán, en el mismo escenario, cantidades distintas de datos privados, sin sentir por ello que su intimidad y vida privada ha sido vulnerada. En suma, el marco proporcionado por Nissenbaum actúa dentro de las fronteras normativas de un determinado contexto, pautas que subrayan los deseos y el poder de decisión y control de los

sujetos, valorando el nivel de protección que se considera deseable en cada escenario.

Esta peculiaridad hace que dicha aproximación resulte muy apropiada para solventar la problemática derivada de las diversas nociones culturales de intimidad y vida privada que se dan en los distintos países y que confluyen en este espacio global y sin fronteras que es Internet, simplemente enarbolando la bandera del respeto a las leyes y usos sociales de cada área geográfica. Refuta, asimismo, la idea de que solo por el hecho de que los usuarios emplacen cierta información privada en los espacios públicos mediados deban perder todas las expectativas de control, poniendo en valor esa facultad del individuo de potestad sobre sus propios datos personales y que completa el derecho a la intimidad.

Resulta necesario clarificar en este punto, que cuando eludimos a «normas específicas que imperan en cada contexto» no nos referimos, exclusivamente, al entramado normativo jurídico, sino a pautas que emanan de otras fuentes como la convención social o de los usos y costumbres. Dentro de cada coyuntura a la que nos veamos expuestos las normas existen, tanto implícita como explícitamente, conformando y limitando comportamientos y perspectivas. Y, dado que todas las actividades que realizan los individuos tienen lugar en una pluralidad de escenarios distintos, los agentes involucrados, los tipos de información y los principios de transmisión presentes en cada entorno se combinan para dar forma de estas normas que gobiernan la información[425]. Consecuentemente, la idea central de la integridad contextual se fundamenta en la siguiente creencia:

> No hay arenas de la vida no gobernadas por normas informativas […] Prácticamente todo: las actividades que llevamos a cabo, los acontecimientos que suceden, las transacciones que realizamos… todo ocurre en un contexto no solo en cuanto a lugar, sino que conllevan unas convenciones y expectaciones culturales […] En nuestras actividades cotidianas la gente está en casa con sus familias, van a trabajar, buscan consejo médico, visitan amigos, consultan psiquiatras, hablan con abogados, van al banco, a centros de oración, votan, compran y más. Cada uno de esos escenarios o contextos está definido por un conjunto distinto de

[425] BARTH, A. (2006): «Privacy and contextual integrity: framework and applications» en *IEEE Symposium in security and privacy»,* pp. 184 y 186.

> normas que gobiernan sus varios aspectos como roles, expectaciones, acciones y prácticas[426].

En el ejemplo propuesto por Nissenbaum no hay ningún peligro evidente para la intimidad y vida privada del sujeto: la gente enlaza sus actividades diarias, pasando de manera anónima por ellas, sin que se pueda inferir un daño en el ámbito reservado del individuo. La información privada que este despliega es aquella que se considera pertinente y necesaria en cada coyuntura para completar sus actividades diarias y satisfacer sus necesidades de interacción social. Es por ello que definir una teoría general sobre la protección de la vida privada en cada una de estas situaciones concretas, esto es, sobre qué información personal se debe desplegar para evitar intromisiones indeseadas resultaría imposible, pero sí «debemos aceptar la existencia de dichos dominios, ampliamente enraizados en la experiencia común y gobernados por normas específicas»[427]. Si entendemos que el marco de protección de los datos privados responde a la integridad contextual, una trasgresión de las normas que regulan el dicho escenario supondría un quebrantamiento de la intimidad y vida privada. En este sentido, Helen Nissenbaum da un paso más en la definición del bien jurídico protegido por el derecho a la intimidad y vida privada, subrayando que no se trata solo una necesidad de secreto y control de la información, sino «un derecho al apropiado flujo de información personal»[428]. No obstante, se ha de tener en cuenta que dicha infracción puede estar justificada en contables ocasiones como, por ejemplo, a través de una orden judicial, si se entiende que los hechos que se dan cita puedan ser constitutivos de delito.

El respeto a las normas contextuales resulta esencial en los entornos digitales dado que deben dar forma y respaldar los flujos de datos que conforman cada escenario. Por ende, de igual manera que las pautas de comportamiento cambian en función de cada situación específica, las normas que gobiernan la incursión de datos en los entor-

---

426 NISSENBAUM, H. (2004): *Op. cit.,* pp. 119 y 137.

427 Al hablar de esta pluralidad de dominios Nissenbaum hace referencia a los trabajos de Van der Hoven, J. (1998): «Privacy and the varieties of informational wrongdoing», en *Austr. Journal of Professional and Applied Ethics*, vol. 1, n. 1, pp. 30-43. (2001): *Privacy and the varieties of informational wrongdoing*, p. 430;

428 NISSENBAUM, H (2010): *Op. cit.,* p. 127.

nos digitales también varían, indicando hasta qué punto el individuo puede desplegar ciertos contenidos. Del mismo modo, señalan cuándo el amparo de nuestra vida privada es susceptible de ser dañada, algo que se produciría si las normas de información que rigen el contexto son contravenidas, bien sea por nuestra propia acción o por aquellas emprendidas por otros agentes involucrados en el intercambio comunicativo. El respeto a estas cláusulas resulta crucial, más aún teniendo en cuenta la habilidad que poseen las tecnologías digitales para agregar, almacenar, procesar, analizar y transmitir cantidades ingentes de información sobre un individuo concreto, catalogándole en las gigantescas bases de datos que operan en el ciberespacio.

3.1 LAS NORMAS CONTEXTUALES O DE INFORMACIÓN DEL CONTEXTO

Centrémonos ahora en los ejes referenciales que guían el intercambio comunicativo. Las normas contextuales o de información dictaminan qué tipo y qué cantidad de datos privados son relevantes o resulta apropiado revelar en función de la coyuntura, así como a cuántos interlocutores y escenarios debe fluir. Proporcionan, por tanto, información sobre los límites hasta los que es pertinente desplegar ciertos datos personales y, de ser infringidas, estaríamos frente a una invasión de nuestra vida privada. En definitiva, podemos afirmar que son aquellas que promueven el mantenimiento de una cierta coherencia en los flujos informativos que dan forma a cada escenario concreto.

En cuanto a su procedencia, existe un número ilimitado de posibles fuentes que incluye la historia, la cultura, la ley o la convención, entre otras. Nissenbaum las agrupa en dos clases normativas generales:

1) las «normas de pertinencia» o «de propiedad de la información»
2) de «distribución» o «de flujo de información»

La integridad contextual se mantiene cuando ambas normas son respetadas, por el contrario, se entiende que se habrá producido una vulneración si una sola de ellas es quebrantada en un momento dado[429].

---

[429] ZIMMER, M. (2007): *Op. cit.,* p. 11.

3.2 LAS NORMAS DE PROPIEDAD O PERTINENCIA DE LA INFORMACIÓN

Son las que «circunscriben el tipo o naturaleza de información sobre los individuos que, en un determinado contexto, se considera es aceptable, esperado o, incluso, demandado sea revelado»[430]. En otras palabras, definen en qué escenarios y bajo qué condiciones resulta apropiado compartir ciertos datos. A modo ilustrativo, observamos cómo en una visita al médico se considera oportuno que el individuo aporte datos sobre su condición física o los medicamentos que toma, pero no esperamos que el doctor nos hable acerca de su salario. De igual modo, tampoco sería apropiado que se nos requiriera cierta información sobre nuestro estado de salud en nuestro lugar de trabajo, a no ser que estuviese justificada o fuese necesaria para desempeñar dicho cargo.

En definitiva, estas normas que Thompson denomina «de corrección»[431] versan sobre «lo que se considera correcto que delimite nuestros actos: las conocemos, contamos con ellas y actuamos sobre la base de las mismas» [432]. Tal vez por ello, bien podrían denominarse, igualmente, «de lógica del contexto», «de concordancia» o, más comúnmente, «de decoro». Su naturaleza es, por tanto, variable y, como mencionábamos en el ejemplo de los dos amigos, en función de la situación se tornan más o menos abiertas. De este modo, en una conversación entre colegas la información personal fluye libremente y las normas son más flexibles que en una clase o en una entrevista de trabajo, lugares en los que el flujo de información privada adecuado es regulado más estrictamente[433]. Es por ello que las pautas aplicables en un momento determinado no necesariamente pueden aplicarse en otro: «lo que se considera correcto como las pautas de flujo de información que se aplican en la relación médico-paciente no son necesariamente las mismas que se aplicarían en relaciones de amistad o entre empleados y empleadores»[434]. Este hecho viene a subrayar que no es dable identificar información privada con datos privados. Dado

---

430 NISSENBAUM, H. (2004): *Op. cit.,* p. 120.
431 THOMPSON, J. B. (2011): *Op. cit.,* p. 31.
432 Ibídem.
433 NISSENBAUM, H. (2004): *Op. cit.,* p. 120 y 121.
434 THOMPSON, J. B. (2011): *Op. cit.,* p. 31.

que no hay lugares fuera del amparo de las normas de información, estar en el más público de los lugares no significa que debamos dejar fluir todos nuestros datos privados o que todo esté legitimado en términos de nuestra información personal, porque «incluso en un espacio público por antonomasia como sería la calle [argumenta Nissenbaum] sentiríamos que se están entrometiendo en nuestra vida privada si un desconocido nos pregunta por nuestros nombres»[435].

Las leyes de propiedad de Nissenbaum parten de las aproximaciones filosóficas enunciadas por James Rachels en su célebre opúsculo: «Why privacy is important», quien estableció que las distintas relaciones humanas se encuentran parcialmente definidas, por distintos patrones que indicarían la cantidad de información que se comparte en cada coyuntura. En este sentido, la visión de Rachels reclama una adecuada protección de la vida privada, otorgando al ciudadano el poder de compartir información discriminadamente, capacitándole no solo para determinar cómo de cercana es la relación con los otros, sino la naturaleza de sus relaciones: «En cada caso, la clase de relación que cada individuo tiene con otro envuelve una concepción de cómo es apropiado comportarse con él y la clase y grado de conocimiento concerniente sobre cada uno que es apropiado para ellos»[436].

3.3 LAS NORMAS DE DISTRIBUCIÓN O DE CORRECTO FLUJO DE LA INFORMACIÓN

Las normas de distribución o de flujo de la información se refieren al movimiento o transferencia de datos de un escenario a otro en función de la finalidad a la que estos se destinan, es decir, establecen los límites que evitan la distribución abierta e indiscriminada de la propia información si no se cumplen ciertos requisitos. Nissenbaum comparte aquí el pensamiento de Ferdinand Schoeman en «Privacy: philosophical dimensions of the literature», quien arguye que los individuos mantienen diversas relaciones con diferentes personas en función de las coyunturas, por lo que «obtener información de una

---

435 NISSENBAUM, H. (2004): *Op. cit.*, p. 121.

436 RACHELS, J. (1975): «Why privacy is important», en *Philosophy & Public Affairs,* vol. 4, n. 4, pp. 323-333.

situación e insertarla en otra puede constituir una violación»[437]. Volviendo al ejemplo anterior, asumimos que lo que le contamos a nuestro médico es confidencial, por lo que bajo ningún concepto esperamos que lo comunique a otros sin haber sido informados, ni haber dado nuestro consentimiento explícito. Es por ello que «si nuestro historial médico apareciera en un sitio electrónico y se ofreciera a la venta sin nuestro consentimiento, entonces la norma de distribución o flujo de información ha sido claramente violada»[438].

Siguiendo, pues, las normas de distribución, el contexto de una conversación con un amigo cercano permitiría un mayor flujo y un tipo más amplio de información privada desplegada: nuestro día a día, opiniones políticas, emociones, experiencias sexuales… etc.; si bien, estas prevendrán a nuestro interlocutor de distribuir dicha información a una tercera persona.

3.4 LA APLICACIÓN DE LA INTEGRIDAD CONTEXTUAL PARA LA PROTECCIÓN DE LAS INFORMACIONES PRIVADAS EN LOS ESPACIOS PÚBLICOS MEDIADOS DIGITALES

La teoría de la contextual integridad está diseñada para considerar cómo la introducción de una nueva tecnología en un determinado contexto cambia las normas que gobiernan el flujo de información, lo que significa que es capaz establecer qué datos son o no pertinentes en cada contexto, aunque se trate de un escenario digital. Afirma la autora al respecto:

> Si la introducción de una nueva tecnología o práctica en un determinado contexto se encuentra en conflicto con las normas de flujo de información establecidas, una bandera roja es desplegada, indicando que la integridad contextual ha sido violada[439].

---

437 SCHOEMAN, F. D. (1984): «Privacy: philosophical dimensions of the literature», en Schoeman, F. D. (ed.): *Philosophical Dimensions of Privacy*, Cambridge: Cambridge University Press, pp. 1-33;

438 THOMPSON, J. B. (2011): *Op. cit.,* p. 31

439 Nissenbaum, citada en ZIMMER, M. (2007): «*Op. cit.,* p. 2.

Desde la perspectiva propuesta por Nissenbaum, en la vida diaria la pertinencia de informaciones privadas en el espacio público está mediatizada por contextos sociales altamente granulados. En este sentido, la aplicación de ambas normas contextuales referiría, por tanto, a la información privada que es necesaria desplegar para satisfacer las interacciones sociales en un determinado escenario comunicativo. Zimmer lo ilustra con un ejemplo de la vida cotidiana:

> Cuando compramos en la droguería, no hay nada secreto inherente a este hecho: lo hago en público, el cajero comprueba lo que me llevo, quizás también la persona que está en la misma cola e incluso se puede grabar en un perfil de comprador. Pero eso no significa que el contenido de mi bolsa: unas vitaminas, algo para el pelo o para mi salud sexual sea divulgado a todo el mundo en la tienda, compartido con los compañeros de trabajo, familia o incluso gente que no conozco[440].

Es por ello que, aun advirtiendo que si un acto privado es conocido, se convierte *de facto* en un dato público, «el hecho de que la información sea, en cierto modo, accesible al público no disuelve, automáticamente, el interés individual por controlar cómo dicha información es diseminada»[441]. En este sentido, el correcto uso de las normas de propiedad y flujo de la información indicaría que esos datos no deben divulgarse más allá del entorno donde se ha producido el intercambio de información. Y, dado que estas informaciones juegan un papel necesario y pertinente en el escenario citado en el ejemplo y su introducción se encuentra justificada, no se habría producido una violación de la vida privada.

De la misma manera que sucede en las relaciones en el entorno físico, cada escenario virtual conlleva o está determinado por una serie de normas informativas destinadas a mantener la integridad del contexto. Así, del respeto de ambas normas se derivaría una protección integral de las informaciones privadas en entornos mediados, subrayando dos elementos clave: la capacidad de control de los datos por parte del usuario, sustentada en las normas de propiedad, y la importancia de respetar la finalidad inicial por la que dichos datos fueron

---

440 Ibídem., pp. 4-5.

441 MOZOROV, E. (2010): «e-outed. Review of Privacy in context», en *The Times Literary Supplement*, 12 de marzo de 2010: Disponible en: https://www.evgenymorozov.com/essays/review_tls_privacy. PDF. [14/04/2012]

desplegados, facultad recogida en las normas de distribución. Por citar un caso concreto que sortee la abstracción del enunciado, traeremos a colación el siguiente ejemplo: si introducimos unos datos en Internet bajo unas condiciones determinadas estos no deberán ser usados para otros propósitos distintos a los que justificaron su volcado, algo que sucede, por ejemplo, en el caso del perfilado de usuarios o de las aplicaciones de las redes sociales. Este hecho, del todo ilícito, constituiría, bajo las lentes de la integridad contextual, una violación flagrante de nuestra intimidad y vida privada.

4. LA PROTECCIÓN DE LA INTIMIDAD Y VIDA PRIVADA EN ENTORNOS DIGITALES EN FUNCIÓN DE SU DIMENSIÓN SOCIOTÉCNICA

A pesar de su novedad, no queremos dejar pasar la ocasión de mencionar una novedosa aproximación a la problemática que nos ocupa, defendida por los investigadores Petra Ilyes y Carsten Ochs: se trata de la protección de los datos personales en función de su dimensión socio-técnica (*sociotechnical privacy*)[442]. Una revisión que valora la salvaguarda de las informaciones privadas en relación no solo a los contextos y a su pertinencia en el espacio público, como ocurre con la teoría de la integridad contextual, sino que acentúa la importancia de dos factores concomitantes en la comunicación mediada: los usos sociales y el papel desempeñado por las herramientas tecnológicas[443].

Esta concepción parte de la base de que, en la actualidad, «tecnología y privacidad son nociones interrelacionadas que deben analizarse conjuntamente»[444]. Partiendo de las premisas de Nissenbaum, la protección de la intimidad y vida privada se ha convertido, hasta cierto punto, en una cuestión que depende de flujos de información, pero estos flujos dependen a su vez de las herramientas tecnológicas, por

---

[442] ILYES, P. y OCHS, C. (2013): «Sociotechnical Privacy. Mapping the Research landscape», en *Tecnoscienza, Italian Journal of Science & Technology Studies,* n. 4, vol. 2.

[443] Ibídem., p. 75.

[444] Friedewald, M. y Pohoryles, R. J., (2013): «Technology and privacy», en *Innovation: The European Journal of Social Science Research*, n. 26, vol. 1-2, p. 5.

cuanto los procesos técnicos de procesamiento de datos dan forma, de manera decisiva, a dichos flujos de información[445]. La dimensión socio-técnica recoge la mezcolanza de las teorías coevolutivas de Latour con los axiomas Nissenbaum, así como de Boyd y Ellison, quienes definen estos sistemas socio-técnicos como de aquellos en los que «los factores sociales y técnicos dan forma el uno al otro»[446].

Así pues, los autores de esta revisión de las teorías contextuales creen más apropiado referirse a la dimensión socio-tecnológica de la vida privada en los contextos públicos mediados y en los que los procesos de manejo de datos personales tienen un papel protagonista.

Aunque esta nueva concepción se encuentra todavía en su estadio más inicial, pues fue enunciada por primera vez a finales de 2013, actualiza de manera eficaz los postulados de Nissenbaum toda vez que se consolida como una de las aproximaciones más interesantes para desarrollar sistemas de protección de la intimidad y vida privada de los usuarios de las Tecnologías de la Comunicación y la información.

5. REFLEXIONES SOBRE EL CAPÍTULO

Una de las consecuencias más importantes de la adopción social de las tecnologías, ya lo adelantaba McLuhan, es la transformación de la cultura[447] y, en este sentido, tanto la concepción como las atribuciones de lo que se considera vida privada, lejos de mantenerse estáticas, han visto alteradas su substancialidad. Lo mismo sucede con los planteamientos de amparo tradicionales, ligados a la demarcación de un espacio de no intromisión por oposición al ágora pública, cuya eficacia se torna pretérita tras la aparición de las tecnologías digitales. En este escenario, uno de los mayores desafíos que nos plantean las tecnologías es definir qué debe quedar protegido y qué se considera intromisión.

---

445 NISSENBAUM, H. (2004): *Op. cit.*, p. 120.

446 ELLISON, N. B. y BOYD, D. (2013): «Sociality through social network sites», en DUTTON, W. H. (ed.) *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press, p. 166.

447 MCLUHAN, M. (1964): *Understanding Media. The Extensions of Man*, California: McGraw-Hill, p. 7.

Para entender el proceso que nos lleva a dibujar semejante premisa, previamente hemos esbozado cómo desde las primeras concepciones hasta la actual visión normativa la protección de la intimidad y vida privada del individuo se ha centrado, primordialmente, en la distinción entre el ámbito privado por oposición a lo público, perdiéndose en delimitaciones conceptuales acerca de lo que incumbe a cada esfera y revelándose, a la postre, ineficiente en escenarios reales donde esta distinción no es meridiana. Desde esta perspectiva, la mayoría de aproximaciones centran su estudio en la atribución de competencias a uno u otro ámbito, observando la problemática a través de las lentes de las intromisiones, ya sean producidas en la esfera privada o, por el contrario, por la desaparición del ágora pública a favor de lo personal. Este movimiento oscilatorio ha propiciado la articulación de un espacio intermedio, un área de atribuciones indefinidas que no resuelve el dilema sobre qué se considera o no intromisión en la intimidad y vida privada.

Nos encontramos, pues, ante una problemática de hondo calado en el que la dialéctica esfera privada y esfera pública revela conceptos meramente descriptivos, pero poco útiles en última instancia. Como consecuencia, se equipara erróneamente intimidad y vida privada con esfera privada, lo que provoca que las informaciones privadas emplazadas fuera del ecosistema reservado del individuo no sean consideradas legítimas de ser protegidas. ¿Cómo podemos proteger entonces esos datos privados que aparecen en los espacios públicos recreados gracias a la mediación de las tecnologías digitales?

A la vista de la base teórica aportada no resulta incoherente afirmar que la clásica demarcación de «lo privado» por oposición a «esfera pública» posee un alto valor descriptivo pero se revela ineficiente para abordar una salvaguarda efectiva al no contemplar muchas de las intromisiones producidas en los espacios públicos mediados digitales. Igualmente, el carácter público del lugar donde se emplacen los instrumentos técnicos no es un elemento determinante para excluir, *per se*, un supuesto de intrusión ilegítima en la intimidad y vida privada[448].

No significa esto que la barrera entre «lo privado» y «lo público» se haya diluido, dado que convenimos en que, como es connatural a su esencia, la naturaleza de lo privado se desvanece en el momento en que es hecha pública. Pero sí observamos, no obstante, cómo han

---

[448] MEDINA GUERRERO, M. (2005): *Op. cit.,* pp. 84-85.

aflorado una variedad de escenarios cuyos elementos constitutivos provocan que estas diferencias no aparezcan claras ni meridianas, algo que no es nuevo del entorno digital pero sí se ha visto acentuado tras la popularización de las tecnologías digitales. Es por ello que resolvemos abordar la protección de la intimidad y vida privada desde otras perspectivas más acorde a los novedosos escenarios creados por las tecnologías, centrándonos en las aportaciones conceptuales que parten del valor relativo de la intimidad y vida privada en función del escenario comunicativo, de las pautas de comportamiento compartidas por una comunidad y la información proporcionada por las normas de cada escenario. Las teorías contextuales y primordialmente su máximo exponente enunciado por Nissenbaum, parten de la idea de que el respeto a la vida privada es cuestión de flujos informativos, corrientes que, en última instancia, aparecen modeladas no solo por los usos sociales sino por las propias herramientas tecnológicas, tal y como señala la elaboración teorética de Ilyes y Ochs, que no abordaremos en este trabajo.

Se revela aquí el axioma demostrativo según el cual si el despliegue de información depende de las normas concretas que regulan un contexto y este se configura, a su vez, en torno a una serie de flujos informativos determinados, obtener la información sobre dichas condiciones se revela necesario para decidir qué datos privados se pueden desplegar en cada momento. En otras palabras, la identificación de dichos escenarios, esto es, lo que nos permite averiguar qué datos privados son pertinentes o no, está directamente ligada a la obtención, por parte del usuario, de la información necesaria para interpretar el contexto. De este modo, además de recalcar el poder decisorio del individuo, la teoría de Nissenbaum subraya la importancia de la finalidad a la que se destinen nuestras informaciones como precepto fundamental, a la vez que consigue lidiar con las múltiples nociones de intimidad y vida privada imperantes en cada país o región geográfica.

En resumidas cuentas, esta aproximación no hace sino subrayar la importancia que un correcto flujo de información tiene en la protección de la intimidad y vida privada, capacitando al individuo para ejecutar la ya mencionada autodeterminación informativa y, por extensión, sus derechos democráticos. Un ciudadano informado es capaz de llevar a cabo, de manera activa, su potestad sobre sus informaciones privadas y personales y, en definitiva, sus derechos a la inti-

midad y vida privada, valorando, en consecuencia, cuándo desplegar cierta información sin que eso suponga un riesgo para la preservación de su ámbito reservado.

Con todo, la realización práctica de estos planteamientos chocará, como veremos en el subsiguiente análisis, con un problema de base: el individuo no obtiene la suficiente información para interpretar las normas que operan en los escenarios, por cuanto los flujos de información no son transparentes e implican un grado de complejidad que dificultan la comprensión u posterior toma de decisiones.

ACLARACIÓN:

No obstante, antes de sumergirnos en el examen más pormenorizado de las propensiones delineadas resulta preciso aportar una aclaración para no perder la perspectiva. En las páginas sucesivas nos inmiscuiremos en un aspecto negativo de las redes sociales, por lo que mantendremos la visión centrada en una atribución que, por definición, ya es censurable en tanto que la definimos como injerencias en el ámbito protegido del individuo. Sin embargo, esta dimensión refleja solo una parte de toda la realidad que representa el progreso tecnológico; una consecuencia indeseable que, si bien es preciso minimizar, no debe extrapolarse para calificar u oscurecer los beneficios aportados. Por ello y entendiendo que no haríamos justicia si calificáramos bajo la misma óptica el indudable conjunto de ventajas que nos aportan las herramientas de Internet, pedimos al lector que no pierda esta referencia durante la lectura del presente estudio, ya que, en ningún modo, esta faceta perversa debe estigmatizar al todo.

En otro orden de cosas, aunque durante nuestro análisis podremos observar cómo estas aplicaciones de la Web semántica contravienen frecuentemente el paradigma de la integridad contextual enunciado por Nissenbaum, no será hasta el apartado *Discusión* cuando estudiemos en profundidad este hecho. Vayamos primero, por tanto, a esos flujos de información que promueven un terreno propicio para la emergencia de intromisiones en Internet.

PARTE III

DESARROLLO DE LA INVESTIGACIÓN

CAPÍTULO V. LA VULNERACIÓN DE LA INTIMIDAD Y VIDA PRIVADA EN LAS REDES SOCIALES

SÍNTESIS

Proseguiremos nuestro análisis esbozando, a grandes rasgos, en qué consiste uno de los fenómenos que mejor resume la esencia de la Web 2.0: las redes sociales. Abordando su estudio a través de su funcionamiento, estructura, posibilidades y naturaleza de las interacciones que en ellas se producen, hemos descubierto cómo encarnan a la perfección la filosofía que impregnaron los inicios de toda esa Red de redes que es Internet: un ente libre, sin restricciones, descentralizado y con infinitos focos de acceso a la información. En su vertiente negativa, no obstante, nos vemos impelidos a desvelar cómo este fenómeno, de alcance global, también se halla en el ojo del huracán debido a los peligros que entraña en lo referente a la protección de la intimidad y vida privada de los individuos. Concretamente, la complejidad para controlar los propios datos personales, así como la exposición continúa de la identidad son dos factores que vuelven transparentes a los usuarios quienes, en muchas ocasiones, ni siquiera son conscientes de dicho proceso. Es por ello que, desde su propagación de manera mundial hasta el momento actual, las implicaciones de las redes sociales en la preservación y concepción de nuestro recinto privado conforman, con diferencia, la problemática más estudiada desde el ámbito científico y la que más repercusión ha adquirido en medios de comunicación. Sepamos ahora por qué.

1. INTRODUCCIÓN: LAS REDES SOCIALES Y LA PROTECCIÓN DE LA VIDA PRIVADA

Los pensamientos secretos
están pensados para diarios íntimos,
no para la Web

Jens Winther y Jesper Balslev, *Weblogs*[449]

La interconexión, el contacto con otros individuos, el intercambio comunicativo… todas estas facetas forman parte ineludible de nues-

---

[449] WINTHER, J. y BALSLEV, J. (2004): «Weblogs», en *PC Cuadernos Técnicos*, n. 19, mayo de 2004, p. 71.

tra naturaleza humana. Y ello explica que, desde los albores de la humanidad, el individuo se haya agrupado, creado asociaciones e impulsado sociedades u otras formas asociativas destinadas a compartir intereses y experiencias con iguales. La novedad, sin embargo, existe, y es aquella que introducen las tecnologías digitales: la que se refiere a las comunidades fomentadas por la interconexión mediada, capaz de posibilitar que los vínculos entre actores adquieran un alcance global. Este hecho distintivo hace surgir una nueva comunicación que no conoce fronteras, transformado nuestras vidas e imprimiendo un rasgo diferenciador a la sociedad en la que vivimos. Empero, también genera una coyuntura respecto a la cual aún no sabemos cómo actuar y que provoca la emergencia no solo de novedosos usos sociales, costumbres y nociones culturales, sino que pone en entredicho la concepción y protección de ciertos aspectos fundamentales del ser, tales como la demarcación de su recinto privado.

Una de las áreas de estudio que más artículos científicos e informaciones periodísticas ha protagonizado en los últimos años es, sin duda, la referida a los cambios introducidos por la integración de las herramientas digitales en nuestros procesos comunicativos. Y dentro de dicha transformación, la forma de interactuar de los individuos, la recolección de datos e informaciones privadas, así como la reconcepción de lo que debe ser mostrado y lo que no, ha movido el foco de análisis hacia el estudio de las redes sociales.

Este interés se ve incrementado por otras muchas razones: en primer lugar, lo que distingue a las redes sociales de otros espacios anteriores a la Web 2.0 es que representan una esfera social única, altamente mediada, donde una gran cantidad de datos personales se acumulan y son agregados[450]. La inclusión de dichas informaciones no es opcional. Por su naturaleza, las redes sociales digitales necesitan de los datos de los usuarios para seguir creciendo, por lo que los perfiles constituyen páginas personales únicas en las que el usuario puede construir su propio ser[451] y en las que su elaborado diseño anima a

---

[450] GOVANI, T. y PASHLEY, H. (2005): *Op. cit.*

[451] La frase original de Suden es: «*type [themselves] into being*», esto es, «escribir su propio ser», y se refiere a la plasmación y contrucción del ser virtual a través de la información que el usuario escribe en su red social, por lo que hemos decidido interpretar la palabra «type» como «contruir». Sundén, J.

introducir más contenidos, aumentando las interacciones que actuarán como verdadero carburante de la red social. Estos datos pueden ser fácilmente copiados, distribuidos más allá de la plataforma en la que fueron introducidos, replicados, sacados de contexto[452] y usados para otros fines. Finalmente, a diferencia de las aplicaciones de la Web 1.0 los usuarios hacen explícita su red social[453], es decir, muestran sus amistades, conocidos, familiares… contactos en definitiva, indicando quienes conforman su entorno y, por omisión, quienes no, lo que permite que las redes sociales se vayan articulando en función de estos lazos a la vez que se torna visible la realidad que rodea al sujeto. Incluso los vínculos menos consolidados también ayudan a sustentar el tejido que mantiene viva la red social[454]. Todo ello, alimentado por el hecho de que las redes sociales digitales dan la impresión de ser un espacio semipúblico en el cual uno puede actuar con su círculo social como lo haría en la esfera privada. Coyunturas, todas las citadas, novedosas y difusas que al sumarse provocan que los individuos no tomen las debidas protecciones y se dejen arrastrar por la dinámica de estas herramientas, anteponiéndolas a la salvaguarda de su espacio confinado.

2. LAS IMPLICACIONES PARA LA INTIMIDAD Y VIDA PRIVADA: PRINCIPALES PELIGROS DE LAS REDES SOCIALES

Como adelantábamos en el apartado precedente, la facilidad con que los usuarios desvelan su dimensión más reservada constituye una problemática que se ha incrementado en las redes sociales respecto a otro tipo de servicios de Internet. A la vez, la percepción general de los individuos sobre los riesgos que esta práctica involucra parece haberse desvirtuado; aun cuando su capacidad para controlar y configurar de forma adecuada dichas herramientas es limitada. Este ex-

---

(2003): *Material Virtualities: Approaching Online Textual Embodiment*, New York: Peter Lang, p. 3.

452 BOYD, D. (2006): *Op. cit.*

453 BOYD, D. y ELLISON, N. B. (2007): *Op. cit.*

454 Es lo que se denomina Teoría de los lazos débiles. HAYTHORNTHWAITE, C. (2005): «Social networks and Internet connectivity effects», en *Information, Communication & Society*, vol. 8, n. 2, pp. 125-147.

tremo no conlleva que los ciudadanos se sientan seguros en Internet. De hecho, según las opiniones recogidas por el *Eurobarómetro Especial 359, Attitudes on Data Protection and Electronic Identity in the European Union,* aunque el 54% de los usuarios se declara informado de las condiciones de la recogida de datos y del uso que posteriormente se le da a estos, solo un 26 % siente que controla sus propias informaciones[455].

La preocupación de usuarios y expertos tiene una base real, puesto que son muchos los peligros detectados a raíz de la generalización del uso de estas herramientas digitales. Sólo por citar algunos, podemos señalar:

— La obtención de informaciones personales de los miembros de las redes sociales, así como la usurpación de datos de carácter sensible o relativos a aspectos económicos.

— La suplantación de identidad, reconstruyendo con nuestros datos y fotografías nuestra persona digital. Según la AEPD, cada vez es más frecuente que usuarios que nunca se habían registrado en redes sociales *online*, comprueben como, en el momento en el que intentan acceder, su identidad digital ya está siendo utilizada[456].

— La obtención de informaciones del usuario para crear un público objetivo al que destinar la publicidad hipercontextualizada: una práctica que roza la ilegalidad puesto que, para poder personalizar dicha publicidad deben examinarse antes los datos y preferencias que los participantes introducen en la plataforma bajo otras condiciones.

— El rastreo mediante la instalación y uso de *cookies* que permiten a la plataforma conocer cuál es la actividad del sujeto tanto dentro como fuera de la misma, sin siquiera advertirle. Mediante estos programas específicos se puede detectar el lugar desde el que el interactor accede, el tiempo de conexión, el dispositivo de acceso, las páginas más visitadas, el número de «clics» realizados e infinidad de informaciones relativa a la navegación del usuario.

---

[455] European Commission (2011): Special Eurobarometer 359. *Op. cit.*

[456] AEPD e INTECO (2009): *Op. cit.,* p. 11.

— La revelación de la identidad real del interactor. Dado que las redes sociales tienden a extraer multitud de datos personales, es posible averiguar el nombre y apellidos reales de los individuos mediante la comparación de dicha información a través de la Red, incluso cuando estas aparecen parcialmente ocultas. Encontrar datos personales está en la mano de cualquier persona con competencias digitales y un conocimiento medio: basta con cruzar los resultados obtenidos tras las búsquedas públicas en motores de Internet y otras herramientas de la Web 2.0.

— La indexación no autorizada por parte de buscadores de Internet y el acceso ilimitado a informaciones a través del perfil. La existencia de perfiles públicos induce a que cualquier usuario de Internet o de la propia comunidad virtual pueda acceder a datos de carácter personal ajenos sin que el propietario de dichos contenidos pueda denegar o dar su consentimiento expreso.

Además de estas situaciones, altamente recurrentes, podríamos citar un largo etcétera. No en vano, Max van Manen equipara estas particulares comunidades virtuales a las «tecnologías del Momo», en meridiana referencia al mito de las ventanas del hombre: «proporcionan un acceso directo a lo que es más interno y simultáneamente pueden tener el efecto de trivializar y difundir ampliamente lo privado en planos dispersos de lo público»[457]. Un juego en el que hemos entrado los propios usuarios, en tanto que, seducidos por los beneficios percibidos no sopesamos los riesgos de la información personal revelada.

Por ello, pese a que estas herramientas sociales favorecen la interacción entre individuos promoviendo «el mantenimiento y creación de capital social»[458], son muchas las voces críticas que han abordado cómo su proliferación e imbricación en la sociedad desvelan algunas contraprestaciones que desbordan los preceptos tradicionales aplicables a la salvaguarda de la intimidad y vida privada. No obstante, antes de comenzar a abordar en detalle el alcance de dichas contra-

---

457 VAN MANEN, M. (2010): «The Pedagogy of Momus Technologies: Facebook, Privacy and Online Intimacy», en *Qualitative Health Research*, vol. XX, n. X, pp. 1-10, pp. 1-3.

458 ELLISON, N. B., STEINFIELD, C. y LAMPE, C. (2007): *Op. cit.*

prestaciones, veamos cuales son las principales dinámicas de una red social en Internet.

3. FUNCIONAMIENTO DE UNA RED SOCIAL: LOS CONTENIDOS PERSONALES COMO ELEMENTOS ESTRUCTURANTES DEL SISTEMA

La columna vertebral de las redes sociales se compone de los perfiles visibles de los miembros, en los que se muestra una lista de contactos que son también participantes del sistema. Estos perfiles son páginas propias y únicas donde cada usuario se da a conocer ofreciendo una serie de informaciones identificativas para que otros integrantes del sistema puedan localizarles y contactar con ellos. Para satisfacer dicho objetivo, cuando un sujeto decide darse de alta en una red social debe rellenar en primer lugar un formulario (el legendario apartado «sobre mí») cumplimentando una serie de preguntas que configurarán su «carné» de pertenencia a la comunidad e indicando, entre otros, datos referentes a su edad, sexo, población, profesión, intereses y creencias, así como una descripción de sí mismo. Deberá, además, añadir una foto que servirá para que otros participantes le encuentren y, como requisito imprescindible, se le solicitará que enlace su perfil a una dirección de correo electrónico mediante la cual podrá acceder a su cuenta, así como localizar a los amigos, conocidos, compañeros de clase, de trabajo… etc. que figuren en la lista de direcciones de dicho correo electrónico. Cuantos más datos se suministre al sistema, más fácil será que la plataforma acote y proporcione contactos relacionados o que puedan ser de interés al usuario.

Este proceso, que le permitirá ser identificable por otros habitantes de la comunidad y crear su red de enlaces, equivale en realidad a cumplimentar una entrada en una base de datos donde quedará catalogado. Del mismo modo, nos revela una de las peculiaridades propias de este entorno y que constituye la base misma de su éxito: en las redes sociales son los usuarios los que «voluntariamente» hacen el trabajo de entregar sus propios datos a la plataforma. Esta es, afirma Byung-Chul Han, la principal fuerza de este *panopticon* digital emergente: «sus moradores mismos colaboran de manera activa en su

construcción y en su conservación, en cuanto se exhiben ellos mismos y se desnudan»[459].

El entrecomillado aplicado a la palabra «voluntariamente» no es accesorio. Aunque, a primera vista, los usuarios publican *motu proprio* sus datos y, por tanto, son los responsables últimos de esta acción, los efectos sobre su intimidad y vida privada pueden tener un alcance mayor al que consideran en un primer momento. Estas plataformas, que poseen una alta capacidad de procesamiento, se estructuran en torno a la transferencia de información mediante flujos de datos que los sujetos no conocen, ni son capaces de percibir, pero que están en la esencia misma del mecanismo de funcionamiento de las herramientas digitales. Igualmente, junto a los datos que introducen conscientemente el sistema es capaz de recolectar preferencias, gustos y otras informaciones de todo tipo, de cuya acumulación los individuos no son partícipes. Una ecuación que se complica si tenemos en cuenta las aplicaciones y otros servicios de terceras empresas que habitualmente se integran en estas redes, sin mencionar el hecho de que, en muchas ocasiones, permiten a los motores de búsqueda de Internet indexar los perfiles de los usuarios, en los que se encuentra su información de contacto y la de sus amigos. Prácticas, todas ellas, que pueden suponer un riesgo no percibido *a priori*. Y una vez que la información ha salido de los confines de la plataforma, el proceso de eliminación en la Web es muy complicado si no imposible.

La principal amenaza para los usuarios de las redes sociales recae, pues, no solo en la recopilación de datos que en ellas se realiza, sino en la formulación y estructura propia de estas comunidades. Si bien, sabemos que esta acumulación de datos no nace por generación espontánea sino que, en un primer estadio, parte de lo que el individuo o sus contactos etiqueten directamente en la citada base de datos personalizada. Razones que llevan a la Agencia Española de Protección de Datos a alertar de que el momento del registro es especialmente conflictivo, en la medida en que habitualmente no se configura correctamente el nivel de visibilidad del perfil, aun cuando se publica información sensible desde el inicio de la actividad en la red.

Asimismo, en el informe conjunto con INTECO, titulado: *Estudio sobre la privacidad de los datos personales y la seguridad de la infor-*

---

[459] HAN, B-C. (2013): *La sociedad de la transparencia*. Barcelona: Herder, p. 89.

mación en las redes sociales online, la AEPD destaca otros dos momentos en los se producen la mayoría de las injerencias en la intimidad y vida privada del sujeto:

> [Durante la] participación en la red como usuario, en la medida en que el grado de información, datos e imágenes publicados pueden ser excesivos y afectar a la privacidad, tanto personal como de terceros. […] Al darse de baja de la plataforma, en la medida en que el usuario solicite dar de baja su perfil, pero aún así continúen datos publicados por éste, o información personal e imágenes propias publicadas en los perfiles de otros usuarios[460].

Desde el punto de vista de las plataformas que gestionan estos servicios, la problemática es percibida de manera distinta. La recolección de datos que se da en todos estos momentos no constituye una desventaja para el uso del sistema, más bien al contrario, pues lo retroalimenta. Ni siquiera es considerado como un daño colateral que deba ser minimizado, dado que se encuentra en la base misma de la filosofía empresarial de las redes sociales. Y es aquí donde alumbramos el verdadero motivo que legitima, a través de la óptica del mercado, ese exhaustivo acaparamiento de contenidos privados: las informaciones de los usuarios se transforman en la materia prima de un negocio que, a pesar de ser percibido como gratuito, estamos pagando con la moneda de nuestra intimidad, una práctica que pasa inadvertida en numerosas ocasiones. Para justificar la contundencia de dicho dictamen, expondremos más en profundidad en qué consiste este particular negocio cuyo carburante se elabora a partir de la propia substancialidad humana.

3.1 EL NEGOCIO DE LAS REDES SOCIALES: LA MONETIZACIÓN DE LOS DATOS PERSONALES

Las directrices empresariales que subyacen a cualquier plataforma de redes sociales se resumiría en una frase: la acumulación de datos que requieren para funcionar conforma la materia prima que necesitan para financiarse, ya que su gestión se traduce en dinero. La aritmética es sencilla: Cuanto más elevada sea la cifra de participantes y

---

460 AEPD e INTECO (2009): *Op. cit.,* pp. 109-110.

más ricos y completos los perfiles creados, mayor capacidad tendrá la red de conseguir nuevos miembros y esto incrementará su valor como plataforma publicitaria y/o para la prestación de aplicaciones o servicios complementarios.

Desde esta perspectiva, las redes sociales representan la faz visible de un negocio perfectamente estructurado y en el que nuestras informaciones personales forjan el motor gracias al cual se sustentan, por lo que, para que la empresa resulte rentable, deben alcanzar una masa crítica de usuarios y así optimizar su explotación comercial. Si muchos individuos optan por usar una misma red para comunicarse, la financiación está asegurada dado que una de las ventajas primordiales de este tipo de plataformas consiste en la enorme capacidad de obtener beneficios económicos derivados de la publicidad y de las aplicaciones internas:

> La facilidad con la que los usuarios pueden anunciar o ser receptores de anuncios de productos y servicios es muy elevada si se compara con el mundo físico, ya que junto a la sencillez con la que se pueden comercializar productos y servicios a distancia, las redes sociales cuentan con una base de datos de usuarios (potenciales clientes) perfectamente segmentados por gustos y perfiles, lo que implica que las capacidades de éxito del procedimiento comercial sean muy altas[461].

En comparación con la búsqueda del público objetivo o *target* a cargo de los tradicionales estudios de mercado, estas herramientas ofrecen información de manera más precisa sobre las preferencias y propensiones de los individuos, encontrando nuevos nichos de posibles compradores sin apenas esfuerzo y de manera fiable[462]. Y esto es posible porque cuando señalamos nuestros gustos o indicamos que nos interesa un anuncio, en realidad estamos dejando una serie de pistas que delatan cómo somos y cuáles son nuestros hábitos de consumo. De este modo, las redes sociales han hecho realidad la utopía de la publicidad personalizada, convirtiendo al usuario en un potencial cliente sin que se percate.

Esta publicidad está tan focalizada que, aprovechando los servicios de localización, permite ofrecer anuncios a los usuarios de co-

---

[461] Ídem., p. 13.

[462] LACALLE, C. (2011): «La ficción interactiva. Televisión y Web 2.0.», en *Ámbitos*, n. 20, pp. 87-107, p. 100.

mercios cercanos a su situación geográfica[463], una posibilidad que se ha acrecentado bajo el uso de las redes sociales a través del móvil y teléfonos inteligentes (*Smartphones*). No obstante, si esta práctica es legal o no, es ya otra cuestión. Si bien los datos de geolocalización se necesitan para que el prestador de servicios pueda ofrecer cobertura, no deberían ser utilizados para introducir publicidad personalizada.

Figura 5.1 El negocio de la publicidad en la Web 2.0[464]

Este cambio se ha reflejado en las cifras de la inversión publicitaria destinadas a estas herramientas. Las redes sociales se han convertido en la brújula de las empresas de publicidad, así como de cualquier pequeño negocio que quiera publicitar sus productos o servicios de manera altamente eficiente. Y estas plataformas permiten, a su vez, rastrear a los consumidores latentes a través de sus distintas aplicaciones, comunidades y páginas más relevantes, en función del produc-

---

463 Algunos de los sitios de las redes sociales que empezaron a ofertar este servicio son Google Buzz, Facebook places, Tuenti sitios, Twitter y Foursquare aunque, actualmente, el uso de este servicio está ampliamente extendido.

464 Fuente: Display advertising technology landcaper, http://www.lumapartners.com/resource-center/

to que se quiera promocionar; observando, a la par, la acogida de los usuarios mediante el análisis de sus interacciones. De este modo, la información volcada por los sujetos provee de un gran poder predictivo en cuanto a propensiones y futuras actitudes. Es lo que comúnmente se conoce como «seguimiento o control a través de las herramientas sociales» (*social media monitoring)*. Esto revela que, paradójicamente, en el caso de las redes sociales su supuesta gratuidad económica es su máximo valor:

> Las bases de datos valen mucho dinero (…). Es el elevado valor de las bases de datos con información personal lo que hace que muchas compañías ofrezcan sus servicios online de forma gratuita. El precio a pagar, nos demos cuenta o no, es altísimo y lo pagamos con creces permitiendo el acceso y el uso de nuestra información personal con fines comerciales[465].

El dilema moral, no obstante, va más allá de etiquetarnos, segmentarnos y tornar nuestro estatus en el de posibles clientes. El peligro real recala en que, al mismo tiempo que quedamos agrupados en función de nuestros gustos y hábitos de compra, estas herramientas capturan informaciones personales que revelan mucho de nuestra identidad y cuya comparación puede, a la postre, conducir a la pérdida de anonimato del usuario. Incluso cuando los «individuos prefieren mantener en la intimidad algunos detalles como sus preferencias políticas o su orientación sexual»[466] los contactos propios pueden revelar informaciones que el usuario desea y cree mantener en secreto. Es así como lo que otrora se consideraba reservado al conocimiento del individuo y su círculo privado, se torna ahora colectivo mediante un cúmulo de informaciones personales ante las que un alto mando de la Stasi no se resistiría. Y todo ello sin mencionar el hecho de que, además, puede propiciar su rastreo, práctica que se lleva acabo de manera más frecuente de la que pensamos.

---

[465] ALCÁNTARA, J. F. (2008): *La sociedad del Control*, Barcelona: El Cobre, p. 195.

[466] HORVÁT E. A., HANSELMANN M., y HAMPRECHT. A. L. (2012): «One Plus One Makes Three (for Social Networks)», en *PLoS ONE,* vol. 7, n. 4.

En resumidas cuentas, la realidad que se esconde tras los servicios de redes sociales puede vulnerar la intimidad y vida privada de las personas en dos direcciones:

— Catalogando al usuario a través de sus intereses, predilecciones y características personales, lo que le convierte en público objetivo y, aunque permite su rastreo, no necesariamente le identifica con nombres y apellidos. Esta práctica, comúnmente denomina *targeting* y que traduciríamos por «creación de público objetivo», conforma uno de los mayores flancos de vulnerabilidad con los que se topa el interactor.

— Desvelando su identidad tras el rastreo, agregación y cruce de sus informaciones personales desperdigadas dentro y fuera de la plataforma y cuya triangulación permite imputar a los contenidos un nombre y apellidos. Dicha técnica, conocida como «seguimiento» (*tracking down*) constituye el mayor desafío al que se enfrenta el individuo cuando interactúa con las tecnologías digitales, dado que no se rastrea ya un identificativo numérico: directamente, se sigue la pista de la identidad real de un usuario. Y aunque este peligro ha existido desde las primeras aplicaciones informáticas, a diferencia de lo que sucedía en los primeros años de expansión de la Red, la interacción e integración de las herramientas Web 2.0 y, en concreto, de las redes sociales, permite que las posibilidades de éxito se multipliquen.

Bajo estas dos situaciones subyace una realidad aún más alarmante: desde el momento en que no es correctamente informado o acepta unas condiciones de uso que no se corresponden con la realidad, las armas con las que cuenta el interactor para mantener su dimensión privada a buen recaudo son escasas. Y lo mismo sucede con las posibilidades de resarcimiento pleno una vez que dichas intromisiones se han producido. El mensaje que se desprende de las políticas de protección de datos seguidas por las susodichas empresas no deja margen de error: el responsable último es el usuario.

3.2 LA TRAMPA DE LAS CONDICIONES LEGALES: LAS POLÍTICAS DE PRIVACIDAD[467] Y AUSENCIA DE RESPONSABILIDAD

Dado que cuando nos registramos en una red social se establece una relación de carácter comercial en la que estamos cediendo nuestras informaciones personales, los apartados que explicitan los acuerdos a los que deben atenerse ambas partes deberían tener un papel preeminente. Sin embargo, es este uno de los asuntos que más dudas suscita sobre la legitimidad del negocio que sustentan estas plataformas.

Desde el punto de vista de los mecanismos del mercado, nuestra vida privada es un punto negociable, un atributo humano susceptible de ser explotado económicamente en vez de un derecho inalienable. Partiendo de esta interpretación forzada de una dimensión propia de la naturaleza humana, las políticas de protección de datos equiparan «usuarios» a «consumidores», a la vez que paralelamente los «cosifica» al convertirlos en objeto de consumo. A este tenor, resulta pertinente realizar una aclaración: la mayoría de las plataformas de redes se crean en Estados Unidos donde la preservación de la intimidad se mide como protección de los derechos de los consumidores, óptica que estas empresas han transpuesto a todo el planeta, pero que choca con las concepciones normativas de otras zonas geográficas como, por ejemplo, la europea.

En el extremo contrario de la ecuación, encontramos que el individuo tiene poco margen de maniobra por cuanto no sabe o no comprende cómo se gestionarán sus datos. De hecho, aunque es cierto que las TIC democratizan las habilidades develatorias esto no se traduce en más información a disposición del usuario, ni significa que la que reciben no esté altamente mediada (que lo está por definición). Estas políticas de privacidad y de tratamiento de datos personales son meramente descriptivas y la única obligación que se les impone a las plataformas es que dichas cláusulas estén incluidas en un apartado de su sitio Web. En este sentido, las citadas disposiciones no siempre

---

[467] Aunque ya hemos comentado que en este estudio abogaremos por las voces «intimidad y vida privada» aplicamos aquí el anglicismo *privacidad* cuando nos refiramos a la expresión «políticas de privacidad». La razón es que es la locución mayormente aceptada para estos apartados y una denominación distinta llevaría a equívocos.

tienen entre sus objetivos resaltar las prácticas más controvertidas de las empresas, más bien al contrario: si se reseñan aparecen escritas en un lenguaje engañoso, poco claro e integradas en tal abundancia de datos que no hacen sino alentar la desinformación.

Las plataformas eluden así su responsabilidad ante la acción de cualquier usuario y ofrecen pliegos de condiciones que les eximen de cualquier contratiempo, toda vez que les permiten manipular los datos ajenos a su antojo. En otras palabras, a través de las condiciones de registro aceptadas por los miembros de la comunidad éstos ceden derechos plenos e ilimitados sobre la totalidad de contenidos que alojen en la plataforma, lo que significa que podrán ser explotados económicamente por parte de la red social. Y, una vez registrados, esto puede producirse en cualquier momento, es decir, no volverán a solicitar consentimiento para negociar con informaciones privadas. De este modo, trasladan toda la responsabilidad a los individuos quienes, en última instancia, deberán informarse acerca de lo que la empresa puede o no hacer con sus contenidos, tarea que no se presenta meridiana. A todo ello, se le suma el hecho de que uno de los mayores peligros de las redes sociales proviene no solo de la desprotección legal con que se encuentra el usuario, sino de que este tiene en cuenta solo las intromisiones procedentes de otros usuarios pero no las injerencias provocadas por la propia plataforma, de la que presupone que actuará dentro de la legalidad. Como botón de ejemplo, reparemos en uno de estos acuerdos de usuario para evaluar cómo funcionan y saber a qué nos referimos.

3.2.1 Términos y condiciones de uso del servicio: el ejemplo de LinkedIn

He aquí el tinglado de la antigua farsa
Benavente, *Los intereses creados* [468]

Cada vez que usamos cualquiera de las redes sociales que habitan el universo Internet, debemos aceptar una lista tediosa de términos y condiciones de uso como requisito ineludible para darnos de alta en el servicio. Estas cláusulas, comunes a todos los servicios di-

---

[468] BENAVENTE, J. (1907): *Los intereses creados*. Acto I: Prologo. Cátedra: Madrid.

gitales, es lo que se denomina genéricamente *Términos y condiciones de uso del servicio* y describen un acuerdo entre el usuario y la compañía en el que también se detalla cómo se gestionarán los datos personales, normalmente, en los apartados: *Política de privacidad* o *Política de protección/gestión de datos personales*. De este modo, cuando se utiliza el servicio se entiende que se han aceptado todas las normas del mismo, incluidos los términos de privacidad. Y es aquí donde encontramos las primeras irregularidades: Dicho asentimiento no siempre es explícito. Mientras que el usuario que se registra en Tuenti debe dar su consentimiento de manera activa, es decir, marcando una casilla que le da permiso para efectuar el registro, en Facebook dicha casilla nunca aparece, ni se menciona, sino que las condiciones se dan por leídas si el usuario decide abrir una cuenta.

A todos los efectos, no obstante, la aprobación de dichos acuerdos constituye más un mero trámite que una garantía legal. El usuario a menudo no es consciente de lo que está firmando, pero necesita sortear dicho obstáculo y dar su visto bueno para poder registrase. Desde la óptica de la empresa, este paso representa un acto simbólico que no nace encaminado a la aclaración de términos entre las partes implicadas, sino para satisfacer una imposición legal y justificar ciertas prácticas. Este hecho resulta constatable al observar que dichas políticas no están diseñadas para ser leídas: Son altamente complejas, el lenguaje usado contiene demasiadas ambigüedades como para saber, exactamente, qué sucede con los datos introducidos y tiende a ser farragoso. La ecuación se complica teniendo en cuenta que el interactor no siempre está familiarizado con los términos jurídicos de dichas declaraciones y, por tanto, no es capaz de comprender el alcance ni lo que implica su aceptación. De hecho, este concepto es bastante nuevo ya que, por ejemplo, nunca hemos tenido que firmar un acuerdo de usuario para una línea telefónica terrestre, pero sí debemos hacerlo si usamos un teléfono inteligente o un *kindle*.

Por su parte, el diseño tipográfico no es accesorio, sino que añade más dificultad. Suelen usarse fuentes difíciles de leer, cuerpos de letra pequeños y, a ser posible, en mayúsculas, propiciando que la tipografía se convierta en texturas más que en palabras y espacios. Finalmente, la extensión de dichas condiciones tampoco es desdeñable: si el

usuario leyera todo lo que acepta le llevaría un mes de trabajo, es decir, 180 horas[469].

Comparando algunas de las políticas de las redes sociales más profusamente usadas, observamos que existe un modelo más o menos común a todas ellas. Consultemos, a modo ilustrativo, uno de los acuerdos más sencillos, el correspondiente a la red social profesional LinkedIn. En el apartado *Condiciones del servicio. Licencia y garantía sobre los contenidos que facilites a LinkedIn,* leemos: «(Tú)[470] seguirás siendo el propietario, pero nos otorgas una licencia sobre el contenido y la información que nos proporciones» [471]. Concretamente:

> […] Entre LinkedIn y tú, eres el propietario del contenido y de la información que facilitas a LinkedIn en virtud de este Acuerdo, y puedes solicitar su eliminación en cualquier momento, salvo que hayas compartido información o contenidos con otras personas y no los hayan eliminado u otros usuarios los hayan copiado o almacenado. Asimismo, otorgas a LinkedIn un derecho no exclusivo, irrevocable, a nivel mundial, perpetuo, ilimitado, sujeto a cesión o sublicencia [sic], gratuito y sin canon para copiar, preparar obras derivadas, mejorar, distribuir, publicar, eliminar, conservar, agregar, tratar, analizar, utilizar y comercializar mediante todas las modalidades de explotación conocidas actualmente o descubiertas en un futuro cualquier información que facilites a LinkedIn, directa o indirectamente, incluido, sin que suponga limitación, cualquier contenido generado por los usuarios, ideas, conceptos, técnicas o datos de los servicios que tú facilites a LinkedIn sin ningún consentimiento adicional, notificación o compensación para ti o un tercero[472].

En una primera lectura, si es que hemos conseguido abordar esta declaración de una sola vez y sin marearnos, resulta curioso destacar el uso de la tercera persona del singular concordante con el nominativo «tú» en vez de el plural «usted» que sería esperable de un escrito legal. A todas luces, se trata de una argucia más que de un fallo de traducción intencionado; una estrategia encaminada a revestir de trivialidad el acuerdo y restar trascendencia al alcance de los principios firmados. El texto prosigue:

---

469 HOBACK, C. (2013): *Terms and Conditions May Apply*, Documental emitido en *La noche temática: control tecnológico*, La 2, 26 de octubre de 2013.

470 El énfasis me pertenece.

471 Acuerdo de usuario de LinkedIn: http://es.linkedin.com/legal/user-agreement

472 Ídem.

> En virtud de esta licencia, LinkedIn puede otorgar a otros Miembros o Visitantes acceso y compartir derechos sobre tu contenido e información de conformidad con este Acuerdo, con tu configuración y con el grado de contacto que tengas con ellos. En lo que se refiere a tu contenido de *SlideShare*, puedes escoger compartirlo con Miembros y Visitantes en virtud de la licencia de Creative Commons de tu elección[473].

En definitiva, podríamos resumir dicha cláusula en la siguiente frase: «LinkedIn se queda con todo para siempre», al igual que hace Google, Facebook, Pinterest… y un largo etcétera de servicios que la gente considera gratuitos. Consecuentemente, cuando introducimos informaciones de cualquier tipo en una red social no solo estamos perdiendo el control de los mismos, sino que se nos niega parte de nuestros derechos legítimos sobre dichos datos, un extremo peligroso cuando se trata de contenidos que deseamos mantener en privado. Y aunque el individuo sigue siendo el propietario del contenido, más que nada porque en el caso de aquellos relativos a la intimidad y vida privada nos referimos a un derecho irrenunciable, ha firmado una cesión de derechos de por vida. Volviendo a LinkedIn:

> Cualquier contenido e información que nos transmitas será por tu propia cuenta y riesgo. Al proporcionarnos contenido e información, declaras y garantizas que tienes derecho a hacerlo, que no es confidencial y que no viola ninguna ley, restricciones contractuales u otros derechos de terceros (incluido cualquier derecho de propiedad intelectual)[474].

Por supuesto, el usuario ostenta «la responsabilidad de mantener la información de perfil actualizada y que sea correcta». Además, aprueba que pueda compartirse con LinkedIn cualquier información adicional a través de sus aplicaciones, acuerdo que vincula, igualmente, a aquellas que utilice desde el móvil:

> Si usas una Aplicación de LinkedIn o navegas por un sitio Web que ha instalado un complemento, aceptas que se nos pueda remitir información sobre ti y tu uso de los Servicios, incluidos, sin que suponga limitación, tu aparato, tu operador de red móvil, tu proveedor de acceso a Internet, tu ubicación física o páginas Web que contengan complementos de LinkedIn que se cargan en tu navegador. […] Por último, al utilizar una aplicación descargable que te permita usar los Servicios, estás

---

473 Ídem.
474 Ídem.

> confirmando explícitamente tu aceptación de los términos del Acuerdo de Licencia del Usuario Final asociada con la aplicación en el momento de la descarga o instalación, o las modificaciones que puedan introducirse de vez en cuando[475].

En suma, tras aceptar los Términos de uso el individuo da permiso «informado» para que las plataformas puedan usar sus datos personales como deseen, incluso compartiéndolos con terceros y aun cuando dichas normas cambien sin previo aviso[476]. Es cierto que leer la «letra pequeña» que se acepta al registrarse en un sitio Web es algo que nadie suele hacer, pero dado que se firman estos acuerdos pueden llegan a aplicarse y, en la medida en que se ha tomado decisiones vinculantes, se supone que esas condiciones son válidas.

Este es, a grandes pinceladas, el panorama que encontramos en la madeja de redes sociales que pululan por el universo Internet. Dicho esto, cabe señalar que LinkedIn no es la empresa que más controversias suscita ya que al tratarse de una red social profesional los miembros rara vez introducen datos privados (aunque sí personales como correos electrónicos). No obstante, la complejidad y preocupación aumenta cuando hablamos de redes generalistas, principalmente, aquellas cuyas políticas son especialmente enrevesadas como es el caso de Facebook, a la que dedicaremos los siguientes capítulos.

4. LA ATRACCIÓN DE LAS REDES SOCIALES Y LA DELIMITACIÓN DEL ÁMBITO INTROSPECTIVO

A pesar de la cantidad de inconvenientes citados anteriormente, queda preguntarnos por qué cada vez más personas deciden entrar en el juego de la exposición continuada de las redes sociales por Internet. Estar conectado resulta imprescindible para participar es la sociedad

---

475 Ídem.

476 Tal vez el mejor ejemplo de que nadie lee los acuerdos de privacidad de los sitios Web lo encontramos en el caso de la empresa británica Game Station: en 2009 cambió sorpresivamente sus cláusulas añadiendo que, además de ciertos contenidos, los firmantes cedía «su alma». El contrato solo estuvo en línea un día, pero durante ese tiempo la empresa se hizo con más de 7000 almas. Richmond, S. (2010): «Gamestation collects customers' souls in April Fools gag», en *the Telegraph*, 17 de abril de 2010.

de hoy, sin embargo, el beneficio percibido parece hacernos olvidar el necesario amparo que merece nuestra dimensión humana. Así, aunque creamos que somos nosotros los que elegimos exhibir nuestros contenidos, lo cierto es que estamos abocados a copiar los comportamientos de nuestros iguales, cayendo en la inmanencia de lo igual para evitar conductas discordantes.

Habitualmente la gente se une a las redes digitales para reforzar las relaciones sociales con los individuos de su entorno, reencontrarse con gente del pasado e, incluso, para conectar con gente anónima que comparte los mismos intereses. Inmersos en esta dinámica, la evolución de la red es exponencial: cuantas más personas se registren, más sujetos lo harán en el futuro y cuantos más contactos tengan los miembros del sistema, más motivos encontrarán estos para conectarse. Una vez que se consolide ese vínculo entre el usuario y el sistema, más costará romper la relación por cuanto la costumbre tiende a ser conservadora.

Empero, el poder de fascinación de las redes sociales va más allá de quedarse solo en un mero hábito adquirido. Resulta casi una certeza que parte del éxito del que se benefician estas herramientas comunicativas aparece ligado a la exposición continuada de nuestra intimidad y vida privada, un producto genuino y altamente atractivo que emplazamos en un escaparate abierto al mundo. Y es cierto que, cuando aludimos al uso de las redes sociales, alabamos sus bondades como instrumentos que nos permiten intercambiar contenidos y ver las fotos de las personas queridas que viven lejos. No en vano, se trata de herramientas nacidas para satisfacer un cierto tipo de comunicación que no conoce fronteras. Pero ¿realmente lo usamos solo para eso? A nadie se le escapa que la transparencia a la que las redes someten al ser humano, esto es, la alta visibilidad de sus contenidos y la facilidad de acceso es, precisamente, lo que más nos atrae de las redes digitales. Más aún, por cuanto podemos obtener dicha información sin ser percibidos, al igual que el vigilante del *panóptico*.

Es un hecho constatable que la intimidad de los otros nos atrae. Nos permite reconocernos en los otros[477] o, dicho de otra manera,

---

[477] Recordemos la importancia que adquieren «los otros» en la delimitación y formación de nuestra propia identidad: El individuo no es solo una «persona», un ser autosuficiente, es también, como argumenta Béjar, un «ser social»

averiguar las partes de nosotros que hay en los demás y esto no es algo novedoso. De hecho, parte del éxito del cine consiste en mostrar momentos de intimidad que antes no quedaban al alcance de todos: pensamientos, muerte, amor, relaciones en espacios privados y un largo etcétera se dan cita en las pantallas. Ahora, sin embargo, tenemos acceso a este tipo de actividades y comportamientos propios de lo privado aunque, en principio, más reales en tanto que no ficcionados. Y aunque todos sabemos que solo mostramos lo que queremos que se conozca de nosotros y, en este punto, nuestra intimidad puede parecer prefabricada, la realidad es que las interacciones en la Web 2.0 pueden arrojar más certezas sobre nosotros de lo que en realidad deseamos y podemos controlar.

Esto sucede especialmente en las redes de ocio o generalistas, dado que los individuos muestran no solo informaciones de contacto o de carácter profesional, sino que hacen visibles otros contenidos como ideologías, gustos, vivencias, relaciones personales y experiencias que, en última instancia, se traducen en un lienzo visible en que el aparecen perfectamente plasmados todos los aspectos de nuestras vidas, entrelazando lo que es privado y lo que no. No es de extrañar, por ello, que este tipo de espacios comunicativos supongan un mayor riesgo para la salvaguarda del ámbito reservado que las redes sociales profesionales, dado que conlleva la concreción de un mayor número de informaciones privadas y las injerencias en la intimidad y vida privada pueden provenir de más flancos.

De esa exhibición condicionada se desprende otra premisa: las redes sociales reafirman a la persona por cuanto sostienen su sistema de valores y creencias. Es lo que el autor de *La sociedad de la transparencia,* Byung-Chul Han, denomina la «inmanencia de lo igual»:

> Los *social media* y los motores de búsqueda personalizados erigen en la red un absoluto espacio cercano, en el que está eliminado el afuera. Allí nos encontramos solamente a nosotros mismos y a nuestros semejantes. No se da ya ninguna negatividad, que haría posible el cambio. Esta cercanía digital presenta al participante tan solo aquellas secciones

---

y, por tanto, se ve afectado por el proceso de decisiones del entorno comunitario del que forma parte: «En la Sociedad de extraños enunciada por Simmel los individuos están abocados a la búsqueda constante de afirmación y autoidentidad mediante la interacción con los otros». BÉJAR, H. (1988): *Op. cit.,*

> del mundo que le gustan. Así se desintegra la esfera pública, la conciencia pública, crítica y privatiza el mundo. La red se transforma en una esfera íntima o en una esfera de bienestar[478].

Esta recompensa adquirida asegura que la fuerza gravitatoria que emerge en torno a las redes se mantenga en el tiempo, en tanto que el individuo ha interiorizado este tipo de interacciones. Todo ello fomenta una retroalimentación continua que explica no solo el éxito de estas herramientas relacionales, sino su inclusión en otros muchos aspectos de nuestras vidas, en los que conductas y principios hasta ahora inamovibles parecen haber mutado. Es así como los intercambios comunicativos que se producen dentro de estos espacios de la web consiguen mutar la concepción de lo que anteriormente se consideraba intocable, por conceptos difusos cuya aparición emana de la naturaleza propia de las interacciones.

5. CÓMO LAS INTERACCIONES EN LAS REDES SOCIALES CAMBIAN LA ECUACIÓN DE LO QUE SE CONSIDERA PRIVADO

Una de las propiedades de estas comunidades, ya lo citamos al tratar la Teoría de redes, señala que «de las interacciones que se producen entre los miembros surgen propiedades que no pueden explicarse a partir de los elementos aislados» [479]. Sabemos, además, que la estructura de nuestras redes tiene un impacto importante no solo en lo esta es capaz de hacer, sino sobre nuestra propia vida, por lo que estudiar cómo se organizan estos entramados puede ayudarnos a entender tanto la relación entre el comportamiento individual y grupal de los individuos, como la influencia particular de los efectos de dichos comportamientos. Las redes sociales digitales no son ajenas a este proceso y de las interacciones que se generan en ellas derivan en una serie de cambios, ora en la percepción de riesgo y en la forma de comportarse de los individuos, ora en la manera en que se distribuye la información. Dicha coyuntura dibuja escenarios en los que nuestras concepciones más arraigadas se ven alteradas y nuestra intimidad y vida privada se ve altamente comprometida. Señalemos, brevemente, cuáles

---

[478] HAN, B-C. (2013): *Op. cit.,* p. 69.

[479] CACIOPPO, J. T.; FOWLER, J. H. y CHRISTAKIS, N. A. (2009): *Op. cit.*

son esas atribuciones propias de las redes sociales capaces de mudar el comportamiento humano y afectar por ende a lo privado.

5.1 LA VIRALIDAD DE LA RED Y LA «INFLUENCIA DEL TERCER GRADO»

Las redes sociales en el mundo real manifiestan las mismas propiedades que las que hemos creado para Internet: al igual que estas, aumentan exponencialmente y su modelo de crecimiento se basa, fundamentalmente, en un proceso viral, en el que un número inicial de participantes propiciará que otros muchos se unan al sistema mediante el envío de invitaciones, bien a través de los correos electrónicos o agregando directamente desde la propia plataforma. En este sentido, entendemos «viralidad» como la capacidad que ostenta este tipo de entidades para lograr el máximo crecimiento en número de usuarios en el menor tiempo posible[480]. Dicha progresión se ha visto fuertemente incrementada a medida que comienzan a usarse nuevos canales de acceso, como los proporcionados por las tecnologías móviles.

Pero independientemente de la implementación de esta tecnología y teniendo en consideración que las propias herramientas digitales ya arrastran un efecto multiplicador, este atributo, la viralidad, ayuda a explicar no solo su rápida expansión, sino el contagio de muchos de los comportamientos más extendidos y que implican una mala *praxis* respecto a la propia protección de datos privados. Los investigadores expertos en redes sociales James Fowler, de la Universidad de California en San Diego, y Nicholas Christakis, de la Universidad de Yale, matizan en qué se materializa dicho fenómeno: en las redes sociales digitales existe un «efecto de contagio»[481] ya que tendemos a copiar el comportamiento de aquellos con los que estamos conectados; algo similar a lo que puede suceder en la vida real entre un grupo de amigos o conocidos, pero llevado al extremo.

En varios estudios sobre la difusión de la influencia, Fowler y Christakis demostraron que ese contagio en la forma de actuar era

---

480 AEPD e INTECO (2009): *Op. cit.*, p. 43.

481 FOWLER, J. y CHRISTAKIS, N. (2010): *Conectados*. Madrid: Taurus, p. 30.

palpable no solo en relación a la gente con la que estamos directamente conectados, lo que sería algo meramente intuitivo, sino que se observaba en contactos de nuestros amigos y, a su vez, en los enlaces de estos. Esto verifica que las conductas se propagan no solo entre conocidos, sino entre personas que jamás se han visto. Por ello, esta contaminación es más potente que en el universo tangible, dado que la influencia en las redes sociales se distribuye en tres grados de conexión posibles, esquematizados en: «amigos», «amigos de amigos» y «amigos de los amigos de nuestros amigos». Es lo que se denomina la «influencia del tercer grado». Como consecuencia, el impacto afecta no solo a las personas que conocemos sino a todos aquellos que figuran entre sus contactos, por lo que tendemos a copiar los comportamientos de personas con las que nunca hemos tenido relación y lo hacemos de forma casi gregaria.

Esta inoculación a distancia, que para los autores tendría una base genética, fue bautizada por Fowler como la propiedad del «mundo pequeño»[482] en honor a los primeros estudios de Milgram, y se reproduce en todos los ámbitos que tienen cabida en dichas redes. Entre esos aspectos, la protección de los datos personales no es ajena al nombrado fenómeno, por lo que las prácticas y decisiones que toman los individuos pueden contaminarse rápidamente de las emprendidas por otros sujetos. No obstante, este hecho posee dos vertientes: si bien se pueden copiar los buenos hábitos así como actitudes favorables para la propia salvaguarda de contenidos privados, en el extremo contrario provoca que la falta de concienciación se pueda propagar bajo la premisa errónea de que si los demás muestran alegremente su vida privada y, aparentemente, no sucede nada, nosotros podemos hacer lo mismo. Sobra añadir que, habitualmente, la balanza se inclina hacia dicho extremo. Sin apenas percatarnos, estamos compartiendo además de datos personales, las decisiones que emprendemos al verter dichos datos en las redes.

Este fenómeno, unido a la enorme viralidad que caracteriza a las redes por Internet, favorece que ciertos comportamientos, como el referido a la intimidad extimada por iniciativa del sujeto, puedan lle-

---

[482] FOWLER, J. H. (2005): «La participación en un mundo pequeño». En Zuckerman, A. (ed.): *Lógica de la política social*. Filadelfia: Universidad Temple, pp. 269-287.

gar a propagarse por todo el planeta. Especialmente, si tenemos en cuenta que dicha viralidad permite que una persona pueda incrementar su red de contactos entre 500 y 1500 personas[483] en función de su mayor o menor grado de participación en el sistema. Como resulta de este proceso, uno de los patrones de actuación que se reproducen a lo largo y ancho del planeta es la exaltación del «yo» hasta límites antes desconocidos.

5.2 LA EXALTACIÓN DEL «YO»

> Me parece indispensable decir quién soy yo [...] La desproporción entre la grandeza de mi tarea y la pequeñez de mis contemporáneos se ha puesto de manifiesto en el hecho de que ni me han oído ni tampoco me han visto siquiera
>
> Friedrich Nietzsche, *Ecce Homo* [484]

El ser humano adquiere una identidad a través de la interacción social y, en dicha construcción, mostrar es importante porque interviene en la creación del «yo», encontrándose siempre en una posición ambigua entre la voluntad de preservar su dimensión reservada y la necesidad de compartir experiencias y pensamientos con los demás. Este fenómeno que, si bien no es nuevo, sí ha experimentado un crecimiento exponencial con la proliferación de los nuevos espacios mediados, provoca que la visibilidad juegue un papel fundamental en nuestra propia conceptualización: hoy, más que nunca, nos definimos como sujetos en función de lo que enseñamos y lo que otros ven. Lo introspectivo parece haberse debilitado porque la intimidad se ha convertido en algo tan importante para definir lo que somos que hay que expresarla[485].

Esta «exhibición pública», en palabras de Boyd y Ellison, actúa en detrimento de la percepción del individuo; especialmente, en lo que respecta a su estimación del riesgo a la hora de compartir ciertos datos, en tanto que le sitúa en un falso escenario de supremacía y control. En esta simulación de realidad, virtual e idealizada, las redes sociales constituyen un epicentro simbólico de cuyo poder de atracción

---

483 CELAYA, J. (2008) *La empresa en la Web 2.0*. Madrid: Planeta, p. 95.
484 NIETZSCHE, F. (1994): *Ecce Homo*. Madrid: Alianza Editorial, p. 15.
485 SIBILA, P. (2008): *Op. cit.,* p. 20.

es complicado escapar; toda vez que alimentan una sensación de bienestar en la que el sujeto se siente el centro de todo lo que le rodea. Arguye Andrés Durà, a este respecto:

> Nos hacen creer que formamos parte de un todo, que somos uno más, que estamos más unidos y que somos imprescindibles en el engranaje del mundo interconectado. Pero eso sí, yo soy la pieza más importante de la máquina. Todos somos la masa pero yo destaco por encima de los demás. Yo soy importante, y por eso todo el mundo le interesan mis ideas políticas, mi afinidad religiosa, mi color favorito y lo que hago el sábado por la tarde. Todo tengo que ponerlo en mi perfil porque es vital que lo sepan todo de mí. Mejor dicho, los demás saben de ti lo que tú crees que eres. (…) «Soy diferente» pero no tanto como para estar fuera de la red [486].

Para James Fowler, la razón por la que las redes sociales fascinan y atrapan a partes iguales recae en que es la primera vez que los individuos pueden ver cierto tipo de informaciones sobre los otros, al mismo tiempo que aumentan la sensación de poder y participación de la gente en la sociedad. De este modo, el individuo comienza a darse cuenta de que lo que hace da sus frutos en toda la red social humana.

Así, parece meridiano que uno de los secretos del éxito de estas plataformas es que consiguen hacernos visibles, realizar el *dictum* de Warhol según el cual, en el futuro, todos tendríamos unos minutos de gloria. Y si bien es cierto que nos sitúan en el centro del debate, no lo es menos que es esta capacidad la que, paradójicamente, nos vuelve más porosos a las injerencias ajenas.

Consecuentemente, esta exaltación del «yo», de la individualidad como factor a publicitar, nos convierte poco a poco en escaparate de nosotros mismos, sin que la NSA necesite desarrollar un costoso programa para detectar quien se oculta tras nuestros nombres. Los sujetos anónimos que se esconden bajo el disfraz de usuario de las redes sociales:

> Sienten la necesidad de describirse a sí mismos, de explicar todos sus defectos y todas sus virtudes, sus gustos, sus disgustos sus experiencias y sus inexperiencias. Se ha creado una nueva cultura de exaltación del «yo». […] es la sociedad basada en las apariencias, en el «no soy pero

---

[486] ANDRÉS DURÀ, R. (2010): *Op. cit.,* p. 81.

> aparento ser». «Para triunfar primero hay que presentarse como un triunfador»…Que antes se fijarán y creerán lo que aparentes ser que lo que realmente seas[487].

Estas modificaciones, paradójicamente, no se han producido en la vida real, en la que seguimos siendo igual de recelosos con nuestra vida privada: no hablamos con desconocidos, no dejamos que nadie extraño oiga nuestras conversaciones, ni les dejamos entrar en la intimidad de nuestros hogares o les regalamos fotos nuestras. La dimensión propia del ser humano sigue constituyendo nuestro recinto sagrado y sin posibilidad de profanación. Una suerte de desfase entre actuaciones y concepciones, que se traduce en un «quiebre entre el mundo real y el mundo virtual»[488] en palabras de Albornoz, y que viene dado por factores ficticios de confianza que alientan a creer que en la ciudad digital los viandantes controlan la situación.

Este falso dominio del individuo que, como veremos en los capítulos siguientes, juega un papel esencial en muchas de las situaciones de riesgo que se producen en la Web 2.0, propicia que vertamos gran cantidad de información personal en el perfil para conseguir la creación efectiva de ese «yo» virtual ideal que anhelamos ser.

Ahora en Internet todo el mundo es famoso; al menos, entre quince personas, sostiene el teórico David Weinberger[489]. Este narcisismo en pos de una buscada reputación, aun cuando ello implique pagar altos costes en lo referente al resguardo de nuestro ámbito reservado, aparece sustentado en una cierta ignorancia o inocencia del usuario que, a la postre, resulta perjudicado. Tal vez por ello, autores como James Grimmelmann opinan que, la mayoría de problemas asociados a injerencias en la vida privada en Internet son «consecuencias naturales de las maneras entusiastas con que la gente lo utiliza. […] Hay una gran tensión, probablemente irreconciliable, entre el deseo de te-

---

487 SÁNCHEZ ÁLVAREZ, J. (2006): *Manual para cínicos de cómo triunfar en la sociedad de la mentira*, Madrid: Pensamiento alternativo, p. 22.

488 ALBORNOZ, M. (2007): «Cibercultura y las nuevas nociones de privacidad». *Nómadas,* n. 28, pp. 2-17, p. 3.

489 WEINBERGER, D. (2005): «Famous to fifteen people», en *The original,* 23 de julio de 2005.

ner un control fiable sobre la información propia y el deseo de relaciones sociales no planeadas»[490].

Es por ello que, en esta «Web del exhibicionismo» tal y como la denomina Robert Samuelson, se ha fomentado la mayor exposición en masa de la historia de la Humanidad, propiciando que miles de personas emplacen sus informaciones personales donde todo el mundo pueda verlas, comprometiendo seriamente sus derechos fundamentales a la protección de la intimidad y vida privada[491]. La seducción de beneficios inmediatos es mucho más atractiva que el resguardo de nuestra sustancialidad, un movimiento de extroversión que bien recuerda a las tesis de Richard Sennet y lleva según Byung-Chul Han a la «publicación» de propia la persona: «La esfera pública se convierte con ello en un lugar de exposición. Se aleja cada vez más del espacio de la acción común. […] habitada por narcisistas sujetos íntimos a los que les falta por completo la capacidad de distancia escénica»[492].

5.3 LA FRAGMENTACIÓN DE LA IDENTIDAD VIRTUAL EN LAS DISTINTAS REDES SOCIALES

Todos somos biógrafos no oficiales de nosotros mismos
John B. Thompson, *Los Media y la modernidad*

Tal y como mencionamos en el *Capítulo II* del *Marco conceptual* de esta tesis, la esfera privada es el recinto de la individualidad y, por tanto, de la identidad. Es el espacio de ensayo, de actuación del «yo» público[493] y, por ende, es donde los individuos preparan sus actos públicos. Sin embargo, cuando las fronteras de este espacio de ensayo se diluyen, asistimos a otros procesos de formación de la identidad, redefiniciones y reconstrucciones de nuestra esencia individual que ya no provienen de nuestra experiencia directa con la realidad[494] sino de

---

490 GRIMMELMANN, J. (2009): «Saving Facebook», en *Iowa Law Review*, n. 94, p. 1137-1148.
491 SAMUELSON, R. (2006): «The Web of Exhibitionists», en *The Washington Post,* 20 de septiembre de 2006.
492 HAN, B-C. (2013): *Op. cit.,* pp. 69-70.
493 GOFFMAN, E. (1997): *Op. cit.,* p. 123.
494 THOMPSON, J. B. (1998): *Op. cit.,* p. 270.

los escenarios tecnológicos, capaces de propiciar, incluso, la convivencia de varios «yos» o identidades digitales.

Este fenómeno no es gratuito. Cuando decidimos entrar en una de estas comunidades creamos un perfil que nos identifica y dicha página forma parte de nuestra identidad digital, esto es, de nuestro «yo» virtual; aunque, en la mayoría de los casos, es una versión mejorada de nosotros mismos. Esta recreación binaria de nuestra persona cuenta con una traba: las redes sociales no permiten a los individuos realizar la diferenciación de espacios que tiene lugar en las interacciones físicas por lo que, una de las maneras de sortear esta falta de granularidad consiste en fragmentar la identidad creada. De este modo, los individuos pueden elegir aparecer de diferentes guisas en función de la red social, mostrando una serie de datos en las de cariz profesional y ostentando otro *role* en plataformas generalistas. Siempre, se supone, como respuesta a una reflexión previa acerca de cómo uno se quiere presentar a sí mismo en cada escenario.

Este juego, aparentemente inocente, puede conseguir el efecto contrario. Enlazados a esta multiplicidad de identidades digitales, los datos privados de los individuos pueden adquirir visibilidad o no en función de los objetivos de cada usuario. Sin embargo, dado que estos territorios semiacotados no siempre se mantienen inalterables, un cambio en las configuraciones por defecto puede provocar que los datos que introducimos en una determinada red social y que destinamos a un público concreto estén a disposición de todo el mundo. Especialmente, si tenemos en cuenta los contenidos procedentes de perfiles públicos e indexados por buscadores y la retroalimentación que subyace al poder de agregación de la Web semántica. En definitiva, puede llevarnos a generar información sobre todos los ámbitos de nuestra existencia, sin que podamos llevar a buen término la diferenciación entre esferas que hacemos en la vida real, ni controlar la exhibición de nuestras informaciones.

5.4 LA EQUIPARACIÓN ENTRE «CONTACTOS» Y «AMISTADES»

Dado que la percepción del otro juega un papel primordial a la hora de diferenciarnos y dibujar nuestro propio ser, los usuarios de las redes sociales construyen sus identidades en función de sus rela-

ciones, definiendo lo que son a través de las asociaciones que han establecido. Pero los otros no solo son fundamentales para crear la propia identidad, sino que se vuelven substanciales para mantener funcional esa red. Tal y como recalcábamos al citar la Teoría de redes, los nodos compiten por conseguir más enlaces en tanto que ello garantiza la supervivencia y desarrollo del entramado. Y los individuos hacen lo propio en las redes digitales, interactuando para conseguir el máximo de contactos. Esto no supondría ningún perjuicio si no fuera por las implicaciones que tiene compartir los contenidos de todo tipo con personas a las que, no siempre, nos une una relación cercana. Y todo ello, aliñado con el hecho de que en dichos espacios relacionales es imposible separar los diversos aspectos que conforman la existencia humana, sino que la realidad poliédrica que caracteriza a la vida se encuentra centralizada y confinada en un mismo escenario. El interactor debe enfrentar así una mezcolanza de relaciones muy diversas, cuya complejidad camina pareja a la ya citada indeterminación de escenarios que se dan cita en el mismo continente.

Dicha coyuntura se acentúa por la importación del concepto «amigo»[495], voz que hemos tomado prestada de la realidad tangible y que transponemos a los vínculos digitales, olvidando las notables diferencias que establece la comunicación mediada. Las divergencias, no obstante, van más allá de las introducidas por la naturaleza propia de la comunicación vía Internet, y derivan de la manera en que las plataformas y sus participantes reinterpretan la noción de «amistad», según la cual, «amigo» puede ser cualquiera con el que establezcamos un vínculo. Es decir, se equipara «amigo» a «enlaces» y esto, además de vaciar el verdadero contenido del vocablo, es un hecho no exento de peligro.

Dicha conexión no es sinónimo de amistad en el sentido vernáculo. Y, dado que las razones por las que unos individuos deciden conectarse a otros son muy variadas, la duda es: ¿Debemos aplicarle a ese cualquiera las normas sociales que acarrea ser amigo en la vida real? Estas personas con las que enlazamos nuestros perfiles podrán acceder a nuestra información, vídeos, fotografías y demás conteni-

---

[495] Entrecomillamos la palabra para diferenciarla del concepto de amigo tradicional, el de las relaciones que se establecen en el mundo real.

dos compartidos que publiquemos. Aun cuando plataformas como Facebook permiten personalizar la visibilidad de las publicaciones creando listas de contactos, habrá informaciones que siempre serán accesibles a toda nuestra red. Y, por nuestra parte, ante la indeterminación que genera este entramado de relaciones, nos inclinamos más a mostrar a todos nuestros enlaces el mismo contenido que revelaríamos a un amigo, que al extremo contrario, a pesar de que, en las interacciones físicas, otorgaríamos distintos niveles de cercanía a esas personas.

Bien es cierto que los vínculos afectivos preexistentes, es decir, los establecidos en el universo físico pueden derivar en conexiones en el lienzo virtual y, de hecho, uno de los argumentos que más se esgrimen a la hora de usar estas herramientas es que ayudan a estrechar y reforzar los lazos de amistad, así como la comunicación entre familiares y otras personas cercanas. A este respecto, se observa la traslación al escenario virtual de una serie de relaciones preexistentes «con amigos, familiares y vecinos, particularmente, con aquellos que no son fácilmente accesibles en el espacio físico»[496]. Y dentro de estas, tiende a haber un mayor énfasis en relaciones de iguales por encima de jerarquías o lazos familiares.

No obstante, las redes sociales contribuyen a la eliminación de barreras no solo físicas y geográficas, sino también socioculturales y de clase o *status* y ello nos permite contactar tanto personal como profesionalmente con personas a las que antes no teníamos acceso: es la esencia de lo que antes mencionábamos como «vínculos débiles»[497]. De este modo, además de las citadas conexiones se produce la emergencia de enlaces basados en un propósito u objetivo concreto como, por ejemplo, aquellos contactos referidos a un tema específico. El problema estriba en que puesto que a todos les aplicamos la etiqueta de «amigos» no siempre seremos capaces de establecer las debidas precauciones a la hora de compartir informaciones.

Por otra parte, en una red social resulta sencillo hacerse «amigo» de alguien a quien ni siquiera se conoce. De hecho, habitualmente los usuarios de Facebook poseen lazos de amistad que, de media, superan

---

496 BENKLER, Y. (2006): *Op. cit.*

497 GRANOVETTER, M. (1983): «The Strenght of weak ties: a network theory revisited», en *Sociological theory*, vol. 1, pp. 201-233.

los 130 contactos[498], una cifra mucho más abultada de la que seríamos capaces de mantener en la realidad tangible. Realmente, este tipo de conexiones están más cercanas al concepto de «contacto», vocablo mucho más apropiado por cuanto estos intercambios comunicativos no implican necesariamente la aplicación de los valores propios de la amistad. Pero el uso de una terminología más «amable» y que apela a la afectividad no es, en absoluto, inocente, ni mucho menos arbitraria. ¿Quién se puede negar a aceptar una solicitud de amistad de un conocido o compañero de trabajo si ya sabemos que nos considera un «amigo»? Tal vez ahora, la experiencia nos ha vuelto algo más precavidos, pero en los primeros años de uso de la Red casi nadie se habría negado.

El hecho de que la estructura de este sistema promueva la binarización de relaciones sociales entre «amigos» y «no amigos», eliminando otro tipo de coyunturas que se suceden en las interacciones cara a cara, fuerza en cierto modo al usuario a ceder y compartir parte de sus contenidos reservados para evitar desencuentros con otras personas. La dificultad para llevar a cabo las preferencias de visibilidad mina los argumentos que esgrimen las compañías que gestionan las plataformas de redes y según los cuales, los sujetos han «elegido» libremente diseminar su información en la Red. Y todo ello, porque estas plataformas no permiten la existencia de diversas esferas con atribuciones distintas en las cuales el sujeto decide qué datos desea compartir, qué visibilidad otorgarles o con quién hacerlo. El diseño de dichas herramientas parece negar ese derecho del ser humano a mantener una parte reservada y, lo más preocupante, es que eso es algo que comienza a ser visto más como un privilegio, que como un derecho.

5.5 LA ALTERACIÓN EN LA PERCEPCIÓN DE RIESGO

Uno de los elementos diferenciadores de las redes sociales respecto a otras aplicaciones anteriores a la Web 2.0, es que los participantes hacen explícita su red de contactos: quiénes son nuestros amigos y quiénes no, por omisión, es una visión constantemente

---

[498] *Facebook Newsroom,* 2 de mayo de 2012. https://www.facebook.com/FacebookEspana. [08/02/2013].

presente en el interfaz de estos sitios. Los sujetos son forzados, continuamente, a declarar una y otra vez los nombres de sus contactos en diferentes contextos, guiados por la idea de que dicha agregación y centralización es necesaria. Esta deriva faculta que, a diferencia de las redes sociales tradicionales, el potencial de las conexiones digitales se eleve cuantitativamente ya que Internet «da visibilidad a los componentes de la red social del propio individuo respecto al resto, aumentando el grado de comunicación entre los nodos de forma espectacular»[499].

Sin embargo, el hecho de que los amigos estén siempre presentes en el interfaz conlleva otro efecto: estas redes dan la impresión de ser espacios semipúblicos en los que uno puede actuar como lo haría en su esfera privada con su círculo de allegados, algo que nos empuja a bajar la guardia y a comportarnos más desinhibidamente. Esto tiene un reflejo directo en la cantidad de contenidos privados que volcamos.

Por otra parte, aun cuando la amplitud de nuestra lista de contactos puede ser considerada un objeto de medición de estatus donde a más amigos, más reconocimiento, añadir contactos a nuestra red sin criterio constituye una práctica que no está exenta de riesgos. Es más, el problema al que nos enfrentamos cuando tenemos muchos contactos es el excesivo número de tareas que debemos cuidar si queremos proteger nuestras informaciones activamente. Según el profesor Robin Dumbar, el número de estos «amigos» que puede atender nuestro cerebro en redes como Facebook es de 150, cifra que se conoce como «número Dumbar»[500]. El investigador, que entiende como «amigos» a las personas cercanas y conocidas con las que tenemos contacto al menos una vez al año, sitúa en dicho número el límite de sujetos que puede gestionar la zona del cerebro que destinamos a las relaciones sociales, esta es, la correspondiente al pensamiento y el lenguaje. Si a este número le sumamos la necesidad de crear listas o modificar los controles de privacidad, personalizándolos para cada contacto o gru-

---

499 FERNÁNDEZ, S. (2008): «Redes sociales, fenómeno pasajero o reflejo del nuevo interactor», en *Telos,* n. 76, pp. 118-120.

500 Según el antropólogo, este valor, aproximadamente de 150 individuos, está relacionado con el tamaño de la neocorteza cerebral y su capacidad de proceso. DUMBAR, R. (2011): «Don't Believe Facebook; You Only Have 150 Friends» *National Public Radio*, 4 de junio de 2011.

po, intentar satisfacer nuestras necesidades de protección puede convertirse en una empresa imposible. Por ende, aumentar el número de enlaces sin reflexión alguna no solo nos vuelve ineficientes a la hora de modificar los controles por defecto, sino que provoca que seamos incapaces de prestar atención a lo que realmente nos interesa. Todo ello, sumado al resto de interacciones propias de las redes sociales por ordenador, dibuja un escenario en el que el amparo de lo privado parece baldío desde el comienzo.

6. REFLEXIONES SOBRE EL CAPÍTULO

En las redes sociales muchos aspectos de la intimidad y vida privada quedan desprotegidos, amparados por una inmanencia específica y novedosa que nos empuja a confiar nuestra información más reservada sin apenas reflexión. La falta de conocimiento y el auge de la transferencia de los datos personales han alentado que estas plataformas generen y distribuyan una ingente cantidad de información personal, que se transforma en materia prima de las empresas que fundamentan su negocio en la recopilación de datos. Es por ello que en el presente capítulo hemos visto, a grandes rasgos, cómo las redes sociales digitales alteran nuestra percepción de riesgo y nos vuelven inermes. Cabe apostillar, sin embargo, que tan solo nos hemos asomado a la superficie de un fenómeno mucho más complejo y que pretendemos abordar con precisión, hecho que nos apremia a descifrar el papel que detentan los flujos de información que el usuario recibe en la protección activa de sus informaciones personales, así como la naturaleza y dirección del trasvase de datos en estas plataformas. Comprobar, en suma, si la estructura, funcionamiento y filosofía empresarial que impregna a estos tejidos sociales virtuales, permite que el individuo esté en disposición de preservar su dimensión reservada de manera satisfactoria, esto es, si ostenta el conocimiento necesario para actuar acorde a los principios de la integridad contextual. Para ello, en el próximo capítulo comenzaremos un pormenorizado estudio del intercambio de datos que se produce en la red social que contempla todos los casos habidos y por haber en lo que a intromisiones en la intimidad y vida privada se refiere: Facebook.

Artífice de las técnicas más rebuscadas e invasivas de recolección de información, el «libro de caras» ostenta el deshonroso puesto de

ser, en función de la cantidad de estudios científicos, informes y noticias que suscita, la empresa que más poder tiene para dañar nuestra intimidad y vida privada. A la descripción de sus «bondades» encaminamos el siguiente empeño.

CAPÍTULO VI. FACEBOOK, EL *PANOPTICON* VIRTUAL

SÍNTESIS

Las redes sociales, paradigma de la cultura Web 2.0, protagonizan un gran parte de las quejas de los usuarios en lo que respecta a la salvaguarda de sus informaciones personales por lo que, a pesar de sus beneficios que son muchos, su adopción demanda reflexión y una cierta abstracción crítica. En el presente capítulo, nos sumergiremos en dicha problemática, centrando la perspectiva en la plataforma que más controversias ha suscitado durante el tiempo que lleva activa y que, además, posee una mayor comunidad de usuarios a lo largo y ancho del planeta: nos referimos como sabemos a Facebook. No obstante, el análisis de la red social por antonomasia se mencionará con valor genérico, es decir, como ejemplo de la multitud de plataformas que proliferan en el universo digital. La razón es sencilla: A pesar de las distintas especificidades que otras redes puedan contener, la empresa de Mark Zuckerberg ejemplifica a la perfección los innumerables dilemas habitualmente asociados al uso de las redes sociales. Debido al desarrollo alcanzado, la capacidad para obtener y acumular contenidos, y las interferencias generadas por la multitud de funcionalidades que proporciona, Facebook es, con mucha diferencia, la comunidad que más debate plantea en todos los foros; desde grupos de derechos civiles y organismos oficiales dedicados a la protección de datos, hasta los poderes públicos garantes del derecho a la intimidad. Sin olvidar mencionar, como no podía ser menos, las inquietudes que genera a nivel individual en esa pieza clave del engranaje tecnológico que es el ser humano y que se encuentra al otro lado de la pantalla inerme ante esta problemática.

1. INTRODUCCIÓN: FACEBOOK, LA REVOLUCIÓN EN LAS REDES SOCIALES DIGITALES

El 18 de febrero de 2004, tan solo dos semanas después del despegue de la plataforma TheFacebook, Marc Zuckerberg, uno de sus creadores y, sin duda, la cara más visible del negocio, descubrió con

sorpresa que el sitio ya había atraído la atención de más de cuatro mil usuarios. Sin embargo, y a pesar del éxito repentino, era imposible predecir que diez años más tarde su creación sería usada por más de un millardo de personas a lo largo y ancho del planeta[501]. Una progresión inesperada que torna del todo quimérico aventurar qué será Facebook dentro de otros diez años. Pero, ciñéndonos al momento actual, cuando nos referimos a esta comunidad estamos hablando de más de un millardo de usuarios activos que comparten, cada día, cinco millones de informaciones, introducen 350 millones de fotos y presionan el legendario botón «me gusta» más de 4,5 millones de veces al día. Con estas cifras, no resulta osado afirmar que Facebook es la red social más popular del mundo, además de la segunda página Web más visitada por detrás de Google, el otro gran exponente de la agregación de datos en la Web 2.0[502]. Debemos mencionar, eso sí, la excepción de otras regiones geográficas como es el caso de Brasil o India, países donde la red social Orkut concentraba, respectivamente, el 48,0% y 39,2% de seguidores[503]. Esta excepción se quedó en el pasado, ya que la red cerró a finales de 2014 al no poder competir con otros sitios más populares y como parte de la estrategia de Google para allanar el camino a su red Google+, lanzada en 2011.

Facebook ostenta otro record que, curiosamente, también comparte con el buscador: lidera el número de quejas de los ciudadanos por sus prácticas abusivas, toda vez que protagoniza infinidad de informes e investigaciones científicas al respecto. No en vano, la extrema complejidad de la arquitectura del sitio, la perpetuidad de almacenamiento o los acuerdos comerciales con terceras empresas a las que ceden datos personales de los usuarios son solo un ejemplo de la maraña de asuntos controvertidos que implican a Facebook. Este hecho,

---

501 ZIMMER, M. (2014): «Mark Zuckerberg's theory of privacy», en *The Washington Post,* 3 de febrero 2014.

502 Si analizamos este fenómeno por regiones geográficas, aunque la tónica general es la ya descrita, sí hay excepciones como, por ejemplo, China en la que el buscador Baidu (www.baidu.com) se sitúa por delante de Google. Esta preferencia responde, sin embargo, a razones de índole político que no trataremos en esta tesis. ALEXA (2014): «Top sites on the Web». Disponible en: http://www.alexa.com/topsites. [19/05/2014].

503 Global Web Index (2014): *GWI Social Summary*, enero de 2014. Disponible en: https://app.globalWebindex.net/products/report/gwi-social-q3-2014. [30/01/2014].

no obstante, no parece dañar el negocio de la compañía que, por el contrario, obtiene provecho tanto de la inmadurez legal que todavía empaña muchas de las actividades desarrolladas en la Web, como de las asimetrías legislativas entre Estados Unidos y los demás países donde opera la plataforma, actuando sin tan siquiera proponer un nuevo modelo de tratamiento de datos personales capaz de armonizar los beneficios de la red con los derechos fundamentales en juego.

Razones, todas ellas, que indican que la plataforma es tal vez el mejor modelo para ejemplificar esa dinámica *superpanóptica* a la que muchos investigadores aluden cuando se refieren a la Web 2.0. No en vano y teniendo en cuenta que la página de inicio de cualquier participante es una sarta de pequeñas dosis de su vida privada y la de sus conocidos, no es difícil que estas reflexiones, fotos y otras ocurrencias públicas desvelen más de lo que creemos de nuestra propia identidad.

2. FACEBOOK, LA RED SOCIAL QUE CONECTA EL MUNDO. DESARROLLO Y PRINCIPALES SERVICIOS

«Crear una manera más rápida y rica en que la gente pueda compartir la información que sucede alrededor de ellos»[504]. Esta fue la premisa que empujó al creador de la página, Mark Zuckerberg[505], a fundar junto a Eduardo Saverin, Chris Hughes y Dustin Moskovitz la compañía más popular de la última década. Dicho esto, Facebook no es una red social cualquiera, ni siquiera se trata «sólo» de una red social, aunque pueda parecerlo. En realidad, es una plataforma que engloba multitud de servicios y que, como la mayoría de comunida-

---

[504] LOGAN, B. (2009): «Blog post commemorating Facebook's 200 millionth user», en *Facebook blog*. Disponible en: https://www.facebook.com/notes/facebook/200-million-strong/72353897130.

[505] Existe una amplia controversia sobre si la creación y la idea original del sitio proviene del propio Zuckerberg o de otros compañeros de universidad, los gemelos Winklevoss. Dicha polémica, que lastró los comienzos de la compañía, se puede visionar en la película de David FINCHER (2010): *La red Social* (*The social network*) o revisar en el libro: KIRKPATRICK, D. (2011): *El efecto Facebook: la verdadera historia de la empresa que está conectando el mundo*. Barcelona: Planeta; así como en las innumerables informaciones de prensa en las que se reflejan los problemas de autoría.

des de este tipo, pone en contacto a los anunciantes y empresas con su público objetivo. La diferencia, sin embargo, radica en que Facebook lo hace de una manera altamente efectiva y, teniendo en cuenta que somos los usuarios o, mejor dicho, nuestras informaciones privadas las que aportan un valor añadido a este negocio, no está de más efectuar un somero análisis del proceder de la compañía.

Para ello, comencemos bosquejando la evolución de la plataforma a lo largo de su corta pero intensa historia; reseñando, subsiguientemente, aquellos servicios que ofrece y que la hacen tan especial.

2.1 ALGO DE HISTORIA: LOS INICIOS

Ya desde su ingreso en Harvard, Zuckerberg empezó a hacer aplicaciones con un carácter eminentemente social centradas en el ámbito universitario. A lo largo de los primeros meses de otoño de 2003 ideó una herramienta denominada «Coursematch» que permitía a los estudiantes ver la lista de otros compañeros de clase y, poco después, vendría «Facemash.com», una polémica red en la que se calificaba a las alumnas según sus características físicas. Esta última le propició a su creador una primera ronda de denuncias por vulneración de derechos de propiedad y contra la vida privada: Ya entonces, el Departamento de Servicios Informáticos de Harvard le acusó ante la administración por infringir la seguridad informática de la universidad y por violar las políticas de privacidad y de propiedad intelectual[506]. A pesar de este incidente, ambas redes allanaron el camino para la aparición de Facebook, una novedosa herramienta que en un primer momento se llamó «Thefacebook» y que Zuckerberg puso a disposición de los estudiantes de Harvard en febrero de 2004, tras registrar su dominio un mes antes.

La idea de lanzar una comunidad sustentada en la Web como canal de transmisión y en la que la gente compartiera sus gustos y sentimientos, no es nueva. David Bohnett, creador de GeoCities, la había incubado a finales de los años 1980, aunque no la pudo llevar a buen término dado que la época no ofrecía aún las posibilidades tecnológi-

---

[506] KAPLAN, K. A. (2003): «Facemash Creator Survives Ad Board», en *The Harvard Crimson,* 19 de noviembre de 2003.

cas disponibles décadas más tarde; una superioridad técnica que Mark Zuckerberg aprovechó en 2003 para dar forma al mundo de las redes sociales tal y como lo conocemos hoy.

En su origen, Thefacebook era una página Web exclusiva para estudiantes de la Universidad de Harvard, una especie de directorio en el que los universitarios podían buscar a sus compañeros de clase e intercambiar información con ellos, a través de una comunidad privada en Internet. Poco después, se amplió a otras universidades de la Liga Ivy (ocho universidades privadas del noroeste de Estados Unidos) y, ulteriormente, se extendió por más centros de enseñanza superior e institutos de Estados Unidos y Canadá. La compañía, que en 2004 decidió asentar sus oficinas centrales en Palo Alto, California, comenzó a llamarse Facebook en otoño de 2005.

Desbordados por el éxito y debido a la enorme cantidad de peticiones de admisión, la plataforma comenzó a permitir que los estudiantes agregasen a otros compañeros cuyas escuelas universitarias no estaban incluidas en el directorio inicial; desbrozando un camino que, en septiembre de 2006, llevó a Facebook a posibilitar el registro para cualquier persona con una cuenta de correo electrónico, es decir, a todos los usuarios de Internet. Y ello, a pesar de las protestas de gran parte de sus primigenios participantes, decepcionados ante el abandono la base estudiantil sobre la cual se había asentado el sistema. De este modo, tras su creación Facebook se adelantó rápidamente a otros espacios ya consolidados como el citado GeoCities o MySpace, aportando un revolucionario concepto de interacción al posibilitar, a diferencia de otros sitios ya existentes, que cualquiera pudiera darse de alta en la red.

2.1.1 **Expansión de la compañía**

El contexto que vivía Internet en el momento de implantación de la plataforma, con capacidad para interactuar a gran escala, propició que el proyecto rápidamente rebosara las expectativas iniciales y saltase del público general en Estados Unidos a otros países. Así, Facebook se expande inicialmente por Europa y, principalmente, por Reino Unido. En mayo de 2006, la compañía llega a la India y en agosto de ese mismo año agrega universidades en Alemania e Israel a su red. Entre tanto y aunque al principio las membresías se concentraban en

Estados Unidos, Canadá y Reino Unido, a mediados de 2007 son los propios usuarios quienes, de manera no remunerada, comienzan a lanzar versiones traducidas al francés, alemán y castellano para impulsar su uso fuera de Estados Unidos, sembrando el terreno para alcanzar un éxito sin precedentes.

Además de permitir el registro a cualquier interactor con un correo electrónico, una de las estrategias que propició la rápida expansión de la compañía fue que, a diferencia de otros sitios de redes sociales ya existentes, Zuckerberg decidió abrir la plataforma Facebook a otros desarrolladores. De este modo, en junio de 2006 la compañía decide establecer un acuerdo con el reproductor de medios y tienda de contenidos multimedia iTunes Store, para que su aplicación obtuviera datos sobre los gustos musicales de los usuarios y ofrecerles así un enlace de descarga en su propio sitio. También introdujo la importación de blogs de Xanga, LiveJournal o Blogger, entre otros.

Desde entonces el ascenso de la red social fue imparable: en noviembre de 2008 llegó a tener 200 millones de usuarios en todo el mundo y, entre 2008 y 2009, el uso de Facebook se incrementó en un 700%, alcanzando máximos históricos. Estos números obtuvieron su reflejo en el tiempo que los interactores dedicaban a la red, con cifras muy apetecibles para los anunciantes, anteriormente acostumbrados a que sus potenciales clientes saltasen de una página a otra en cuestión de segundos. Sólo por citar un ejemplo, durante abril del año 2009 los miembros del sistema habían dedicado casi 14 millones de minutos a sus aplicaciones[507], prestando a la vez mucha más atención a los contenidos publicitarios.

En julio de 2009, Mark Zuckerberg hizo público que Facebook había alcanzado los 250 millones de usuarios[508] y, en febrero de 2010, contaba ya con 400 millones, seis de ellos en España[509]. En marzo de ese mismo año y con más de 600 millones de usuarios, Facebook era

---

[507] NIELSEN, W. (2009): «Time spent on Facebook up 700%, but MySpace Still Tops for Video». Disponible en: http://blog.nielsen.com/nielsenwire/online_mobile/time-spent-on-facebook-up-700-but-myspace-stilltops-for-video/. [20/01/2012].

[508] «Facebook alcanza los 250 millones de usuarios», en *El País*, 16 de julio de 2009.

[509] ALEXA (2010): «Alexa Traffic Ranks. How popular is facebook.com?» Disponible en: http:// www.alexa.com/siteinfo/facebook.com. [19/11/2011].

la red social más grande del mundo y la segunda página Web más visitada[510]. Su progresión resultaba tan impactante que, según publicó el diario *The Economist*, si Facebook fuera un país, sería el tercer más poblado del mundo solo por detrás de China e India[511].

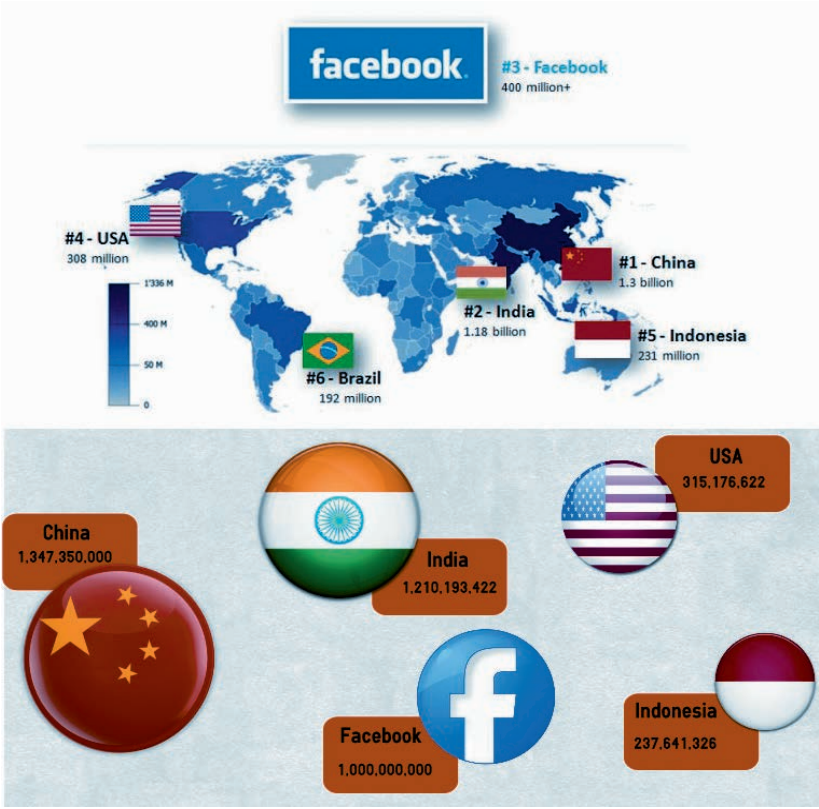

Figura 6.1 Si Facebook fuese un país…[512]

---

[510] ALEXA (2010): «The top 500 sites on the Web». Disponible en: http://www.alexa.com/topsites. [13/02/2012]. En 2014 Facebook continuaba en la misma posición del ranking.

[511] «Facebook has become the third-largest nation», en *The Economist,* 22 de julio de 2010.

[512] Fuente: Ídem.

2.1.2 **Panorama actual**

En septiembre de 2011, la plataforma alcanzaba los 800 millones de usuarios y solo un año más tarde, con más de 900 millones de miembros, ya estaba disponible en 70 idiomas[513]. De los 1230 millones de usuarios[514] de que dispone Facebook en enero de 2013, más de 600 millones son usuarios que acceden a través de dispositivos móviles. Por su parte, Brasil, India, Indonesia, México y Estados Unidos son los países con más miembros, aunque también hay millones de ellos que poseen más de una cuenta.

Es pertinente aclarar que en la mayoría de los casos estos datos provienen de fuentes de la propia plataforma por lo que son difíciles de contrastar. Sea como fuere, nadie pone en duda que Facebook es la red social más profusamente usada en todo el mundo. Una comunidad de habitantes que, en la actualidad, cuenta con más de un millón de usuarios activos que cada día comparten cantidades ingentes de información. Y dado que se trata de un número tan elevado de interactores y sus informaciones contribuyen a nutrir las cuentas de uno de los negocios más lucrativos de todos los tiempos, la reflexión es más que obligada.

2.2 SERVICIOS QUE OFRECE LA PLATAFORMA

Abordar el imparable ascenso de la compañía nos lleva a preguntarnos: ¿Qué hay detrás de este mareante baile de cifras? ¿Qué es lo que tiene Facebook que nos invita a volcar nuestra información privada y aceptamos convencidos? A diferencia del servicio de *microbloging* Twitter o la red social Tuenti[515], su análogo más cercano, dos de

---

513 Facebook España (2012): «Facebook supera los 900 millones de usuarios», en *Facebook Newsroom,* 2 de mayo de 2012. www.facebook.com/FacebookEspana. [08/02/2013].

514 ALEXA (2013): «Alexa Traffic Ranks». www.alexa.com/siteinfo/facebook.com. [08/02/2013].

515 Tuenti es una red social creada en 2006 que cuenta con más de 15 millones de usuarios registrados. Nació centrada en el público adolescente aunque, posteriormente, se amplió su uso a otros rangos de edad. Llegó a estar muchos años en lo más alto de las redes sociales de España y, de hecho, fue la más popular en España entre los años 2009-2012.

las claves que hacen de Facebook una comunidad tan exitosa son su facilidad de uso y que no está destinada a un público determinado de usuarios, como sí sucedía en los inicios con Tuenti. Su navegación fácil, lineal como la de un libro, posibilita que gentes de todo tipo, con mínimos conocimientos de informática, puedan manejarse en el sistema, a diferencia de lo que sucede con herramientas como Twitter que implican mayor dificultad. Asimismo, ofrece una serie de controles muy numerosos que hacen sentir al usuario seguro cada vez que comparte información, aun cuando, en realidad, solo un 25% de los usuarios los usan activamente[516].

El segundo punto fuerte y verdadero atractivo de Facebook son los participantes. El hecho de que la compañía sea la más poblada hace que resulte difícil resistirse a participar en el juego. No en vano, son sus habitantes los que sustentan su éxito frente a otras plataformas, a pesar de que los conceptos en los que se basa no son nuevos y muchos de los componentes de Facebook ya habían sido introducidos en anteriores redes sociales. Entre dichos servicios[517] podemos destacar:

— Lista de amigos: En ella el usuario puede agregar a cualquier persona que conozca y esté registrada en la plataforma, siempre y cuando acepte su invitación (el propio servidor de Facebook posee herramientas de búsqueda y de sugerencia de amigos). Con estos contactos se puede intercambiar fotos, mensajes y comentarios en el perfil, así como enviar contenidos a través de un servicio de mensajería instantánea o *chat* (Facebook Messenger) disponible tanto en dispositivos móviles como computadores de sobremesa.

— «Grupos» y «páginas»: constituyen dos de las utilidades de mayor desarrollo y su cuyo objetivo común es reunir personas con intereses comunes. Las páginas se crean con fines específicos y, a diferencia de los grupos, no contienen foros de discusión ya que están encaminadas hacia marcas o personajes específicos. Por su parte, en los grupos se pueden añadir fotos,

---

[516] GROSS, R. y ACQUISITI, A. (2005): *Op. cit.,* y QUAN-HASSE, A. (2013): *Op. cit.*

[517] Facebook.com. *Servicios que ofrece Facebook*. Disponible en: http://www.facebookla.com/2009/11/ servicios-que-ofrece-facebook.html [8/10/2012].

vídeos y mensajes, entre otros contenidos. Estos, además, también tienen su normativa entre la cual se incluye la prohibición de temáticas discriminatorias, que inciten al odio o que atenten contra la honra de las personas. Si bien estos requisitos no se cumplen en infinidad de ocasiones, existe la opción de denunciar y reportar los grupos que vayan contra esta regla, para lo cual Facebook incluye un enlace hacia un cuadro de reclamos y quejas.

— «Muro» y «biografía» (*Timeline*): El «muro» es un espacio dentro de cada perfil que permite que los amigos escriban mensajes e ingresen tanto imágenes como iconos para que el usuario los vea. En noviembre de 2011, Facebook comenzó a implementar un sustituto del muro que lleva por nombre «biografía» y que tiene como objetivo agilizar y optimizar la visita de los participantes a través de todos los perfiles de sus contactos. Contiene algunas mejoras como, por ejemplo, la fecha exacta de publicaciones, actualizaciones de estado y comentarios; y brinda la posibilidad de llegar a ellas casi de inmediato, aunque sean bastante antiguas. Permite, asimismo, agregar una foto de portada adicional en la parte superior del perfil de la persona. Esta es visible para todo el mundo y no existe la posibilidad de cambiar la opción de privacidad por defecto. Finalmente, la biografía mantiene ordenadas y organizadas las actividades de la persona: lista de amigos, los «me gusta» en las páginas seleccionadas por el usuario, información personal, suscripciones y un largo etcétera, por lo que es más fácil acceder a su información de manera jerarquizada.

— Botón «Me gusta»: Esta célebre función aparece en la parte inferior de cada publicación que realiza el usuario o sus contactos, ya sean actualizaciones de estado, contenido compartido u otros apartados. Aparece representado por un pequeño icono que simula una mano con el dedo pulgar hacia arriba y permite valorar si los contenidos publicados por cada participante son del agrado de sus contactos.

— Aplicaciones (*App Center*): existe una multitud de aplicaciones (*apps*) de terceras empresas integradas en la red social. Muestra los hábitos de cada persona, por cuanto muchas de ellas están relacionadas con su actividad diaria. Cada aplicación tiene una

página con su descripción que incluye imágenes y opiniones de usuarios. Destacan, entre otras populares, aplicaciones como *la galleta de la suerte, quien es tu mejor amigo* o todas aquellas que permiten descubrir cosas de la personalidad del usuario, así como las destinadas a juegos.

Existen muchos más servicios, pero estos constituyen los más emblemáticos de la plataforma. Sin embargo, circunscribir nuestro análisis de la potente maquinaria de Facebook sería quedarnos en la superficie. Vayamos un paso más allá y estudiemos el ideario que cimenta los pilares de la red social.

3. LA FILOSOFÍA DE LA COMPAÑÍA: FACEBOOK, EL GRAN *PANOPTICON* VIRTUAL

El ojo que ves
no es ojo porque tú lo veas;
es ojo porque te ve.
Machado, *Proverbios y Cantares*[518]

Según Richard Allan, director Facebook para la división europea, el espíritu que guía el quehacer de la plataforma se basa en el respeto a tres principios básicos: «control, transparencia y responsabilidad» [519], aplicables tanto al manejo y gestión de los datos personales como a sus comunicaciones con los usuarios. Podemos inferir, partiendo de esta filosofía, que es el individuo quien, *de facto,* detenta el control activo de sus informaciones privadas. Mientras que, por su parte, la compañía responde a los estándares de transparencia necesarios en el tratamiento de contenidos privados y comunicación de diligencias a cada miembro; al igual que se responsabiliza de todas aquellas eventualidades que pudieran poner en entredicho la salvaguarda del ámbito privado del sujeto.

No obstante, el estudio pormenorizado de las prácticas habituales de la compañía revela una ecuación bien distinta: la plataforma detenta el control y no es en absoluto transparente, ni a la hora de gestionar los datos de los usuarios, ni cuando se trata de comunicar

---

[518] MACHADO, A. (1923): *Proverbios y cantares* I, en *Revista de Occidente*, n. III, septiembre de 1923.

[519] ALLAN, R. (2012): *Op. cit.,* p. 164.

pertinentemente las prácticas que tienen lugar en sus confines. A su vez, elude toda clase de responsabilidades que recaen, exclusivamente, sobre el propio individuo, al que se despoja de protección alguna.

Dado que nos situamos en un escenario muy distinto del que se presupone de la asimilación de los dictados de la compañía, el relato del recorrido trazado entre una situación y la opuesta debería arrojar cierta certidumbre. No perderemos de vista dicho esquema y utilizaremos estas tres variables para vertebrar nuestra toma de contacto con Facebook, adelantando ya que obtendremos un sentido a estas palabras muy distinto al que usa la compañía.

3.1 LA FALACIA DE LA VISIBILIDAD Y LA TRANSPARENCIA

Uno de los lemas repetidos *ad nauseum* tanto en las políticas de privacidad como en las intervenciones públicas de los representantes de la compañía es que la transparencia masiva es la norma que guía y envuelve todo el servicio, dejando entrever que el interactor obtendrá, de manera clara y concisa, toda la información concerniente al manejo de sus informaciones reservadas. Ostentará, por tanto, el control de los propios datos personales que él mismo «decide» volcar en la red social, en tanto que conoce y es capaz de entender e interpretar el alcance del acuerdo de usuario y las condiciones del servicio que ha suscrito con la plataforma. En resumidas cuentas, dado que es plenamente consciente del tratamiento y uso al que se destinarán sus datos, será el responsable último de todos sus actos y las posibles consecuencias derivadas, dentro del marco definido por la empresa. La realidad, por el contrario, dibuja un lienzo bien diferente y, a pesar de las connotaciones agradables que se enlazan al uso de la palabra «transparencia», la apropiación de dicha voz posee otras lecturas nada desdeñables.

A primera vista, podemos entender —y esta es la baza que juega la compañía— que esa transparencia refiere a la accesibilidad de la información procedente de Facebook, es decir, que sus prácticas serán legítimas en tanto que nos informarán, de forma veraz, del uso que se dará a nuestros contenidos y que, además, nos lo comunicarán de la manera más apropiada para nuestro entendimiento. Esto se debe a que el concepto que engloba dicha voz tiende a confundirse, habitualmente, con «disponibilidad» de la información; sin embargo, acomu-

nar acceso y transparencia hace que nos olvidemos de otras connotaciones y realidades del fenómeno. De hecho, el que se mencionen todas las actividades de la compañía en interminables políticas de privacidad no es, en absoluto, sinónimo de que el usuario sepa qué se hace con sus datos. En otras palabras, no hay nada transparente en el acto de mostrar una cantidad ingente de información que el individuo no tiene tiempo material para leer, criterio para entender, ni marco referencial para contrastar. El simple hecho de que los datos se muestren desestructurados o como una mera acumulación de enunciaciones, genera resistencia, derivando, a la postre, en la consabida desinformación. Consiguientemente, no es lícito establecer una equiparación entre acceso y visibilidad de la información. Es algo similar a lo que nos ocurre cuando debemos interpretar una base de datos: si se nos presenta desestructurada, dicho amontonamiento neto de datos nos resulta, por definición, opaco.

Por otra parte, enarbolando la bandera de la tan manida transparencia la empresa consigue mover el foco hacia lo que le interesa destacar, eludiendo las posibles repercusiones derivadas de prácticas no legítimas en la transferencia y uso de datos por terceras empresas y/o con fines distintos a los que los destinó el usuario. Este fenómeno posee su epicentro en la mediación inherente a la estructuración del contenido informativo, en este caso, de las cláusulas de privacidad elaboradas por la compañía. La organización de la información suministrada nunca es neutral por lo que nos permitirá obtener un significado concreto e interpretarla en un determinado sentido. En definitiva, sí sacaremos algo en claro de la lectura de las condiciones del servicio, pero dicho mensaje condicionado arrojará luz, intencionalmente, sobre ciertas prácticas, a la vez que procederá a la ocultación de una serie de procedimientos no tan destacables.

El discurso de la transparencia funciona así como un potente lema que en realidad no aporta nada más que confusión. Y dado que la transparencia es, necesariamente, fruto del filtro previo de la mediación y no aparece por generación espontánea, observamos aquí la segunda falacia: lo que se muestra como evidente puede llegar a oscurecer la certeza. En suma, aunque resulte paradójico, la relación que se establece entre transparencia y opacidad no se produce siempre en términos de antagonismo, puesto que «poder ver» no significa «poder saber»; una asimilación que Facebook y otras aplicaciones de la Web 2.0 esgrimen para legitimar su negocio. Hablar de transparencia

nos impele, en consecuencia, a indagar en las mediaciones que la generan, propiciando que se hagan visibles unos datos o conclusiones en lugar de otros.

3.1.1 La exposición de la identidad en la retórica «zuckerbergiana» de la transparencia…

> La gente se ha acostumbrado a compartir más información
> y a hacerlo más abiertamente con más personas.
> La norma social es siempre algo que evoluciona.
> Zuckerberg, en los Crunchie Awards[520]

«Queremos ser transparentes [y que el usuario tenga el control]» [521], reza la política de privacidad de Facebook. Sin embargo, bajo el tamiz de esta visibilidad extrema, somos los propios interactores los que, al hacernos visibles, caemos en las redes de lo que es de todo menos evidente: el negocio que hay detrás de nuestras informaciones personales.

La plataforma Facebook propicia interacciones forzadas que tienen como objetivo explicitar el máximo de información de sus miembros. A tal efecto, los usuarios deben dar sus datos de manera concisa, descriptiva y veraz; al fin y al cabo, se trata de posibles compradores a los que mostrarles publicidad personalizada. Y para que los sujetos colaboren convencidos en dicha empresa, justificar la nombrada sobreexposición de la personalidad y evitar que los interactores recurran a dobles identidades, la compañía ha elaborado todo un ideario *ad hoc* al que poder remitirse, una filosofía que impregna toda la plataforma y que, de manera insistente, alude a la responsabilidad moral del individuo. Según explicaba el propio Zuckerberg en una entrevista concedida a David Kirkpatrick en 2009:

---

[520] MARK ZUCKERBERG durante una conferencia en los Crunchie Awards, en San Francisco. Declaraciones recogidas en: Johnson, B, (2010): «Privacy no longer a social norm, says Facebook founder», en *The Guardian*, 11 de enero de 2010.

[521] KIRKPATRICK, D. (2011): *Op. cit.,* p. 58. Kirkpatrick realiza una pormenorizada semblanza del pensamiento que Zuckerberg ha esbozado para legitimar las prácticas abusivas de su compañía.

> El nivel de transparencia que el mundo tiene hoy no permitiría que una persona tuviera dos identidades […] Los tiempos en que uno daba una imagen distinta a los colegas de trabajo y al resto de la gente, están llegando a su fin. […] Tienes una identidad […] Tener dos identidades demuestra falta de integridad. […] ¿Por qué no querría la gente compartir? ¿Por qué no querrían ser más abiertos? A no ser que tengas algo que ocultar, claro[522].

Dicho de otro modo, aunque uno quiera usar la red social con un nombre falso o desee separar lo profesional de lo privado, la plataforma no permite diferenciar entre los diversos ámbitos del ser humano, aun cuando estos aparecen enlazados habitualmente con distintas normas y usos sociales. Es decir, a diferencia de otras comunidades que se centran en el aspecto eminentemente profesional o, por el contrario, en el personal, y permiten separar con una cierta claridad dichos espacios, en Facebook se dan cita todas estas dimensiones del individuo, contribuyendo a la creación un completo dossier virtual altamente personalizado.

Por ende, esta plasmación íntegra de nuestra persona se completa con la exigencia al usuario de que actué con su nombre real, mostrando su identidad y personalidad ante la mirada del escaparate público. Una nueva conciencia que, para el periodista del diario *The New York Times,* Clive Thompson, «nos devuelve a la dinámica de la vida en los pueblos pequeños, donde todo el mundo sabe lo que haces»[523].

Esta retórica sobre las «bondades» del mundo accesible que Zuckerberg comenzó a esgrimir en 2008, acabó convirtiéndose en la bandera de la compañía. Lo repetía una y otra vez en sus intervenciones públicas y en las declaraciones a la prensa, como en un artículo de opinión en *The Washington Post* en el que rubricaba que compartir más información, incluyendo fotos, opiniones o fechas de cumpleaños harían del planeta «un sitio más abierto y conectado. Y un mundo que es más abierto y conectado es un mundo mejor»[524].

---

[522] Ibídem, pp. 237 y ss.

[523] THOMPSON, C. (2008): «Brave new world of ambient intimacy», en *The New York Times,* 7 de septiembre 2008.

[524] ZUCKERBERG, M. (2010): «From Facebook, answering privacy concerns with new settings», en *The Washington Post,* 24 de mayo de 2010.

La lectura soterrada va más allá de ese emblema *naïve*. Bajo esta aparente moralidad en la que se pide a los sujetos responsabilidad sobre sus actos en cualquier ámbito, incluso en aquellos desarrollados fuera del mundo virtual, no hay nada ético. El universo cristalino de Zuckerberg parte del supuesto de que en un mundo más abierto y transparente, en el que la gente asuma las consecuencias de sus actos, es un lugar más justo, aun cuando acercar a la gente a ese punto de transparencia extrema choque, radicalmente, con el amparo de la intimidad y vida privada. Y esa dinámica se plasma en el funcionamiento mismo de la plataforma. Facebook obliga a cada persona que se registra en la red a clarificar su identidad, a la vez que le agrega significados que completan, minuciosamente, su «yo» virtual, volviéndoles reconocibles y localizables. La realidad no tan amable que subyace revela que dicho acceso directo a nuestro «yo» responde a la necesidad de convertirnos en público objetivo de la publicidad personalizada, razón por la que a la empresa le interesa que introduzcamos nuestros datos correctos para poder asociar los mismos a una persona que, de verdad, existe. En resumidas cuentas, la retórica en la que se escuda el fundador de la compañía para justificar el funcionamiento de Facebook adolece de un tinte moralista poco creíble. El resultado es que, ya sea para bien o para mal, la compañía ha ido reconfigurando el binomio «visibilidad» *versus* «ámbito reservado» para deleite de la mirada ajena.

Esta exposición de la identidad sin precedentes comienza en 2006 con la introducción de una herramienta denominada «canal de noticias» (*News Feed*) y que permite mostrar todas y cada una de las actividades que realiza el usuario a su red de contactos u otros integrantes del sistema. Aunque en el próximo capítulo dedicaremos un apartado al estudio detallado de esta funcionalidad, sí resaltaremos ahora su importancia dado que se considera como la precursora de una importante transformación en la forma en que hoy los individuos comparten información. No en vano, creaciones como el canal de noticias provocan que la exhibición de la personalidad sea incontrolable, ya que, aunque uno mismo intente salvaguardar sus contenidos privados de la mirada pública, los comentarios propios o de otros contactos insertados en las acciones automáticas de Facebook pueden mostrar retales de la vida privada que el individuo creía protegidos, llegando incluso a contradecir su discurso social. Para David Kirkpa-

trick, el lugar donde la información se vuelve más transparente es en la aplicación de fotos:

> No hay manera de controlar si otra persona cuelga una foto tuya. Se puede eliminar la etiqueta identificativa y que provoca que esa información sea distribuida por tu lista de amigos, pero, en general, cuando la eliminas la noticia de tu etiquetado ya ha aparecido en el canal de noticias. Las fotos son visibles por defecto a menos que ajustes los controles de privacidad, lo que la mayoría de usuarios no hace. A pesar de eliminar la etiqueta la foto nunca se elimina[525].

Ante la controversia suscitada por esta herramienta, el fundador de la compañía recurrió a su habitual argumentación para disculparse, aludiendo a una motivación personal: «cuando creé Facebook, hace dos años, mi objetivo era ayudar a entender a la gente qué está ocurriendo en su mundo un poco mejor»[526]. Discurso que matizó posteriormente, reafirmando su necesidad de «ayudar a la gente a ser más abierta, [ayudándoles a] compartir más información»[527], esto es, suscribiendo de nuevo los pilares de su mundo accesible.

3.1.2 **…y la mirada del *Panopticon***

> La transparencia es solo el primer grado de la opacidad, un mínimo de corporeidad es necesario para que se transmita la luz.
>
> Goethe, *Teoría de los Colores*[528]

Transparencia en tanto que información, acceso y uso legítimo es lo que desea el usuario, a la vez que necesita salvaguardar sus datos que, en definitiva, conforman parte de su identidad virtual. Sin embargo, hemos observamos cómo al equiparar transparencia a visibilidad hay algo que se hace tremendamente evidente: la persona que hay detrás de dichas informaciones. Es por ello que, para el semiólogo Juan Alonso, estamos ante «la transparencia detestable, la del ser

---

525 KIRKPATRICK, D. (2011): *Op. cit.*, p. 249.
526 Ídem, p. 237.
527 ZUCKERBERG, M. (2010): *Op. cit.*
528 GOETHE, W. (1810): *Zur Farbenlehre*. En castellano (1999): *Teoría de los colores*. Madrid: Celeste.

humano», que nos muestra al hombre en un escaparate y le «despoja de toda protección»[529]. Y en este sentido Facebook es casi cristalino.

Esta «invivible transparencia»[530] posee un sentido único: la persona es expuesta tras las vitrinas de la red cual objeto de museo y junto a una leyenda explicativa que le añade significados. Dicha acumulación de significados provoca que cada personalidad virtual sea más o menos susceptible de convertirse en un potencial cliente de las empresas que venden sus productos a través la plataforma. Del mismo modo, cuantas más interacciones alimenten o produzcan estos sujetos, más valor le darán a la compañía. En sentido contrario, los usuarios no saben para qué sirve la recolección de datos que realiza la red; es más, ni siquiera son conscientes de las condiciones en las que se ejecuta, ni de los flujos de información que se dan en la plataforma. En última instancia, no poseen conocimiento suficiente que les capacite para tomar decisiones sobre si introducir o no sus datos. Así, esta transparencia desaparece al situamos al otro lado del espejo, en la óptica del usuario.

Si vamos más allá, observaremos que la cara menos amable de esta transparencia oculta su conversión en vigilancia. De hecho, la visibilidad total nos retrotrae de nuevo a la mirada totalitaria del *panóptico,* donde se supone que los presos no harán nada malo ya que creen que son vigilados en todo momento.

El diseño de Bentham muestra cómo la vigilancia puede ser un instrumento efectivo para el control social, pero solo en la medida en que los sujetos vigilados no tienen otra opción que la de someterse ellos mismos a la mirada vigilante del inspector. De este modo, «la 'aparente' transparencia posee un resquicio: el *panopticon* plantea una jerarquía de las miradas en la que el observador de la torre lo ve todo. Ese observador es la transparencia misma»[531]. La transparencia se presenta así como un dispositivo de control, en una relación muy

---

[529] ALONSO, J. (2015): «Mesa redonda: Vigilancia, secretos, transparencia, cultura, documentos, periodismo». *XV congreso de la Asociación Española de Semiótica*. 5 de mayo de 2015, UCM.

[530] AGUILAR, M. A. (2014): «La opacidad necesaria», en Albergamo, M. (ed.): *La transparencia engaña*, Madrid: Biblioteca Nueva, pp. 83-97, p. 85.

[531] RAYCO, G. (2014): «La transparencia como efecto de sentido», en Albergamo, M. (ed.): *Op. cit.,* pp. 99-115, p. 107.

distinta a la esgrimida por Richard Allan para satisfacer las prácticas abusivas de la red social.

3.2 LA FALACIA DEL CONTROL

> Tengo 4.000 correos electrónicos y sus contraseñas,
> fotos y números de seguridad social.
> La gente confía en mí
> Marc Zuckerberg[532]

Todas las invenciones humanas tienen alma. Y, para bien o para mal, esta suele ser la de sus creadores así que si atendemos a las declaraciones públicas de Marc Zuckerberg podemos hacernos una idea de lo que se puede esperar de la plataforma Facebook. Michael Zimmer, director del *Centre for Information Policy Research*, narra en su página Web cómo se siguen en la compañía las directrices del fundador sobre la creación del mundo accesible:

> En 2011, estuve en las oficinas centrales de Facebook, en Palo Alto, California, para participar en un encuentro del *Future of Privacy Forum*, una organización ubicada en Washington. Allí se dieron cita varios ingenieros de Facebook, así como directores de publicidad y ejecutivos de políticas públicas de la compañía. Todos estos empleados de Facebook fueron preguntados por las preocupaciones relativas a la protección de la intimidad y vida privada, en una sala llena de defensores de la privacidad, pero ni una sola persona pronunció nunca la palabra «*privacy*» en sus respuestas a nuestras preguntas. Por contra, hablaban de «control del usuario» o «opciones del usuario» o promovían la apertura de la plataforma. Era como si un memorándum hubiera estado circulando aquella mañana para indicarles que no usasen nunca la palabra «*privacy*»[533].

Tras la experiencia en la que nunca pudo preguntar directamente al padre de la criatura, Zimmer decidió lanzar el proyecto: *The Zuckerberg Files*[534], un archivo con todas sus apariciones públicas —y no tan públicas— como blogs, cartas a los accionistas, entrevistas en medios y presentaciones, en las que comparte su particular visión de la

---

[532] Zuckerberg citado en «El efecto Facebook la historia oculta: la gente confía en mí, son tontos del culo», en *El Economista,* 30 de mayo de 2010.

[533] ZIMMER, M. (2014): *Op. cit.,*

[534] Los «*Archivos Zuckerberg*» se pueden consultar en: http://zuckerbergfiles.org.

protección de la vida privada. Y el resultado fue demoledor: Zuckerberg había afirmado categóricamente proclamas tan impactantes como «que la era de la vida privada había muerto»[535] o que «si volviera a crear Facebook lo haría todo público por defecto»[536]. Entre estas intervenciones, en las que tanto Zuckerberg como sus colaboradores rehúsan mencionar la palabra *privacy* más que para anunciar su extinción, destaca la que protagonizó como portada de la revista *Time*, «Mark Zuckerberg: 2010 Person of the Year». Teniendo en cuenta que gran parte de la charla versa sobre las injerencias en el ámbito reservado de los usuarios, la mención a la citada palabra parecía ineludible. Sin embargo, lo más parecido que hace Zuckerberg es hablar de «control», alegando que «lo que la gente quiere no es privacidad completa, ni secretismo, lo que quieren es control sobre lo que comparten y lo que no» [537].

Según Lev Grossman, autor de la entrevista, el jefe supremo de Facebook tiene un talento innato para entender cómo trabaja la gente, pero algo tan necesario como la necesidad de mantener un espacio secreto a los ojos de los demás parece ser un sentimiento ajeno a él: «A veces, Zuckerberg actúa como el portavoz de la policía secreta de algún futuro estado totalitario»[538].

Centrándonos en el uso del término «control», este no es casual. Responde a otra de las estrategias de la compañía para evitar hablar de la controversia que les vincula a la vulneración de la vida privada de los usuarios, trasladando a estos un poder endeble que, en última instancia, se traduce en responsabilidad sobre cualquier injerencia acontecida. De hecho, en sus múltiples y polémicos cambios en las condiciones del servicio, la red social utiliza este subterfugio para afrontar las quejas de distintos organismos, desde grupos en defensa de los derechos civiles hasta los propios miembros del sistema. Sólo por citar un ejemplo, en respuesta a las críticas recibidas en 2009 por modificar las condiciones del servicio sin previo aviso, Zuckerberg

---

[535] JOHNSON, B. (2010): *Op. cit.*

[536] KIRKPATRICK, M. (2010): «Facebook's Zuckerberg Says The Age of Privacy is Over», en *Readwrite*, 9 de enero de 2010.

[537] GROSSMAN, L. (2010): «Person of the Year», en *Time,* 15 de diciembre de 2010.

[538] Ídem.

rectificó mediante un apartado titulado: «en Facebook, la gente controla y es propietaria de su información» [539].

El inconveniente de la filosofía esgrimida por Zuckerberg es que, en los diez años de historia de la plataforma, la habilidad de controlar los contenidos privados por parte de los miembros ha decrecido ampliamente. Las opciones de privacidad por defecto son más abiertas y, cada vez más, los servicios integrados de terceras empresas extienden la información de los usuarios fuera de los confines de la red, perdiendo los individuos no solo el citado control sobre sus propios datos, sino todos sus derechos. Y esta práctica viene respaldada por unas políticas de privacidad y términos del servicio confusas y tremendamente abusivas.

3.2.1 Las políticas de privacidad y condiciones del servicio: cláusulas abusivas y cambios sin previo aviso

La vida privada se ha acabado. Asimílalo.
Scott McNealy [540]

«Política de privacidad», «Licencia y términos de uso», «Política de protección de datos», «Condiciones del servicio», «Política de datos» … Cuando mencionamos el pliego de cláusulas de Facebook resulta complicado averiguar si quiera a qué debemos remitirnos exactamente; más aún si tenemos en cuenta no solo su heterogeneidad, sino el amplio catálogo de cambios que la empresa ha acometido desde su comienzo. En suma, y aun cuando son el centro de la polémica que rodea a Facebook, estos pliegos de condiciones son un mosaico de retales difícil de ver en su totalidad. Sin embargo, si hemos seguir un hilo conductor para desenmarañar la madeja de la incertidumbre, este sería sin duda la progresión de las configuraciones por defecto que se derivan de las actualizaciones en las condiciones del servicio.

---

[539] CHAN, K. (2009): «People own and control their information», *Facebook Blog*, 16 de febrero de 2009.

[540] En algún momento tendríamos que acabar citando la manida frase «You have zero privacy anyway. Get over it» de Scott McNealy, presidente de Sun Microsystems, y que ya es un clásico en cualquier escrito sobre tecnologías digitales y protección de la esfera privada. SPRENGER, P. (1999): «Sun on Privacy: 'Get Over It'», en *Wired,* 26 de enero de 1999.

Dichos cambios siempre se han dado en un mismo sentido: hacia la mayor visibilidad del sujeto, el incremento de la optimización de los datos recabados con fines comerciales y unas capacidades superiores de intercambio de información con terceros.

Como hemos comentado anteriormente, en la mayoría de los casos estas modificaciones en las cláusulas vienen motivadas por la necesidad de no perder usuarios y/o para sortear los posibles problemas legales. Así tratan de adaptarse a normativas más proactivas en la protección de la intimidad y vida privada, cediendo ante las presiones de organismos y grupos civiles que defienden estos derechos. Sin embargo, como coloquialmente suele decirse, quien hace la norma, hace la trampa y el resultado final es que Facebook propone unas políticas poco claras en las que da al individuo un control «mediado» sobre sus propios datos y que no puede ejercer de manera efectiva. Al revestir el servicio con esa supuesta seguridad, le vuelve mucho más vulnerable; la desinformación es lo que tiene.

Por otra parte, resulta palmario que Facebook esconde muchas trampas a lo largo de las diferentes actualizaciones de sus condiciones del servicio. Estas se presentan con una redacción ambigua en la que abundan frases carentes de contenido e, incluso, contradictorias. El lenguaje utilizado, aunque pretendidamente simple, está sembrado de retruécanos y vaguedades entre las que prolifera el uso de expresiones que alimentan la duda como, por ejemplo: «puede que usemos sus datos…», «en ocasiones sus datos pueden usarse para…» o «en general, se entiende que si no hay un icono para compartir, la información será pública» [541]. Una miríada de imprecisiones enunciativas que revelan que el individuo no detenta realmente ningún control sobre su información. Y eso que estamos hablando de contratos, es decir, hay dos partes firmantes que, en principio, deberían comprender los términos de lo acordado. Esta práctica, inmersa en un proceso de apertura por defecto de la información que detallaremos a continuación, nos revela que el mito del control no es más que una creación utópica destinada a justificar un negocio sustentado en lo ilegítimo.

---

[541] Facebook. Licencia y términos de uso. https://es-es.facebook.com/legal/terms?locale=es_ES.

3.2.2 Los controles de configuración de «privacidad»[542]: la vida privada se vuelve pública «por defecto»

Significados en los iconos de una bola del mundo, siluetas humanas, una tuerca o un candado, Facebook ofrece una serie de controles para que el usuario decida qué miembros de la plataforma tendrán acceso sus publicaciones. Si bien es cierto que estos controles eran algo rudimentarios al principio, en la actualidad permiten realizar muchas combinaciones, alternando entre la visibilidad total en ciertas publicaciones y una elección más personalizada en otras en las que es posible compartir información solo con unos contactos determinados. Admite, incluso, modificar estas configuraciones *a posteriori,* es decir, una vez que la publicación ya se ha hecho visible.

De este modo, el individuo puede elegir quién accede al contenido volcado, jerarquizando la vida social entre: acceso «público», esto es, a todos los miembros del sistema; «amigos de mis amigos», si deseamos que sea visible para contactos de tercer grado; solo para «amigos», si queremos que únicamente lo vean nuestros contactos; «personalizado», para seleccionar exclusivamente a algunas personas de entre todos los contactos o, incluso, se nos permite usar la categoría «sólo yo» en algunas publicaciones y para ciertos datos. Así según la compañía, cada participante comparte solo lo que «desea» mostrar, en tanto que tiene la posibilidad de dominar de manera eficaz la visibilidad de sus contenidos, al aplicar las configuraciones de privacidad a su antojo:

> Facebook ha sido diseñado para que te resulte sencillo compartir información con quien tú quieras. Tú decides cuánta información deseas compartir en Facebook, y tú controlas su distribución a través de tu configuración de privacidad. Debes comprobar la configuración de privacidad predeterminada y cambiarla si es necesario para adaptarla a tus preferencias. También debes tener en cuenta esta configuración siempre que compartas información. […] Facebook no es un simple sitio Web. Se trata de un servicio mediante el cual puedes compartir

---

[542] Al igual que ya comentamos en el capítulo precedente al hablar de «políticas de privacidad», usaremos aquí la misma voz, traducción literal de *privacy*, para evitar equívocos, ya que es la que la plataforma utiliza en sus pliegos de condiciones para referirse a las configuraciones que controlan la visibilidad de la información.

> información en sitios Web y aplicaciones que están vinculados con Facebook. Puedes controlar cómo compartes información con estos sitios Web y aplicaciones de terceros a través de la configuración de las aplicaciones e informarte sobre cómo se comparte la información con ellos en nuestra página. […] También puedes limitar el modo en que tus amigos comparten tu información con aplicaciones mediante la configuración de privacidad[543].

En consecuencia y al igual de lo que sucede en otras actualizaciones de las políticas de privacidad, los enunciados como el anteriormente citado retratan al usuario bajo un *role* activo en la preservación de sus propios contenidos: está informado y puede modificar eficazmente el acceso a sus datos, *ergo* él es quien decide. Se construye así la ilusión de dominio gracias a una redacción en la que se enumeran con plétora expresiones como: «información que [tú] 'decides' hacer pública» y otras de similar talante, y que se materializa en una serie de botones como los plasmados en el siguiente ejemplo.

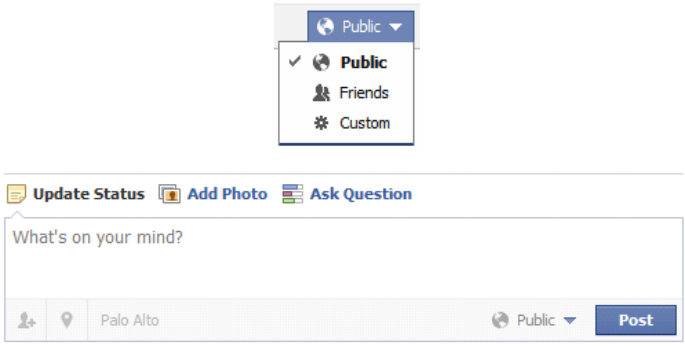

Figura 6.2 Controles de configuración de privacidad para las publicaciones de los usuarios[544]

Esta es, por tanto, la segunda falacia de la que se vale Facebook para legitimar su empresa: hacer creer al sujeto que al otorgarle estos controles tiene el poder de decidir y controlar qué será visible. Lo no tan evidente es que la compañía posee estrategias muy potentes para

---

[543] TOSBACK (2009): *Política de privacidad de Facebook, 29 de octubre de 2009*. Disponible en: http://www.tosback.org/version.php?vid=961/ «http://www.facebook.com/privacy/» [14/02/2010].

[544] Fuente: Facebook.

hacerse con el control de más datos de los que el usuario imagina. Por otra parte, la existencia de dichas configuraciones no significa que el individuo sea el dueño del contenido y pueda retirarlo cuando desee. Es más, una de las mayores polémicas que rodea el negocio de las redes sociales nace del hecho de que el sujeto cede la propiedad de su información, lo que a la larga significa que la plataforma podrá usarlas cómo y cuándo estime conveniente:

> Al publicar una foto se concede una licencia, no exclusiva, transferible, con posibilidad de ser subotorgada [sic], sin royalties, aplicable globalmente para utilizar cualquier contenido de propiedad intelectual que publiques en Facebook. Esta licencia finaliza cuando eliminas la cuenta (aunque Facebook guarda una copia de tus fotos) o el contenido, pero no así cuando se ha compartido con terceros y estos no lo han eliminado[545].

Volviendo a esos controles que en principio posibilitan que el usuario muestre solo lo que desea hacer accesible, Facebook los actualiza junto con sus políticas, cada cierto tiempo, bajo el lema de otorgar más seguridad a los miembros del sistema. No obstante, en la década que lleva operando la plataforma la capacidad de control que los individuos son capaces de ejercer sobre sus datos ha decrecido ampliamente, toda vez, que las configuraciones de privacidad son cada vez más abiertas: hacen la información más visible y lo que es más preocupante, lo hacen bajo la configuración «por defecto». En cada etapa, asevera Mark Rotenberg, «Facebook se propone hacer más difícil que necesaria la protección del usuario»[546].

Kurt Opsahl, abogado de la Electronic Frontier Foundation, escribió un ilustrativo artículo titulado: «Facebook's Eroding Privacy Policy: A Timeline»[547], en el que plasmaba cómo las políticas de privacidad de la red social han evolucionado hacia esa peligrosa visibilidad que sienta las bases del mundo accesible de Zuckerberg. La simple comparación entre el período comprendido entre 2005 y 2010, ciclo

---

[545] *Política de privacidad de Facebook de 2014*. https://www.facebook.com/terms.php?locale=es_ES

[546] Mark Rotenberg, declaraciones vertidas en la página de la Electronic Privacy Information Center (EPIC). Disponible en: https://epic.org/privacy/facebook/ [02/01/2012].

[547] OPSAHL, K. (2010): «Facebook's Eroding Privacy Policy: A Timeline» *Electronic Frontier Foundation,* 30 de abril de 2010. Disponible en: https://www.eff.org/es/deeplinks/2010/04/facebook-timeline [12/03/2011].

que coincide con las modificaciones más significativas, explica cómo dichos cambios quebrantan de manera flagrante el supuesto control que la red afirma adjudicar a sus moradores.

Para ilustrar estas afirmaciones, nada mejor que observar la evolución de ese contrato que «firma» el usuario al entrar a formar parte de la red social, entrelazando los textos de las políticas de privacidad con la representación visual de su evolución.

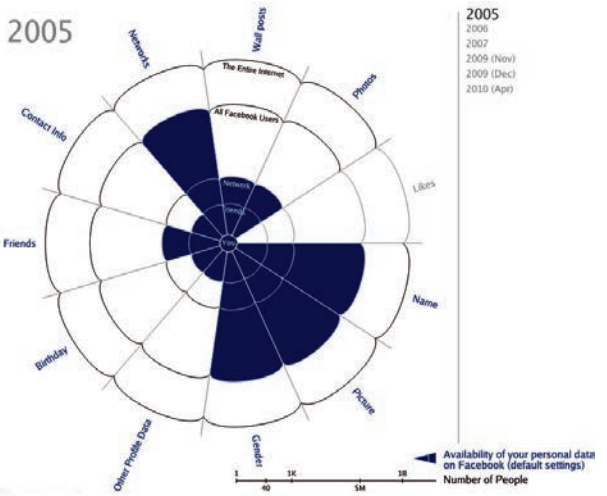

Figura 6.3 Configuración de los controles de privacidad por defecto de Facebook, año 2005[548]

Esta es la configuración de Facebook por defecto en 2005, divida en doce categorías en las que lo que aparece sombreado es lo que el usuario comparte de manera pública por defecto. Tal y como explicaba en su política de privacidad:

> La información que [tú] introduces en *Thefacebook* no estará disponible a ningún usuario de la Red [de Facebook] que no pertenezca, al menos, a uno de los grupos especificados por ti en tus configuraciones de privacidad[549].

---

[548] Fuente: MCKEON, M. (2010): «The Evolution of Privacy on Facebook. Changes in default profile settings over time». Disponible en: http://mattmckeon.com/facebook-privacy/ [10/01/2011].

[549] Archive.org (2007): *Política de privacidad de Facebook, 2005*. Disponible en: http://Web.archive.org/Web/20050809235134/www.facebook.com/policy.php [14/02/2010].

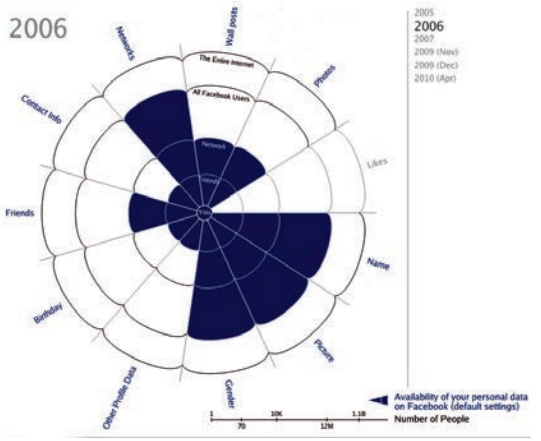

Figura 6.4 Configuración de los controles de privacidad por defecto de Facebook, año 2006[550]

Política de privacidad de Facebook en 2006:

> Entendemos que [tú] puedes no querer que todo el mundo tenga la información que compartes en Facebook, por este motivo le damos control sobre tu información. Nuestras configuraciones de privacidad por defecto limitan la información desplegada en tu perfil ciñéndola a tu colegio universitario, tu área local específica así como otras posibles limitaciones comunitarias de las que le hemos informado[551].

Simples y efectivas, tanto las condiciones de 2005 como las de 2006 son las que más cobertura y garantías otorgaban a los miembros de la plataforma. No deja de ser paradójico que cuando Facebook era un sitio solo para estudiantes de Harvard la protección de la información privada era más conservadora. De hecho, en 2005 ni siquiera existía algo similar a un perfil público que todo el mundo pudiera ver. O se era usuario de Facebook y esto permitía acceder a un grupo selecto de gente o, simplemente, no se estaba en la plataforma.

Por el contrario, a partir de 2006 los participantes ven como las opciones para mantener sus datos personales a buen recaudo empiezan a mermar, a la vez que desaparecen las opciones de privacidad en

---

[550] Fuente: MCKEON, M. (2010): Ibídem.

[551] Archive.org (2007): *Política de privacidad de Facebook, 2006*. Disponible en: http://Web.archive.org/Web/20060406105119/http:/www.facebook.com/policy.php [14/02/2010].

muchos apartados que se vuelven universalmente accesibles por defecto. No es por ello sorprendente que, a medida que la plataforma empieza a expandirse, aparezcan las primeras sospechas sobre el verdadero uso al que Facebook destina los datos recabados.

Veamos ahora como aumenta a partir de 2006 la cantidad de información que los usuarios comparten por defecto:

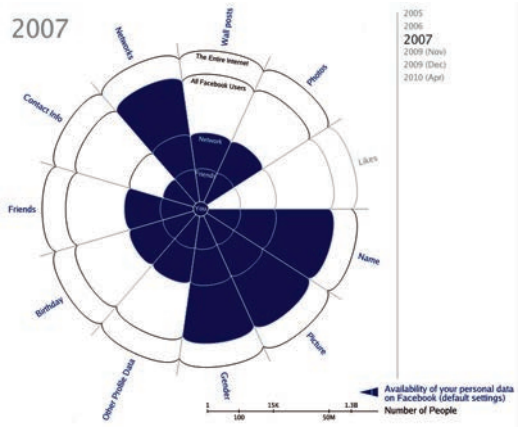

Figura 6.5 Configuración de los controles de privacidad por defecto de Facebook, año 2007[552]

Política de privacidad de Facebook en 2007:

> La información de perfil que [tú] introduces en Facebook estará disponible a usuarios que pertenezcan a, al menos, una de las redes a las que [tú] permites acceder a la información a través de tus configuraciones de privacidad (por ejemplo, colegio universitario, ámbito geográfico, amigos de amigos). Tu nombre, el nombre de tu universidad e imagen de perfil estarán disponibles en los resultados de búsqueda a través de la red de Facebook si tú no cambias las configuraciones de privacidad por defecto[553].

Uno de los datos más significativos que aparece en esta actualización de 2007 es la apertura por defecto de perfiles públicos a la indexación de motores de búsqueda[554]. Aunque la configuración de pri-

---

[552] Fuente: MCKEON, M. (2010): Ibídem.

[553] Archive.org (2007): *Política de privacidad de Facebook, 2007*. Disponible en: http://Web.archive.org/Web/20070118161422/ http:/www.facebook.com/policy.php. [14/02/2010].

[554] BBC (2007): «Facebook Opens Profiles to Public» en *BBC Online*, 6 de septiembre de 2007.

vacidad sí permitía bloquear esta opción, cuando los usuarios se habían percatado del cambio sus fotos ya estaban en los resultados arrojados por Google y otros buscadores de Internet. Si además se había introducido algún otro contenido bajo la configuración «todos» como, por ejemplo, la participación en un evento, esta información también se asociaría al individuo fuera de los límites de la plataforma.

El cambio no era, en absoluto, baladí. Los miembros de la red social se había vuelto fácilmente accesibles, un hecho que ya entonces se verificó en el programa de la BBC, *Watchdog,* en el que se pudo comprobar lo sencillo que resultaba averiguar información personal de alguien simplemente escribiendo su nombre en Google. Y dichos contenidos eran accesibles para cualquier interactor[555], pero su propietario no podía ejercer control, ni rectificación alguna sobre ellos.

No obstante y aunque las repetidas denuncias en medios de comunicación forzaron que la compañía rectificase estas condiciones y volviera a introducir opciones de configuración de privacidad, cierta información como el nombre de usuario, el sexo, foto de perfil y redes, continuaron siendo públicos[556].

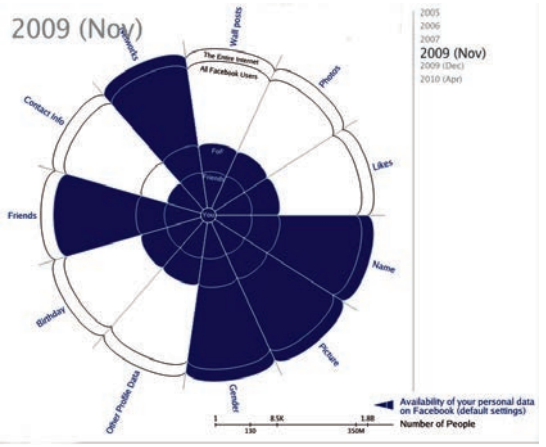

Figura 6.6 Configuración de los controles de privacidad por defecto de Facebook, octubre de 2009[557]

---

[555] BBC (2007): «Facebook security», en *BBC Online*, 24 de octubre de 2007. [10/11/2010].

[556] Facebook: «Controlling How You Share». Modificación de 2010. http:// www.facebook.com/privacy/ explanation.php [08/02/2010].

[557] Fuente: MCKEON, M. (2010): Ibídem.

Política de privacidad de Facebook de octubre de 2009:

> Facebook ha sido diseñado para que te resulte sencillo compartir información con quien tú quieras. Tú decides cuánta información deseas compartir en Facebook, y tú controlas su distribución a través de tu configuración de privacidad. Debes comprobar la configuración de privacidad predeterminada y cambiarla si es necesario para adaptarla a tus preferencias. También debes tener en cuenta esta configuración siempre que compartas información. […] La información compartida con «todos» permanecerá accesible y visible para todo aquel que entre en Internet (incluidas las personas no registradas en Facebook) queda sujeta a indexación por parte de motores de búsqueda de terceros, puede asociarse contigo fuera de Facebook (al igual que cuando visitas otras páginas de Internet) y puede ser importada y exportada por nosotros o por otros usuarios sin limitaciones de privacidad. La configuración de privacidad predeterminada para ciertos tipos de información que publicas en Facebook está establecida en «todos». Puedes revisar y modificar la configuración predeterminada en tu configuración de privacidad. Si eliminas el contenido compartido con «todos» previamente publicado en Facebook, lo borraremos de tu perfil de Facebook, pero no podemos controlar su uso fuera de Facebook[558].

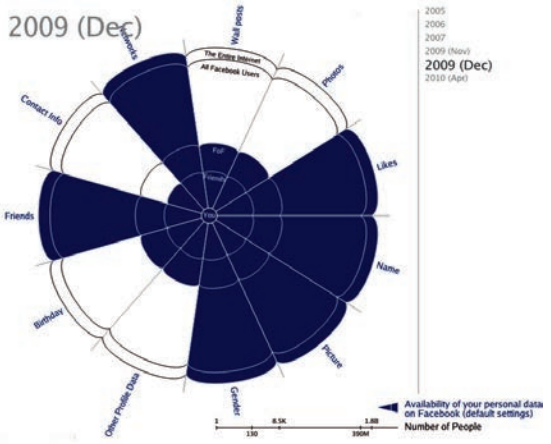

Figura 6.7 Configuración de los controles de privacidad por defecto de Facebook, diciembre de 2009[559]

---

[558] TOSBACK (2009): Política de privacidad de Facebook, 29 de octubre de 2009.

[559] Fuente: MCKEON, M. (2010): Ibídem.

Política de privacidad de Facebook de diciembre de 2009:

> Algunas categorías de información como su nombre, foto de perfil, lista de amigos, páginas de las que se hace, género, región geográfica y redes a las que pertenece están consideradas información públicamente disponible a todo el mundo, incluyendo aplicaciones que funcionan en la plataforma Facebook, y por lo tanto, no tienen configuración de privacidad. [Tú] puedes, sin embargo limitar la posibilidad de otros de encontrar esta información usando sus configuraciones de privacidad en lo que respecta a la búsqueda[560].

En 2009, Facebook comienza a compartir información personal por su cuenta con todo Internet. Sin embargo, todavía queda dar un paso más para llegar a ese anhelado mundo accesible anunciado por Zuckerberg. Algo que ocurrirá con el siguiente cambio:

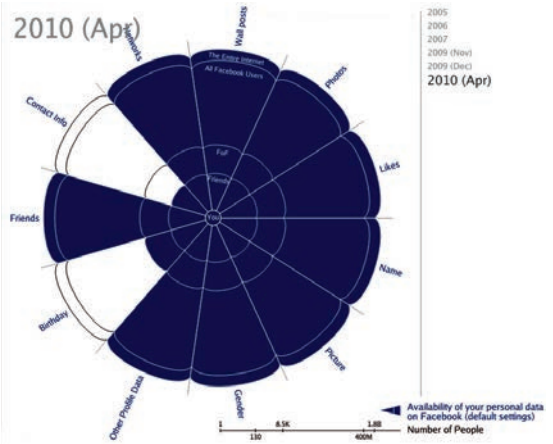

Figura 6.8 Configuración de los controles de privacidad por defecto de Facebook, año 2010[561]

Política de privacidad de Facebook, abril de 2010:

> Cuando te conectas con una aplicación o sitio Web este podrá acceder a la información general sobre ti. El término información general incluye tu nombre y el de tus amigos, vuestras imagines de perfil, género

---

[560] EFF (2010): *Política de privacidad de Facebook, 9 de diciembre de 2009*. Disponible en: https://www.eff.org/deeplinks/2010/04/handy-facebook-english-translator» \l «pages» [19/04/2010].

[561] Fuente: MCKEON, M. (2010): Ibídem.

> e identificador de usuario, conexiones y cualquier contenido compartido utilizando la configuración de privacidad «todos». Para ciertos tipos de de información, los controles de privacidad por defecto están establecidos en «todos». […] Si está incómodo con que estas conexiones estén disponibles públicamente, debería considerar eliminarlas o directamente no efectuar dicha conexión[562].

Puestas en conjunto, las sucesivas políticas parecen narrar un discurso meridiano: Originariamente Facebook ofrecía unos controles simples y eficaces; pero, a medida que comienza a expandirse, en vez de optar por mantenerlos o incluso mejorarlos, se decidió limitar el control de los usuarios en favor del uso que terceras empresas, socios comerciales y la propia plataforma pudieran obtener de ellos. El libro de caras ha pasado de ser un espacio acotado destinado a que los estudiantes de las universidades suscritas pudieran comunicarse con un grupo determinado de contactos, a una plataforma usada por todo el mundo en la que mucha de la información vertida es hecha pública por defecto. Y esta es la misma dinámica que ha seguido la red social en sus siguientes años de maduración. De hecho, aunque en el presente año 2014 Facebook ha anunciado cambios en sus aspectos más controvertidos, la filosofía del mundo accesible sigue impregnando sus pilares básicos:

> Cuando te registras en Facebook, te pedimos que introduzcas ciertos datos como, por ejemplo, tu nombre, dirección de correo electrónico, fecha de nacimiento y sexo. En algunos casos, es posible que puedas registrarte utilizando otro tipo de información, como tu número de teléfono. Tu nombre, fotos del perfil, fotos de portada, sexo, redes, nombre de usuario e identificador de usuario se tratan del mismo modo que la información que decides hacer pública. […] Cuando usamos el término «información pública» (al que en ocasiones nos referimos como «información que se comparte con todos») estamos hablando de la información que decides hacer pública, así como la información que está siempre disponible públicamente[563].

Sin embargo, desde la red social no se especifica, por ejemplo, que la configuración de los distintos servicios que ofrece Facebook viene

---

[562] EFF (2010): *Política de privacidad de Facebook, abril de 2010*. Disponible en: https://www.eff.org/ deeplinks/2010/04/handy-facebook-english-translator» \l «connections [10/01/2011].

[563] *Política de privacidad de Facebook, actualización de 2014*. Disponible en: https://es-es.facebook.com/ about/privacy/update [12/05/2014].

definida como «información pública» por defecto y que es el propio individuo el que debe modificarla si no desea que esta sea accesible. La empresa se escuda en el revestimiento del usuario bajo un supuesto rol activo mientras se cubre las espaldas afirmando:

> Si decides hacer pública esa información esta puede aparecer cuando alguien hace una búsqueda en Facebook o en un motor de búsqueda público, puede asociarse contigo (es decir, tu nombre, fotos del perfil, fotos de portada, biografía, identificador de usuario, nombre de usuario, etc.) incluso fuera de Facebook y estará accesible para los sitios Web, aplicaciones y juegos integrados en Facebook que utilizáis tú y tus amigos[564].

Como ya es habitual en su discurso, esta asunción concluye de manera tan confusa que es imposible saber lo que será público y lo que no; llegando a contradecir, incluso, todo lo anteriormente expuesto:

> En ocasiones, cuando publiques algo (como cuando escribas en el muro de una página o comentes un artículo periodístico que incluye nuestro *plugin* de comentarios) no podrás elegir un público concreto. Esto se debe a que algunas historias son siempre públicas. En general, se entiende que si no hay un icono para compartir, la información será pública. Cuando otras personas comparten información sobre ti, pueden optar a hacerla pública[565].

El resto de cláusulas parecen haberse vuelto, si cabe, aún más obtusas y ambivalentes, por lo que acabaríamos antes resumiendo que es del todo imposible saber qué controles han sido modificados para hacerlos públicos por defecto. En pocas palabras, el resultado es que los nuevos controles de privacidad están diseñados para que el individuo comparta aún más información, es decir, Facebook muestra cada vez más aspectos de la personalidad de sus habitantes sin que ellos mismos lo sepan. Y, dado que el truco que usa la compañía es no informar adecuadamente, el negocio se mantiene indemne mientras la responsabilidad de los actos acometidos recae en los habitantes de la red social.

3.3 LA RESPONSABILIDAD

Cabe inferir, tras todo lo anteriormente expuesto, el verdadero alcance que tendrá la responsabilidad que se arroga la compañía: poco

---

564 Ídem.
565 Ídem.

o nada podrá echarle en cara el usuario cuando ciertas prácticas dejen al descubierto retazos de su vida privada. Este tercer punto constituye la deriva lógica de los dos estadios anteriores, puesto que se entiende que un individuo que previamente ha recibido información suficiente sobre cómo se gestionarán sus contenidos y cuenta con las herramientas necesarias para manipular la visibilidad de estos a su antojo, será, consiguientemente, dueño de sus acciones y podrá responder por sus actos. Este razonamiento desemboca en una total exención de responsabilidad por parte de la empresa gracias a una situación recreada convenientemente por sus portavoces y en la que se insiste en que cada miembro de la red social cuenta con toda la información necesaria para entender el funcionamiento y comprender los flujos de trasvase de datos que se dan en la plataforma (información que, recordemos, es fruto de esa transparencia por definición mediada). Del mismo modo, se entiende que podrá satisfacer sus deseos de visibilidad, resguardando sus contenidos mediante los controles proporcionados. La plataforma pone los medios y el sujeto, supuestamente informado, decide y actúa en consecuencia.

Sin embargo, existe una muestra flagrante de que dicho negocio no es tan cristalino como promulgan sus defensores: aun cuando las anteriores condiciones colmasen los niveles de protección requeridos por los usuarios (algo que, por cierto, no sucedía) dado que el elemento a preservar constituye un derecho inalienable del individuo, este debe otorgar siempre su permiso respecto a la utilización de sus datos; especialmente, cuando estos son destinados a otros fines. Dicho punto, cardinal para garantizar el tratamiento legítimo de los datos personales, nunca se materializa de manera correcta en las redes sociales. Para ilustrar pertinentemente este punto, examinemos en qué momento nos solicitan permiso para el uso de nuestros contenidos.

3.3.1 **El consentimiento del usuario**

En el ideario de Facebook se repite hasta la saciedad que se trata de «un servicio gratuito que se financia a través de la publicidad» [566]. Seguidamente, se añade:

---

[566] TOSBACK (2009): *Política de privacidad de Facebook, 29 de octubre de 2009*.

> No compartimos información sobre ti con anunciantes sin tu consentimiento. No compartimos esta información con otros a menos que nos hayas dado tu permiso; te hayamos advertido, como informándote de ello en esta política, o hayamos eliminado tu nombre y cualquier otro dato por el que se te pueda identificar[567].

Muchos lectores se estarán preguntando ahora: ¿En qué momento se da ese consentimiento? ¿Lo pedirán cuando vayan a usar datos del usuario? ¿Lo habrán hecho ya? Pues bien, si no recuerdan en qué momento la plataforma les pidió autorización es porque, simplemente, nunca lo hizo. Al igual que la gran mayoría de las aplicaciones de Internet, la red social utiliza el sistema de consentimiento pasivo *(Opt-out)* lo que implica que el interactor no es preguntado sobre si se pueden usar sus datos, sino que se da por hecho que si no manifiesta lo contrario y sigue usando el servicio, otorga su aquiescencia. Y, dado que dicho consentimiento no es explícito en la mayoría de redes sociales, al firmar el acuerdo de usuario y aceptar las condiciones del servicio, también se está dando el asentimiento para el uso y disfrute de nuestras informaciones. Rizando el rizo, veremos que en el caso de Facebook ni siquiera es necesario dar la aprobación sobre las condiciones del servicio, sino que estas se dan por asumidas una vez que el individuo decide abrir una su cuenta en la plataforma. Así, bajo las lentes de las compañías de redes sociales, el uso y revelación de la información personal, incluso cuando se destine a fines distintos a los que motivaron su introducción, estaría auspiciado por el propietario de los contenidos quien, supuestamente, cuenta con la información adecuada para valorar cada escenario:

> Para los servicios en los que la gente ejerce un control específico cada vez que comparte los datos, la proporción de información contextual representa un modelo efectivo de obtención de un consentimiento valioso. Facebook se ha esforzado al máximo por garantizar que su política de uso de datos se explique de forma clara y comprensible, con información adaptada a los distintos grupos de edades[568].

Desde la óptica del interactor, no obstante, esta práctica solo refleja la ilegitimidad de sacar provecho económico de una materia prima que ha sido sustraída sin mediar consentimiento expreso. Con todo, la

---

[567] *Política de privacidad de Facebook, actualización de 2014.*
[568] ALLAN, R. (2012): *Op. cit.,* p. 165.

única certeza que parece derivarse del proceder de la compañía es que no informa debidamente a los miembros del sistema a quienes se les ha denegado la posibilidad de dar su asentimiento explícito y de manera informada. De este modo, aunque el usuario puede llegar a creer que al registrarse en la plataforma su información nunca será usada sin una notificación previa, dado que no existe ningún tipo de advertencia previa, la confidencialidad de los datos vertidos en el perfil se diluye. Y, puesto que hemos firmado un contrato vinculante, estaremos atados de pies y manos si la compañía, atendiendo a su estrambótica concepción de responsabilidad, decide utilizar dicha información.

3.3.2 Garantías que da Facebook a los usuarios y exención de responsabilidad

> Aunque te permitimos definir opciones de privacidad
> que limiten el acceso a tu información,
> ten en cuenta que ninguna medida de seguridad
> es perfecta ni impenetrable.
> Política de privacidad de Facebook, 2009[569]

Tal y como se repite en cuantiosas ocasiones en sus términos de uso, la plataforma actúa como mero intermediario, lo que implica que no responde de las actuaciones de las terceras empresas que operan en ella. Dicho de otra manera, si no deseamos que nuestra información sea compartida con cientos de desarrolladores de aplicaciones, simplemente, no deberíamos usar Facebook. La exención de responsabilidad es meridiana en todos y cada unos de los supuestos: «cualquiera de tus datos personales puede hacerse público. No podemos garantizar que el contenido que cuelgas en el muro no será visto por personas no autorizadas» [570].

Por su parte, en lo que compete al otro actor, la propia plataforma le ha otorgado responsabilidad total sobre sus actos desde el mismo momento en que decide abrirse una cuenta:

> Intentamos mantener Facebook en funcionamiento, sin errores y seguro, pero lo utilizas bajo tu propia responsabilidad. Proporcionamos Facebook tal cual, sin garantía alguna expresa o implícita, incluidas, entre

---

[569] TOSBACK (2009): Política de privacidad de Facebook, 29 de octubre de 2009.
[570] *Política de privacidad de Facebook, actualización de 2014.*

> otras, las garantías de comerciabilidad, adecuación a un fin particular y no incumplimiento. No garantizamos que Facebook sea siempre seguro o esté libre de errores, ni que funcione siempre sin interrupciones, retrasos o imperfecciones. Facebook no se responsabiliza de las acciones, el contenido, la información o los datos de terceros y por la presente nos dispensas a nosotros, nuestros directivos, empleados y agentes de cualquier demanda o daños, conocidos o desconocidos, derivados de o de algún modo relacionados con cualquier demanda que tengas interpuesta contra tales terceros[571].

Sin embargo, dado que estas condiciones provocarían que muchas personas rehusasen registrarse o seguir usando el servicio, como medida de garantía la red social alude a su adscripción a los programas TRUSTe y el Acuerdo de Puerto Seguro *(Safe Harbor):*

> Facebook es titular de una licencia de certificación del programa de privacidad TRUSTe. Esto significa que nuestra política y nuestras prácticas han sido supervisadas por TRUSTe, una organización independiente dedicada a comprobar las políticas y prácticas de privacidad y seguridad para garantizar que cumplen los estrictos requisitos de su programa. El programa TRUSTe solo incluye la información recopilada a través de este sitio Web, y no comprende otros datos, como información que pudiera recopilarse a través de software descargado de Facebook. […] Como parte de nuestra participación en Safe Harbor, nos comprometemos a resolver todos los posibles conflictos que puedan surgir en relación con nuestras políticas y prácticas a través de TRUSTe[572].

TRUSTe es una empresa creada para garantizar a los clientes de comercio en Internet el anonimato en sus transacciones. Por su parte, Safe Harbor contempla una serie de acuerdos bilaterales firmados de una parte entre el Departamento de Comercio de Estados Unidos y la Unión Europea, y de otra entre Estados Unidos y Suiza. Mediante dicho convenio se comprometen a actuar en un marco común en lo relativo a la recopilación, uso y retención de datos de los ciudadanos pertenecientes a estos ámbitos geográficos. Su finalidad es que las informaciones de los ciudadanos europeos que se gestionen fuera de su territorio sean motivo de una protección más acorde con la que se da en la Comunidad Europea, puesto que en Estados Unidos, como ya adelantábamos en capítulos anteriores, la salvaguarda de estos contenidos atiende a consideraciones menos restrictivas.

---

[571] Ídem.
[572] Ídem.

Esta garantía es, cuanto menos, difusa[573]. Sí, Safe Harbour es un sistema de autocertificación mediante el cual las empresas firmantes se comprometen a cumplir con los acuerdos establecidos entre Estados Unidos y la Comisión Europea en lo que respecta al tratamiento de los datos personales de los ciudadanos europeos. Sin embargo, la adherencia al citado tratado es una formalidad sin carácter de obligatoriedad, ni poder impositivo. Es decir, se trata de una certificación que representa el compromiso de la empresa con lo manifestado en el acuerdo y que esta incluye en su página Web pero, dado que no exige su cumplimiento, ni obliga a la empresa a seguir unas determinadas directrices, habitualmente las buenas intenciones quedan en papel mojado. Es más contrariamente a lo que se cree, la obtención de este sello no implica que el sitio Web que lo luce haya sido aprobado por el Departamento de Comercio de Estados Unidos.

Además, tenemos la siguiente afirmación vacía de contenido la aplicación de lo estipulado en *Safe Harbour*:

> Facebook puede compartir información por vías internas en el seno de su grupo de empresas o con terceros con los fines que se describen en esta política. La información recopilada dentro del Espacio Económico Europeo («EEE») puede, por ejemplo, transferirse a países de fuera del EEE a los efectos descritos en esta política[574].

El caso de TRUSTe es diferente. Esta entidad fue creada para garantizar a los clientes de servicios comerciales en Internet la seguridad de los datos vertidos en sus transacciones económicas. No obstante, recuerda Andrés Durà, su complejo entramado accionarial no está exento de polémica, por lo que algunos de sus detractores denuncian la falta independencia ligada a su gestión. Creada en 1997 por Lori Fena de la Electronic Frontier Foundation y el empresario Charles Jennings, la llegada de posteriores responsables con intereses en el negocio de la Web relacional cambió la dinámica de la compañía. Como muestra de este viraje, un botón: en su accionariado se encuentran también accionistas de Facebook, por lo que su libertad de actuación queda, por lógica, en entredicho.

---

573 ANDRÉS DURÀ, R. (2010): *Op. cit.,*

574 *Política de privacidad de Facebook, 2014.*

3.3.3 ¿Qué sucede si el usuario se arrepiente?

Lo primero que deberían saber todas las personas que desean entrar a formar parte de la comunidad de habitantes de la red social es que, simplemente con abrirse una cuenta, ya han firmado un contrato vinculante que incluye la cesión de todos los contenidos que se viertan en la plataforma, sean del tipo que sean. Esto a su vez significa que ya no hay marcha atrás, puesto que ni siquiera cerrando la cuenta recuperarán el control absoluto sobre su información: incluso cuando el usuario decida darse de baja, los ordenadores de Facebook mantendrá una copia de seguridad de sus datos, así que la cancelación efectiva de la información es casi una utopía.

Desde 2010, Facebook ofrece dos opciones a todos aquellas personas que deseen abandonar la plataforma: bien desactivar sus cuentas, esto es, una especie de hibernación del perfil con carácter temporal; o bien eliminarlas permanentemente, opción que conlleva una mayor dificultad y trabajo por parte del usuario:

> Cuando desactivas una cuenta, ningún usuario podrá verla, pero no será eliminada. Guardamos la información de tu perfil (amigos, fotos, intereses, etc.) por si más tarde decides volver a activarla. Muchos usuarios desactivan sus cuentas por motivos temporales y al hacerlo, nos piden que mantengamos su información hasta que vuelvan a Facebook. Seguirás pudiendo reactivar la cuenta y restaurar tu perfil en su totalidad. Cuando eliminas una cuenta, se borra de forma permanente. Sólo deberías eliminar tu cuenta si estás seguro de que nunca querrás reactivarla[575].

En principio, cuando el usuario decide desactivar su cuenta los datos se pueden almacenar en copias de seguridad hasta un máximo de 90 días, aunque no estarán disponibles para los demás integrantes del sistema. El perfil no será invisible, pero la información enlazada a él se almacenará en los servidores de Facebook con la excusa de que si el sujeto cambia de opinión podrá reincorporarse en cualquier momento. Sólo deberá escribir su antiguo nombre de usuario y su contraseña, y su cuenta aparecerá como si nunca la hubiese cerrado. Sobra decir que el borrado total de los datos no está garantizado en ningún supuesto, ni siquiera cuando se elimina permanentemente la

---

[575] Ídem.

cuenta. De hecho, una vez superado el tiempo estipulado y aun cuando el individuo desea eliminar todo el contenido asociado a su perfil activamente, dicha información puede permanecer en los ordenadores de la compañía indefinidamente, tal y como se ha denunciado en cuantiosas ocasiones desde numerosos organismos y asociaciones (entre ellos, la Electronic Privacy Information Center (EPIC) y la Electronic Frontier Foundation (EFF) así como desde la Comisión Europea). Es constatable por lo tanto que los contenidos, aunque no sean públicos, se almacenan de forma perenne en las bases de datos de la red social, hecho que vulnera las leyes de protección de datos de diversos países, como sucede en el caso de los Estados Miembros de la Unión Europea.

Este proceder ha despertado la indignación no solo de las citadas instituciones, sino que ha suscitado arduas críticas en países como el Reino Unido, donde se acusó a la plataforma de violar el Acta de Protección de Datos[576]. La compañía, no obstante, se escuda en la necesidad de garantizar una cierta seguridad en torno a los datos personales del usuario para justificar este extremo: «podemos conservar cierta información para evitar el robo de identidades y otras conductas inadecuadas, incluso si se ha solicitado la eliminación»[577].

Por otra parte, del mismo modo que los contenidos nunca desaparecen de la memoria de Facebook, tampoco lo harán de la Web 2.0 si dicha información, aún introducida bajo otras condiciones, ha superado los confines de la red social. Esto sucede, por ejemplo, con aquellos datos de registro que la compañía obliga a hacer públicos por defecto, así como con todos aquellos que otros miembros del sistema han publicado sobre nosotros y optan por hacer accesible bajo la configuración «todo el mundo» o «público». En este sentido y dado que a través de Facebook se comparten datos más allá de las barreras de la plataforma, eliminar toda la información resulta una empresa quimérica. Más aun, si sumamos el hecho de que la estructura de la red, al igual que el tejido que la sustenta, la Web social, facilita la pérdida de control sobre los propios contenidos. Ante esto, la carencia de responsabilidad de la compañía es absoluta y no proporciona meca-

---

[576] KING, B. (2007): «Facebook Data Protection Row», en *Channel 4*, 17 de noviembre de 2007.

[577] *Política de privacidad de Facebook, actualización de 2014.*

nismos efectivos para hacer desaparecer los datos ni siquiera cuando el usuario ha decidido eliminar su cuenta permanentemente:

> Esta información puede asociarse contigo (es decir, tu nombre, fotos del perfil, fotos de portada, biografía, identificador de usuario, nombre de usuario, etc.) incluso fuera de Facebook; puede mostrarse cuando alguien hace una búsqueda en Facebook o en un motor de búsqueda público; estará accesible para los sitios Web, aplicaciones y juegos integrados en Facebook que utilizáis tú y tus amigos. […] Limitaciones sobre la eliminación: Incluso después de eliminar información de tu perfil o eliminar tu cuenta, pueden permanecer copias de dicha información visibles en otro lugar en la medida en que se haya compartido con otros, se haya distribuido de otro modo conforme a tu configuración de privacidad o haya sido copiada o almacenada por otros usuarios[578].

En este caso, la red social advierte de que son los propios individuos los que deben encargarse de borrar su rastro eliminando, uno a uno, el contenido introducido en la biografía, en las cuentas de otros amigos y en los grupos y páginas en los que se ha participado durante el uso de la red social. Y esto, a un usuario medio de Facebook, podría llevarle horas e, incluso, días.

Abandonar la plataforma es tan complicado que hasta es posible mantener la cuenta abierta aun cuando la persona ya no tenga presencia física en el mundo de los mortales. Recordemos que, por el volumen de negocio que representa, Facebook no puede permitirse perder usuarios: el precio de la compañía se mide a través del valor añadido que estos le otorgan. Por ello, la red social ha desarrollado tantas estrategias para mantener cuentas abiertas que algunas resultan, cuanto menos, sorprendentes e irrisorias. Tal es el caso de las cuentas *in memoriam*, perfiles para aquellos miembros que han fallecido y que, ni aún así, han conseguido eliminar su rastro digital:

> Si se nos notifica que un usuario ha fallecido, podemos convertir su cuenta en una cuenta *in memoriam*. En tales casos, restringimos el acceso al perfil a los amigos confirmados y permitimos a estos y a los familiares que escriban en el muro del usuario en recuerdo suyo[579].

---

[578] *Política de protección de datos de Facebook 2014*.

[579] Facebook. *Solicitud de cuenta conmemorativa*. Disponible en: https://es-es.facebook.com/help/ contact/651319028315841 [01/03/2013].

No obstante, en este caso concreto la compañía sí muestra cierta condescendencia: «Podemos cerrar una cuenta si recibimos una solicitud formal de un pariente del usuario u otra solicitud legal pertinente para hacerlo»[580]. Pero si por el contrario decidimos mantener la cuenta póstuma, compete a Facebook determinar el tiempo que ese perfil funcionara: «estará activa bajo un estado memorial especial por un período determinado por nosotros para permitir a otros usuarios publicar y ver comentarios»[581]. Eso sí, cuando se elimine «permanentemente», sus datos alcanzarán la eternidad en los ordenadores de Facebook.

Si bien, es cierto que no todo el mundo desea ceder a Facebook el derecho de conservar sus datos indefinidamente. Incluso hay multitud de personas que desean no entrar en el universo de las redes sociales. Lo que estos interactores no sospechan es que la red puede obtener la dirección de correo de cualquier persona a pesar de que estas renuncien a participar en el juego de las comunidades virtuales. Y esto es posible por el siguiente motivo: prácticamente, nos recuerda Andrés Durá, la generalidad de los sujetos poseen contactos en el correo electrónico que usan la plataforma, por lo que es probable que les llegue una invitación para que se abran una cuenta[582]. Entonces, Facebook almacenará su dirección para enviar la invitación y dos recordatorios, así que su correo electrónico entrará a formar parte de la base de datos de la compañía. Si el usuario desea que no se almacene esta información de carácter personal, debe ocuparse él mismo de eliminarla poniéndose en contacto con la plataforma. Y, aún así, Facebook ha de guardar una copia de seguridad del correo para asegurarse de que no reenviará más notificaciones, punto que nos remite a la falacia anterior y nos recuerda quién posee el control dentro de este *panopticon* virtual que es Facebook:

> Información de contacto de no usuarios. Si un usuario nos facilita tu dirección de correo electrónico, pero no eres usuario de Facebook y quieres que la eliminemos, puedes hacerlo en esta página de ayuda. Sin embargo, esa solicitud solo se aplicará a las direcciones que tengamos en el momento de la solicitud y no a ninguna dirección que los usuarios nos faciliten posteriormente[583].

---

[580] Ídem.
[581] Ídem.
[582] Andrés Dura, R. (2010): *Op. cit.*
[583] *Política de privacidad de Facebook, actualización de 2014.*

Aunque no se de este supuesto, eludir los tentáculos de la red social resulta una tarea ardua en tanto que numerosas aplicaciones de Internet interactúan a través de servicios de Facebook, produciendo una retroalimentación que, casi siempre, finaliza con los datos del interactor en los servidores de la compañía. Así, servicios como Spotify para escuchar música en *streaming* solicitan una cuenta de Facebook para poder darse de alta y si por ejemplo el individuo ya estaba dado de alta en Whatsapp, aplicación de mensajería instantánea de pago para teléfonos inteligentes, ahora la plataforma también tiene sus datos:

> Podemos compartir la información que recibimos con aquellos negocios que legalmente formen parte del mismo grupo de empresas que Facebook o que vayan a unirse a este grupo (dichas empresas suelen denominarse afiliadas). Del mismo modo, nuestros afiliados también comparten información con nosotros. Esta práctica se lleva a cabo de acuerdo con todas las leyes aplicables, incluso cuando las leyes aplicables hacen necesaria la obtención de consentimiento. Podemos, junto con nuestros afiliados, utilizar la información compartida para proporcionar, reconocer y mejorar tanto nuestros servicios como los suyos.

3.3.4 **La responsabilidad en el caso de los menores**

Aunque en principio los menores no pueden registrarse en la red social, muchos de ellos abren cuentas en Facebook simplemente indicando un año de nacimiento distinto al suyo. Para colaborar con la protección de este segmento de la población la plataforma ha incorporado el denominado «botón de pánico»: una aplicación para que los niños y adolescentes tengan un acceso rápido a una herramienta que les permita ponerse en contacto con las autoridades en caso de detectar un indicio de abuso en línea. Por el momento, la aplicación solo estará disponible en Reino Unido, gracias a que el Centro de Protección Online de Menores Británico (The Child Exploitation and Online Protection Centre, CEOP)[584] negoció durante meses la incorporación de este sistema de prevención, tras haber llegado ya a acuerdos con otros servicios similares como MySpace y BEBO[585].

---

[584] Centro de Protección Online de Menores Británico: http://ceop.police.uk/

[585] BEBO, del acrónimo de «Blog early, blog often», es una red social fundada en enero de 2005.

En otros países como España, esta es la escueta garantía que ofrece Facebook:

> Para proteger a los menores podríamos aplicar una serie de medidas de protección especiales (como limitar la capacidad de los adultos para contactar y compartir contenido con ellos) a sabiendas de que esto puede suponer una experiencia más limitada en Facebook para los menores[586].

3.3.5 ¿Qué medidas pueden tomar los usuarios si ven su vida privada dañada en Facebook?

Teniendo en cuenta que las cláusulas de la compañía eluden toda responsabilidad en prácticamente la generalidad de los ámbitos referidos a la protección de datos de los miembros del sistema, estos tienen un margen de actuación casi inexistente. En principio, cualquier persona que haya visto su intimidad y vida privada dañada tras usar la plataforma, o incluso, sin usarla, puede acudir a la propia compañía[587]. Si bien, lo cierto es que, a buen seguro, recibirán poco asesoramiento, dado que resulta verdaderamente complicado resolver cuestiones que no aparecerán explicitadas en los apartados de preguntas frecuentes *(FAQs)* y requieran la ayuda de un administrador. Igualmente, los servicios de ayuda automática que se usan mediante la cumplimentación de un formulario redirigen a los usuarios a las mismas páginas de ayuda que, además, suelen estar desactualizadas o son inexistentes[588].

Si los usuarios optan por obtener información dentro de la propia plataforma usando la función de búsqueda, se encontrarán con la sorpresa de que no siempre podrán acceder a estos contenidos. Así sucede, por ejemplo, cuando requieren consejos para proteger sus publicaciones. Como botón de muestra, solo hay que citar lo acontecido con el grupo de Facebook MoveOn.org's: Conocido por

---

[586] Política de uso de datos. Los menores y la seguridad. Facebook. (2014). Disponible en: https://es-es.facebook.com / about/ privacy/minors [12/05/2014].

[587] Servicio de atención al usuario de Facebook: https://www.facebook.com/help/? page=746 [08/02/2014].

[588] ARRINGTON, M. (2007): «Is Facebook Really Censoring Search When It Suits Them?», en *TechCrunch*, 22 de noviembre de 2007.

denunciar muchas de las prácticas abusivas de la compañía en esta materia, fue censurado y dejó de aparecer en los resultados de búsqueda. Incluso la propia palabra *privacy* desapareció durante un periodo de los resultados arrojados debido, según la compañía, a un fallo de seguridad[589].

Si finalmente tras esta travesía el individuo consigue contactar con la plataforma y no se soluciona la situación, lo más recomendable será acudir a las autoridades nacionales de protección de datos (en el caso de España, la AEPD) y, posteriormente, emprender acciones judiciales. No obstante, debemos tener en cuenta que podemos toparnos con una serie de restricciones derivadas de las asimetrías normativas entre los países en los que se accede al servicio y el marco legislativo donde tiene su sede la empresa. Problemas que, en el marco de Europa, han producido muchos enfrentamientos entre la red social y la Comisión Europea, al igual que sucede con Google, la otra gran amenaza para la integridad privada de los interactores.

4. REFLEXIONES SOBRE EL CAPÍTULO

En el capítulo que ya toca a su fin nos hemos servido de los principios que sustentan la filosofía de la plataforma Facebook, a saber: «transparencia, control y responsabilidad» para vertebrar un primer acercamiento al estudio de la red social. De este modo, hemos constatado como el esquema inicial que parecía subyacer a las palabras de Richard Allan, esto es: transparencia en el servicio, responsabilidad ante cualquier acto que ponga en entredicho la esfera reservada del individuo y control para el usuario, toma un cariz bien distinto en la práctica.

El discurso de la transparencia va encaminado a intentar legitimar prácticas de la compañía y fomentar la creencia de que es el individuo el que posee en todo momento el dominio sobre sus datos. Pero dado que dicha transparencia viene mediada, solo dejará ver aquello que se quiere mostrar. Asimismo, la estrategia de la visibilidad extrema es usada como lema para ocultar cómo accede Facebook a los datos de sus miembros, oscureciendo el trasvase de contenidos y flujos de in-

---

[589] Ídem.

formación que tienen lugar en la plataforma y que el individuo no conoce. Una coyuntura que la empresa aprovecha para aumentar su valor, mediante la acumulación de datos que conforman la identidad digital de los participantes del sistema, y que promueve la creación de un completo dossier virtual que cataloga a cada uno de ellos y los vuelve altamente accesibles.

Por el contrario, la información disponible para los miembros de la plataforma como, por ejemplo, la vertida en las políticas de privacidad, no genera el conocimiento necesario para que los miembros de la comunidad sean capaces de proteger su vida privada en la red, mediante acciones previamente meditadas. En este sentido, el control lo ejerce siempre la compañía, toda vez que traspasa la responsabilidad de sus actos al usuario. En este escaparate, la persona que se esconde tras cada miembro de la red social se convierte en el punto al que se dirigen todas las miradas, mientras que Facebook decide el marco visible y dónde ha de ponerse el foco. ¿No son estos los pilares de esa cárcel ideal creada por Bentham?

Esta revisión del *panopticon* merece un estudio más pormenorizado. En primer lugar, porque resumir la maquinaria de la plataforma a las interacciones y situaciones hasta ahora observadas pecaría, cuanto menos, de simpleza. Y, en segundo lugar, si seguimos con la tónica del control y la transparencia, debemos advertir que en este capítulo hemos analizado solo lo que la compañía «declara» en las políticas de privacidad, pero un estudio detallado como el presente nos azuza a escarbar por debajo de la superficie «visible» del fenómeno en cuestión. Con este objetivo en mente, en el próximo capítulo analizaremos las prácticas que la compañía no declara o no especifica claramente en los contratos de usuario; observando, a través del dicho análisis, cómo quedan configuradas finalmente las tres constantes a las que tan decisivamente nos hemos remitido en este capítulo.

CAPÍTULO VII. FACEBOOK, EL GRAN BANCO DE DATOS PERSONALES Y LA CREACIÓN DEL SER VISIBLE

SÍNTESIS

La imperceptibilidad de los flujos de información e intercambio de datos inherentes a la arquitectura de la Web 2.0 y a sus herramientas arquetípicas propician la pérdida de control sobre los propios contenidos sin que los usuarios apenas sean conscientes. Empero, es en la estructura de Facebook donde esta dinámica adquiere un matiz protagonista, por cuanto promueve una adquisición masiva de informaciones y de patrones de comportamiento superior, incluso, a la de muchos de los sistemas de vigilancia diseñados por los servicios de inteligencia. Es por ello que, el sinfín de injerencias en la intimidad y vida privada que aparecen ligadas al uso de la red social por antonomasia, unidas a la multitud de voces que piden la regulación de las prácticas abusivas de la compañía, nos invitan a ahondar en la naturaleza del trasvase de contenidos que se oculta bajo la superficie de esta poderosa plataforma. Nos compele, por ello, a descubrir en qué consisten esos usos exhaustivos de recolección de información que marcan la diferencia entre el estatus de supremacía del libro de caras y otras redes sociales, asunto que se torna primordial, más aún teniendo en cuenta el provecho que saca de ellas.

1. INTRODUCCIÓN: FACEBOOK, EL GRAN BANCO DE DATOS PERSONALES

Habitualmente, desde los grandes emporios de Internet se alimenta la creencia de que las herramientas digitales son moralmente neutras, una afirmación que los usuarios asumimos como si de un dogma de fe se tratase y que lleva implícita una lectura subyacente: en la interacción con las TIC los individuos son los únicos responsables de sus actos. No obstante, si bien la tecnología en sí misma no puede ser calificada como beneficiosa o perjudicial, la manera en la que esta aparece configurada puede responder a la consecución de una serie de objetivos que esconden una intencionalidad premeditada. Y a este

respecto, al examinar el papel que juegan ciertas aplicaciones de la Web 2.0 encontramos que su diseño y las estructuras constitutivas que sustentan dichas plataformas son todo, salvo neutras. El simple hecho de que se trate de espacios mediados, atribución por definición del entorno digital, ya presenta un terreno propicio para la emergencia de conflictos entre derechos, toda vez que señala esa cierta intencionalidad que necesariamente antecede a la mediación.

> En el mundo físico, los usuarios pueden hacer efectivas sus preferencias de visibilidad, por ejemplo, teniendo una conversación a puerta cerrada. La arquitectura de los espacios físicos impone limitaciones considerables en el proceso. Pero dado que la arquitectura de un espacio virtual es una función del código que lo crea y que este puede ser cambiado, tanto la codificación, como el interfaz pueden marcar una enorme diferencia en lo que respecta a la vida privada de la que podrán disfrutar los individuos y en cómo la experimentan[590].

En algunos casos como en las redes sociales esta intencionalidad es consecuencia directa de su arquitectura, destinada no solo a la recogida de datos, sino a facilitar cierta clase de interacciones sociales frente a otras. Y esta particularidad, que puede ser intuida por el sujeto aún cuando nunca es perceptible, adquiere un nivel superior en la comunidad Facebook. De hecho, son numerosas las investigaciones que comparan la arquitectura de la red social *par excellance* con otras plataformas parejas, concluyendo que el entramado que sustenta a esta facilita y promueve un tipo concreto de interacciones encaminadas, de una parte, a extraer el máximo de información de los participantes y, de otra, a exponer sus contenidos a la luz pública, volviéndolos más accesibles y vulnerables. Tanto es así, que se ha señalado tajantemente la intencionalidad oculta bajo el diseño de la plataforma como la práctica desleal y abusiva que mejor refleja la filosofía de la compañía:

> El diseño del interfaz de Facebook, que tiende a ocultar el flujo de información de un contexto a otro, emerge como contribución fundamental a los problemas de para proteger la vida privada […] Las implicaciones son el resultado de decisiones ligadas al diseño [de Facebook], incluso cuando esas decisiones nos tienen que ver en sí mismas, ni de manera obvia con la protección de la vida privada[591].

---

[590] HULL, G., LIPFORD, H. y LATULIPE, C. (2010): *Op. cit.,* p. 296.
[591] *Ibídem,* p. 288.

Adalid pues de las prácticas más dañinas para la intimidad y vida privada, la estructura de la plataforma favorece la pérdida de dominio sobre los propios contenidos personales, toda vez que la firma del contrato de cesión de derechos que cada sujeto acepta al entrar a formar parte de la comunidad elimina la potestad de control sobre dichas informaciones. Esta violación del ámbito íntimo actúa en dos direcciones: en primer lugar, revela datos que los usuarios creen restringidos hasta crear un peligroso escenario en el que pueden ser fácilmente identificables. La caracterización resulta del todo factible dado que no solo se recolectan informaciones privadas, sino otro tipo de gustos personales que delinean la semblanza del individuo que se encuentra tras la pantalla, aún cuando, en principio, este sea tan solo un identificador numérico. Por ende, la exhibición pública de estos contenidos sustraídos sin consentimiento fomenta la vigilancia y seguimiento de cada participante sin que apenas se percate:

> Los datos personales son generosamente proporcionados y las preferencias de privacidad raramente usadas. Debido a la variedad y riqueza de la información personal desplegada en los perfiles de Facebook, su visibilidad, su publicidad y su enlace público con la identidad real de los miembros, así como el alcance de la red, los usuarios podrían estar poniéndose a sí mismos en riesgo, por una variedad de ataques a su persona física y virtual[592].

Conjuntamente, la plataforma saca provecho de los datos derivados de los perfiles captando pautas de comportamiento gracias a la acumulación de gustos e intereses que estos aportan, informaciones que constituyen, a la postre, un poderoso activo para la empresa. De hecho, son este tipo de materiales los que cimentan el gran negocio de la compañía, que se comporta como una gigantesca base de datos al catalogar a sus miembros como público objetivo mediante el cual consigue atraer a los más variados anunciantes. Así, en la actualidad hay más de cincuenta y siete patrones de datos personales susceptibles de ser recopilados[593], entre ellos: nuestras preferencias, intereses por anuncios, rasgos de personalidad… Informaciones que constitu-

---

[592] GROSS, R. y ACQUISITI, A. (2005): *Op. cit.,* p. 79.

[593] Europe *vs*. Facebook (2012): «Facebooks Data Pool», en *Europe vs Facebook Web page*. Disponible en: http//europe-v-facebook.org/ EN/Data_ Pool/-data pool.html [10/11/2012].

yen una fuente inagotable de datos que la red recopila y agrega a un determinado perfil. Esta es, sin lugar a dudas, la gran ventaja competitiva de Facebook: la capacidad de conocer al posible consumidor hasta límites insospechados para poderle ofrecerle una publicidad completamente personalizada y claramente orientada. Dicha recogida de datos no se produce al azar, sino que se perpetra con una intencionalidad concreta: los contenidos que se recolectan provocan que el usuario se convierta automáticamente en un posible cliente; de ahí, el perfilado de sus gustos y preferencias.

La duda que indiscutiblemente nos invade ahora es si esta práctica es legal, si aparece correctamente reflejada en las políticas de privacidad y condiciones del servicio de la compañía y, de ser así, si el individuo es plenamente consciente de este proceso. Para intentar desentrañar estas tres incógnitas, en el presente capítulo repasaremos cómo desde 2005 la empresa ha desarrollado maniobras de recolección y explotación de datos mucho más agresivas de las que, a simple vista, es posible sospechar. Sin embargo, antes de adentrarnos en estas prácticas más complejas, reseñaremos brevemente cuáles son aquellas informaciones que la red social «declara» recolectar en sus pliegos de condiciones.

2. RECOPILACIÓN DE INFORMACIÓN DE LOS PERFILES DE LOS USUARIOS EXPRESAMENTE DECLARADA POR LA COMPAÑÍA

A priori, toda la información que la plataforma asegura almacenar aparece mencionada en sus múltiples versiones de «políticas de privacidad», «condiciones del servicio» o «políticas de protección de datos» (expresión con que se las denomina actualmente). Dichas cláusulas se han ido completando en la misma medida que la plataforma incorporaba un mayor número de miembros registrados e integraba mayores potencialidades, intentando a su vez esquivar las posibles quejas de los usuarios y/o evitar verse involucrada en conflictos legales. En este sentido, el argumento que se esgrime desde la red social para justificar el por qué de esa recopilación masiva de datos obedece a la necesidad de «ofrecer una experiencia segura, eficaz y personalizada […] Gestionar el servicio, ponernos en contacto contigo, ofrecer anuncios personalizados, ofrecer anuncios sociales, com-

plementar tu perfil y hacer sugerencias»[594]. Es decir, en principio, los datos que recopila Facebook se ciñen, exclusivamente, a aquellos requeridos para que el sujeto se registre, pueda hacer funcionar la red social y ofrecerle su amplia gama de servicios y funciones. El resto constituyen toda esa amalgama de contenidos que el propio individuo «decide» compartir por su cuenta y riesgo.

Resumiendo el abanico de datos que desde la red social se estiman necesarios para poder ofrecer el servicio, encontramos que los repositorios de Facebook pueden beber de las siguientes fuentes:

2.1 DATOS DE REGISTRO REQUERIDOS Y OTROS CONTENIDOS PROPORCIONADOS POR LOS USUARIOS

Para hacer funcionar cualquier red social es necesario cumplimentar de una serie de campos, similares a las entradas de una base de datos, que permiten identificar[595], diferenciar y verificar a un interactor concreto del sistema, delimitándole del resto de participantes de la comunidad. En consecuencia, el registro supone un momento clave, pues el sujeto introduce datos claramente indicativos de su identidad. Entre estas informaciones requeridas, Facebook, al igual que sucede con el resto de sitios de redes sociales, solicita los datos de contacto para enlazar la cuenta a un correo electrónico, así como la fecha de nacimiento, el sexo y, por descontado, el nombre y apellidos del individuo; estos últimos bajo la obligación de introducir la identidad real. Sortear este paso con un nombre falso es del todo factible. No obstante, debemos tener en cuenta que la plataforma utiliza cada vez más mecanismos para detectar las cuentas falsas o que no se corresponden con una identidad real.

Por otra parte, la cuestión de que un servicio de comunicación a través de Internet necesite para funcionar nuestra verdadera identidad es algo más que discutible. Si bien este requerimiento podría responder a un comportamiento lógico e incluso deseable, como es el hecho de denunciar posibles casos de fraude o suplantación de identi-

---

[594] *Política de privacidad de Facebook, actualización de 2014.*

[595] Cuando mencionamos la voz «identificar» nos referimos aquí a un identificador numérico, es decir, no a un nombre y apellido, sino a la clave que diferencia a un interactor de otros; por lo que el usuario, si no se realiza un cruce de datos, seguiría siendo anónimo.

dad, también revela una obviedad: un perfil falso no es rentable en tanto que jamás se podrá perfilar fiablemente y no será, por tanto, susceptible de convertirse en un potencial cliente. La duda sobre en qué extremo nos movemos se aclara desde el mismo momento en que efectuamos el registro gracias a otro hecho: al darse de alta, el individuo suscribe la adhesión a la Specially Designated Nationals List (SDN) perteneciente al Departamento del Tesoro de Estados Unidos, listado en el que aparecen recopilados los nombres de las personas u organizaciones con las que los ciudadanos estadounidenses no pueden realizar transacciones económicas[596].

Dejando a un lado la discutible política de nombre reales que ya ha sido implantada por otros gigantes de Internet como Google, la red social almacena además otra información de contacto: la que el usuario «comparte» al comunicarse con la plataforma, aún cuando se ponga en contacto con ellos a través de una dirección de correo electrónico distinta a la indicada en la cuenta[597]. De la misma manera, el teléfono móvil también puede ser recogido, bien como prueba de verificación de la identidad[598] o para sortear la aparición de un código *captcha*[599], un paso engorroso que, cada cierto tiempo, se activa en nuestras pantallas cuando deseamos entrar en nuestra cuenta y que se puede eludir fácilmente verificando la identidad a través de un código enviado al teléfono.

El resto de datos, es decir aquellos que el sujeto «decide compartir», incluyen todo lo que vuelca en Facebook, como los comentarios escritos en la propia biografía o en la de otros contactos, fotos, vídeos, enlaces… y un sin fin de contenidos que decoran los muros de cada una de las habitaciones de nuestra casa virtual. Y en este cajón de sastre también figura toda la información que genera cada miembro cuando ejecuta acciones como: «añadir a un amigo, indicar que le

---

596 Specially Designated Nationals List (SDN) del Departamento del Tesoro de Estados Unidos: http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

597 *Política de privacidad de Facebook, 2014.*

598 Ídem.

599 De este modo y para poder verificar que el usuario es humano, este debe rescribir un código compuesto por unas letras y números distorsionados. Así se evita que los denominados *bots* o robots que hacen acciones automatizadas accedan a las cuentas ajenas.

gusta una página o sitio Web, añadir un lugar a su historia, usar la herramienta de importación de contactos o bien registrar [que tiene] una relación con alguien»[600].

La información de registro como nombre, fotos del perfil, fotos de portada, sexo, redes[601] e identificador de usuario es pública por defecto. Sin embargo, dado que la visibilidad de los datos incluidos en los perfiles de Facebook pueden cambiar en cualquier momento, la compañía puede dejar al descubierto otros contenidos no incluidos en estos apartados sin mediar aviso previo. Lo veremos más adelante.

2.2 INFORMACIÓN PROCEDENTE DE OTROS USUARIOS: EL ETIQUETADO

Facebook puede recopilar información de cada miembro a través de sus contactos cuando, por ejemplo, se le etiqueta en una foto o vídeo o se proporciona detalles de su relación con dicho usuario. En los primeros años de adopción de la red social, este hecho provocó que muchos de los contenidos que los individuos no deseaban hacer públicos saliesen a la luz bajo su total desconocimiento.

Por otra parte, el dominio efectivo de estas informaciones es muy complicado. En principio, cada miembro puede controlar quién verá las publicaciones en las que está etiquetado a través del configurado de las opciones de privacidad y verificarlo mediante la opción «ver cómo». El problema surge porque no siempre es posible acceder a dicha publicación si el contacto que nos etiquetó decide cambiar su visibilidad:

> Si en un área privada (como un mensaje o un grupo) se vincula tu nombre, solo aquellas personas que puedan acceder a ese espacio podrán ver el enlace. Asimismo, si se te relaciona con un comentario, solo las personas que puedan ver el comentario podrán ver el enlace[602].

Si bien es cierto que en la actualidad existe la posibilidad de aprobar y/o denegar dicha etiqueta, revisar una a una las acciones anteriores a este cambio podría llevarnos casi una eternidad. Ante estos casos, la solución que se le ofrece al afectado es algo más rudimentaria: «Si no quie-

---

600 *Política de privacidad de Facebook, 2014.*

601 Durante el desarrollo de esta tesis las redes dejaron de estar activas.

602 *Política de privacidad de Facebook, 2014.*

res que alguien te etiquete, te recomendamos que te pongas en contacto con dicha persona y se lo digas. Si eso no funciona, puedes bloquearla. No podrá volver a etiquetarte»[603]. Por otra parte, no todos los individuos activan dicha función; bien porque no la conocen o porque no sospechan que dicha etiqueta pueda figurar en un contenido visible. Además, esta información no siempre se muestra en la susodicha pestaña «ver cómo».

Igualmente, se advierte que tanto «amigos», como no contactos pueden introducir información sobre cualquier miembro del sistema y que dichos contenidos no solo serán recolectados por la plataforma, sino que podrán hacerse visibles a terceros en cualquier momento:

> Si [otras personas] deciden publicar tu información de contacto o fotos tuyas; te etiquetan en una foto, en una actualización de estado o en un lugar; o bien te añaden a un grupo, esta información puede volverse visible a toda la audiencia. […] Cuando la gente usa Facebook, puede almacenar y compartir información sobre ti y otras personas que tienen como amigos, como cuando suben y gestionan sus invitaciones y contactos. Cuando otras personas comparten información sobre ti, pueden optar a hacerla pública[604].

2.3 DATOS TÉCNICOS PARA HACER FUNCIONAR EL SERVICIO

Como todos los servicios que navegan en la Web, la red social necesita conocer una serie de parámetros de carácter técnico para hacer funcionar su sistema; por ejemplo, aquellos referentes al dispositivo de conexión a Internet. Este hecho, admite la abogada Paloma Llaneza[605], no está reñido por definición con la protección de la intimidad y vida privada siempre y cuando su utilización se ciña, claro está, a la prestación del servicio que motivó la recolección de dichos datos, así como a su período de vigencia. A este respecto, Facebook declara de manera expresa identificar los dispositivos de acceso, recopilar datos destinados a geoposicionar y otros obtenidos que rastrea mediante *cookies* propias de la compañía:

> [Facebook puede obtener] información sobre la comunicación y la red, como la dirección IP o número de teléfono móvil, y otra informa-

---

603 Ídem.

604 Ídem.

605 Paloma Llaneza entrevistada por Vicente Vallés, *24 horas*, TVE, 19 de junio de 2012.

> ción, como tu servicio de Internet, sistema operativo, ubicación, tipo de dispositivo o de navegador (incluido en identificador) que utiliza o las páginas que visitas[606].

Dicha información sobre la recolección de estos datos no siempre ha aparecido reseñada en las políticas de privacidad, sino que comenzó a incluirse tras quejas de diversos organismos en defensa de los derechos de los consumidores.

2.3.1 **Datos sobre la ubicación del usuario**

Dentro de una red social, los servicios de localización permiten ofrecer, con cierto detalle, la localización geográfica de cada miembro: «podemos obtener información de tu GPS u otro tipo de información de ubicación que nos permita comunicarte si alguno de tus amigos está cerca de ti»[607]. Así, cada vez que un sujeto inicia sesión en Facebook la compañía recibe registros técnicos y de localización tales como la información del ordenador, teléfono móvil u otros dispositivos de acceso o desde donde se instalan las aplicaciones. Sabe, incluso, si varias personas inician sesión desde el mismo ordenador. Dada la naturaleza de este servicio, aparece estrechamente ligado al uso de teléfonos móviles y otros terminales de última generación, no obstante, no es algo exclusivo de estos.

Del mismo modo, cuando el usuario publica fotos o vídeos, el libro de caras recibe información adicional, denominada «metadatos», que incluye la hora, la fecha y el lugar en el que se realizaron estos contenidos. De nuevo, cabe mencionar que la utilización de estos datos estaría justificada solo durante el momento de ofrecer el servicio, pero lo cierto es que no existe constancia efectiva del momento en que la compañía decide eliminar sus registros:

> Cuando obtenemos tus coordenadas de GPS, las combinamos con otra información de ubicación (como tu ciudad actual) que tenemos sobre ti, pero solo las conservamos durante el tiempo necesario para ofrecerte nuestros servicios, por ejemplo, los casos en los que conservamos tus últimas coordenadas de GPS para enviarte notificaciones relevantes[608].

---

606 *Política de privacidad de Facebook, 2014.*
607 Ídem.
608 Ídem.

2.3.2 Las *cookies* y el rastreo

Las *cookies,* ya sean de navegador o de seguimiento, son fragmentos de programa necesarios para desarrollar muchas de las acciones que ejecutamos en Internet. Estos pequeños archivos de texto, a menudo encriptados, se ubican en el navegador del usuario, de manera que el sitio Web puede consultar la actividad previa del interactor, así como sus preferencias. Su pertinencia dependerá de que su uso esté justificado o no por la prestación del servicio.

Gran parte de las acciones anteriormente descritas funcionan gracias a las *cookies* propias de la plataforma Facebook que permiten rastrear si cada miembro ha consultado la biografía de otra persona, ha enviado o recibido un mensaje, está buscando un amigo o una página, hace «clic» en un determinado anuncio o interactúa de cualquier otro modo. Arrojan, asimismo, información sobre si se utiliza una aplicación para móviles de Facebook o se realiza una compra a través de la plataforma.

2.4 DATOS SOBRE PREFERENCIAS DEL USUARIO

2.4.1 Datos que recibe de terceros para ofrecer publicidad «del agrado del usuario»

Otra de las vías a través de las cuales Facebook obtiene su materia prima proviene de la recopilación de datos de sus empresas afiliadas, es decir, socios publicitarios, clientes u otras terceras partes. Según la compañía, dicho intercambio nace con el fin de asesorarse mutuamente sobre qué anuncios han sido, o son susceptibles, de atraer el interés del individuo. De este modo, la plataforma mide la eficacia de su publicidad personalizada, intentando interpretar la actividad que se desarrolla en línea y afilando al máximo el perfilado de cada miembro transformándolo en cliente potencial. Esto implica que un anunciante externo a la red social puede facilitarle a la compañía información sobre qué usuarios se interesan por un determinado anuncio, ya esté publicado en Facebook o contenga un enlace que le remita fuera del sitio:

> Podemos solicitar a los anunciantes que nos indiquen cómo nuestros usuarios han respondido a los anuncios que les mostramos. Este intercambio de datos, denominado comúnmente «seguimiento de con-

> versión» nos ayuda a medir la efectividad de nuestra publicidad y a mejorar la calidad de los anuncios que ves. […] Podemos recibir información sobre si has visto o no, o si has interactuado con determinados anuncios de otros sitios, para medir la efectividad de dichos anuncios[609].

En principio, si la compañía no poseía dichas informaciones antes de que los obtuviera de sus anunciantes, les otorgará el carácter de «anónimos» en un plazo de 180 días, lo cual significa que no podrá asociarse a ningún individuo en particular. Por supuesto, estamos ante otra afirmación cuya verificación efectiva resulta imposible para el común de los mortales.

2.4.2 **Los «me gusta»**

Las técnicas de exploración de usuarios que utiliza Facebook, encaminadas a recolectar sus informaciones personales y predecir, de manera automática, sus actitudes como posibles compradores, constituyen el punto fuerte de la plataforma. A través de su popular opción «me gusta», significada en el icono de una mano con el pulgar levantado, los integrantes de la comunidad dan todo tipo de detalles acerca de sus inclinaciones personales, así como sus hábitos de consumo. Esto permite inferir, de manera automática y con bastante precisión, un abanico de características propias, altamente sensibles, como son: «la orientación sexual, la etnicidad, las perspectivas políticas y religiosas, rasgos de la personalidad, inteligencia, felicidad, el uso de sustancias adictivas, la separación de los padres, edad y género»[610], entre otras muchas.

El poder predictivo de los «me gusta» es tal, que se ha llegado a afirmar que el comportamiento en Facebook permite a un ordenador hacer un perfil psicológico de los sujetos más acertado que el que dibujarían sus amigos o familiares. Al menos, esta es la conclusión principal de un estudio de la Academia Nacional de Ciencias Estadounidense[611],

---

609 Ídem.

610 KOSINSKIA, M., STILLWELLA, D. y GRAEPELB, T. (2013): «Private Traits and Attributes are Predictable from Digital Records of Human Behaviour», en *PNAS,* University of California, Berkeley.

611 YOUYOU, W., KOSINSKI, M. y STILLWELL, D. (2015): «Computer-based personality judgments are more accurate than those made by humans», en *PNAS,* University of California, Berkeley, 12 de enero de 2015.

realizado con miles de participantes de la red social. Y lo cierto es que, aunque el hecho de que una máquina sea capaz de conocernos mejor que nuestros allegados resulta, cuanto menos, inquietante, estos hallazgos no son aislados. Son varios los ensayos que han prosperado a este respecto, concluyendo en premisas similares. En concreto, destaca el desarrollado por el Centro Psicométrico de la Universidad de Cambridge, en Reino Unido y el Departamento de Ciencias de la Computación de la Universidad de Stanford, en Estados Unidos. Ambos han obtenido derivas parejas. Partiendo de la idea de que la conducta desarrollada en las redes da pistas fiables sobre cómo se comporta esa persona, los autores del experimento consiguieron que casi 90.000 usuarios, un número nada desdeñable, realizaran un *test* de personalidad de cien preguntas. A su vez, los investigadores tuvieron acceso a sus «me gusta» en la red social. En una segunda etapa del estudio, crearon un programa informático que, como si de un psicólogo digital se tratase, debía desentrañar los principales rasgos de los participantes, partiendo del mínimo número de «me gusta» analizados. Los resultados arrojaron conclusiones sorprendentes: Con solo diez «me gusta» el programa fue capaz de determinar la forma de ser del sujeto con mayor certeza que cualquiera de los juicios emitidos por un colega del trabajo. Este dato tal vez no resulta asombroso. Sin embargo, a medida que la máquina analizaba más información sobre las acciones que los individuos efectuaban en Facebook, más se afinaba su valoración. Así, con solo setenta «me gusta», fue capaz de averiguar más de cada participante que su compañero de piso y, con la cifra de 150, más que su propia madre. Sólo la pareja sentimental de cada sujeto consiguió rivalizar con la máquina… y no en todas las ocasiones: si el programa disponía de 300 «me gusta» o más no existía contendiente posible. Y, teniendo en cuenta que el porcentaje medio de «me gusta» que activa cada usuario es de 227, el dictamen es meridiano: en la mayoría de los casos, el mago Facebook es capaz de conocernos mejor que los propios seres humanos que nos rodean.

Para validar estos resultados, los investigadores recabaron una submuestra de más de 14.000 miembros de la plataforma que habían sido valorados no ya por un allegado si no, al menos, por dos. La sorpresa fue mayúscula: incluso acudiendo al uso del perfil psicológico doble, la máquina volvió a superar a los humanos.

Su trabajo, no obstante, no finalizó aquí. En una tercera medición, se intentó averiguar si el ordenador era capaz de predecir determina-

das conductas propias, como el consumo de drogas, la tendencia a la depresión o la orientación política. Y una vez más, en doce de las trece conductas estudiadas, la máquina afiló el perfilado más que cualquiera de los integrantes del entorno doméstico del sujeto. Los resultados confirman, igualmente, los ya obtenidos en un trabajo anterior de Michal Kosinski y Wu Youyou, según el cual cien «me gusta» de Facebook bastan para saber el sexo, raza o ideología de cada usuario[612].

Este hecho que, a todas luces, constituye una amenaza para lo más íntimo del ser humano, es decir, su forma de ser, proceder o sentir, nos da qué pensar acerca del poder que le otorgamos a la red social cada vez que usamos cualquiera de sus aplicaciones. Sin temor a equivocarnos, podemos afirmar que somos lo que «nos gusta» y, para perjuicio de nuestra integridad personal, Facebook lo sabe.

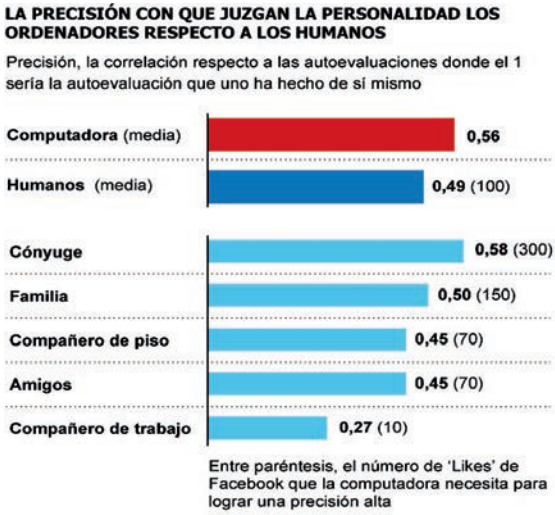

Figura 7.1 Eres lo que te gusta[613]

Ajeno a esta investigación, David García, experto en redes sociales de la Escuela Técnica Federal de Zúrich, demostró recientemente

---

612 CRIADO, M. A. (2013): «Cien 'me gusta' bastan para saber el sexo, raza o ideología de un usuario de Facebook», en *El País*, 11 de marzo de 2013.

613 Fuente: Ídem.

cómo Facebook puede inferir detalles personales no solo de los miembros de la comunidad sino también de sus amigos, aún cuando estos no estén registrados en la red:

> Los patrones que enlazan la amistad con los «me gusta» podrían explotarse para predecir la personalidad de usuarios que no lo desean. Es decir, imaginemos que me gusta Snooki [personaje de un *reality show* estadounidense] pero no quiero que se interpreten mis datos. Si a la mayor parte de mis amigos también les gusta Snooki, quien tenga los datos de mis amigos puede deducir que soy una persona extrovertida sin tener mis «me gusta». [...] El factor social de la privacidad hace que el control de este tipo de predicciones esté fuera del individuo[614].

Simplemente teniendo en cuenta la cantidad de datos que la compañía declara recopilar, un sencillo ejercicio de triangulación nos ayudaría a desvelar, sin problema alguno, no solo la identidad real del individuo que se esconde tras los contenidos, sino la descripción detallada de muchos de los aspectos que conforman su existencia. Todo ello, sin sumar las posibilidades de agregación de datos que añadiría la utilización de informaciones procedentes de otros servicios de la Web 2.0.

No obstante, verificar exclusivamente los efectos que pueden provocar en la integridad privada del individuo esta «declaración de intenciones», sería quedarse en la superficie de la cuestión dado que, lo que no aparece indicado de manera explícita en las cláusulas de uso del servicio es que la empresa puede agregar una cantidad ingente de informaciones a un determinado individuo, usando para ello estrategias más agresivas y no declaradas, o bien indicadas de manera confusa en sus condiciones de uso. Veamos pues cómo Facebook consigue hacer accesible la información privada del sujeto.

3. ESTRATEGIAS AGRESIVAS DE RECOPILACIÓN Y EXPOSICIÓN DE DATOS

Forzada en parte por las quejas de los usuarios y las denuncias de organismos competentes en la protección de la intimidad y vida pri-

---

[614] David García citado en: CRIADO, M. A. (2015): «Eres lo que 'te gusta'», en *El País,* 12 de enero de 2015.

vada, así como por la necesidad de esquivar contiendas legales, a medida que muchas de las prácticas abusivas de la compañía salían a la luz, se han ido incluyendo en sus políticas de privacidad otras fuentes de recolección de la información no mencionadas hasta entonces. No en vano, la plataforma ha sido criticada y señalada periódicamente en los medios de comunicación por usar estrategias más violentas de obtención de datos, propiciando un flujo de intercambio de informaciones privadas opaco para el interactor. Y ello, en parte, aliñado con constantes actualizaciones en las condiciones del servicio de las que no siempre se ha informado correctamente a los miembros de la comunidad. Dicho proceder, hasta entonces insólito, ha propiciado que en países como Alemania, Canadá, Estados Unidos o Irlanda se redactasen informes para evaluar el alcance de las intromisiones en la red social. Analicemos pues, más detenidamente y siguiendo un criterio de aproximación cronológico, dichos métodos de recolección encubiertos.

3.1 LA EXPOSICIÓN DE LA IDENTIDAD LIGADA AL AUMENTO DE LA VISIBILIDAD DEL USUARIO: LA CREACIÓN DEL «CANAL DE NOTICIAS» *(NEWS FEED)*

La exposición de la personalidad constituye una constante en la Web 2.0 y es atribuible, particularmente, a la idiosincrasia de las redes sociales. Sin embargo, es en el caso del libro de caras donde este fenómeno ha alcanzado unos niveles inusitados. Todo comenzó en septiembre de 2006, fecha en la que introdujo una nueva funcionalidad, denominada «canal de noticias», mediante la cual la estructura de la plataforma posibilitaba una exhibición de las acciones del individuo sin precedentes.

Antes de esta fecha, Facebook era una herramienta algo más discreta. Si un miembro de la comunidad quería ver las acciones que habían llevado a cabo sus contactos, debía revisar todos sus perfiles, uno por uno, cada vez que se conectaba a la red e independientemente de si dichos contactos habían realizado cambios o no. Para solventar esta ingrata práctica que hubiese lastrado la expansión posterior de la red social, la compañía resolvió aplicar una herramienta tomada

de las bitácoras y los motores de agregación de noticias: el *news feed feature* o «canal de noticias», como se tradujo a nuestro idioma.

Figura 7.2 Canal de noticias[615]

Dicho «boletín» personalizado que, en realidad, se componía de dos funcionalidades *(news feed y mini feed)* conseguía publicitar al máximo cada una de las acciones que cada participante llevaba a cabo en la red. De una parte, desplegaba información reciente de las actividades de cada miembro en las páginas de inicio de sus contactos *(news feed)*[616] a la vez que hacía lo propio con cada usuario sobre sus propias actividades *(mini-feed)*[617]. En otras palabras: cuando alguien ejecutaba una acción, esta herramienta lo mostraba a todos sus enlaces sin que estos tuviesen que revisar cada perfil. El individuo ya no necesitaba proclamar continuamente su actividad, Facebook, reconvertido en cronista de lo ajeno y lo propio, lo hacía por él.

Para sorpresa de la compañía, la introducción del canal de noticias despertó una amplia reacción en contra por parte de sus miembros

---

615 Fuente: https://epic.org/privacy/facebook/

616 ZIMMER, M. (2007): *Op. cit.*

617 ROSMARIN, R. (2006): «Facebook's Makeover», en *Forbes*, 5 de octubre de 2006.

primigenios (todos ellos, recordemos, estudiantes) afrontando la primera de las numerosas controversias que ha protagonizado a lo largo de su intensa historia. La principal objeción era que mandaba demasiada información sobre cada sujeto a sus contactos, sin que este pudiera controlarlo. Según afirman Hull, Lipford y Latulipe, esta problemática era equiparable a la suscitada por las prácticas de vigilancia pública masiva, como aquella referente a las cámaras de seguridad en calles y otros espacios de uso común ya descrita por Helen Nissenbaum. La diferencia es que esta vigilancia se había centrado en un recinto exclusivo del espacio público mediado, esto es, en los perfiles de Facebook y, para muchos estudiantes, aquello rozaba poco más o menos el acoso. Como resultado, los universitarios se encontraron con menos protección a su vida privada, toda vez que sus contenidos eran más fácilmente visibles.

Para la socióloga Danah Boyd, Facebook convirtió lo que previamente estaba oculto en una información difícil de pasar por alto y apenas olvidable, haciendo que todos esos datos que ya existían antes, pero que nadie se había molestado en recolectar, fuesen ahora cómodamente accesibles. Asimismo, cogió desprevenidos a los primeros moradores de la plataforma. Estos percibían Facebook como un espacio semipúblico destinado solo al público estudiantil y auspiciado por las más prestigiosas universidades, mientras que la red social se dedicaba a expropiar un importante abanico de publicaciones de todo tipo para introducirlas en otros contextos en los que ya no estaban justificadas.

Esta es la primera muestra flagrante, recuerda Boyd, de ruptura del espacio privado por parte de la plataforma y de uso de los datos de los integrantes del sistema más allá de su potestad de control:

> La información no es privada porque nadie la conozca, es privada porque el conocimiento es limitado y controlado. En la mayoría de los escenarios, las limitaciones son a menudo más sociales que estructurales […] Existe un área oscura inmensa entre los secretos y la información que se tiende a proclamar tan públicamente como sea posible. La gente ha usado Facebook como su estuviera inmerso en esa zona oscura […] Cuando las acciones comenzaron a ser difundidas a través del canal de noticias, estas fueron sacadas de con-

> texto y convertidas en mucho más visibles de lo que parece razonable. En otras palabras, con el canal de noticias Facebook alteró esa zona oscura[618].

Tras proliferar grupos en la propia plataforma instando a la compañía a la eliminación del canal de noticias, Facebook resolvió ofrecer a los estudiantes nuevos controles para gestionar la información anunciada en este peculiar noticiero personalizado. No obstante, ni este mecanismo ha desaparecido de la estructura de la red, ni la queja de los miembros del sistema siguió adelante. Paradójicamente, a pesar de que claramente esta funcionalidad violaba la intimidad y vida privada de los miembros de la plataforma, los usuarios comenzaron a aceptar el hecho de que sus acciones fuesen sistemáticamente anunciadas a sus contactos, fomentando incluso ellos mismos la aparición de cierto tipo de actualizaciones[619].

Sin embargo, si bien es cierto que la exposición impulsada por este tipo funcionalidades se ha convertido en una práctica aceptada, no podemos pasar por alto que el pago que generamos con la exhibición de nuestras informaciones personales es más que elevado. Y a esto debemos sumarle un hecho: las posibilidades de control sobre nuestros propios datos que ofrece Facebook a través de las configuraciones de privacidad asociadas a ese canal de noticias se han modificado numerosas veces en los últimos años, pero sin que la salvaguarda de la vida privada figure entre las prioridades que motivan estos cambios.

La problemática va más allá de una simple exposición de acciones e informaciones al instante. Bajo la superficie de esta flagrante vulneración del ámbito privado se averigua un fenómeno más peligroso:

---

618 BOYD, D. (2008): *Op. cit.*, p. 18. Para un análisis más completo al respecto se puede revisar la obra de SOLOVE, D. J. (2007): *The future of reputation: Gossip, rumour and privacy on the internet*. New Haven, CT: Yale UP, pp. 170 y 198.

619 BOYD, D. (2008): *Op. cit.*, p. 15; para evidencias de esta aceptación, véase: JOINSON, A. N. (2008): «'Looking at,' 'Looking up,' or 'Keeping up with' People? Motives and uses of Facebook», en *CHI 2008 Proceedings: Online Social Networks*, pp. 1027-1036, p. 1031.

mediante la manifestación pública y no siempre percibida de datos que los individuos creen protegidos, la compañía alimenta cierto tipo de interacciones entre sus contactos de primero, segundo y tercer grado. Dichas interacciones se refieren a lo sencillo que resulta exhibirse ante los otros sin que suponga, aparentemente, ningún perjuicio para nuestra integridad personal. La visibilidad alimentada desde Facebook actúa así como un motor que desencadena el contagio de pautas de comportamiento, provocando que otros miembros del sistema no tomen las debidas medidas necesarias para salvaguardar sus informaciones, al entender que no se trata de una conducta peligrosa. Al fin y al cabo, si otros ya lo han hecho antes no puede ser peligroso. Aunque, para ser exactos, es la plataforma quien empezó a hacerlo por ellos. Facebook, como si del mensajero de los usuarios se tratase, había decidido por voluntad propia y sin que estos lo supieran, leer su correspondencia a todo el mundo y hacerla accesible en cualquier momento.

En consecuencia, este efecto contagio provoca que los individuos comiencen a mostrarse voluntariamente en el escaparate público, entendiendo que es la mecánica que hay que desarrollar dentro de la red social. Es por ello que esta revelación sin precedentes de la vida privada en las pantallas ajenas impulsada por el canal de noticias, se considera el punto de inflexión tras el cual muchos sujetos deciden modificar sus actitudes respecto al resguardo de sus datos privados. Y no solo al explicitar voluntariamente contenidos que corresponden a su círculo íntimo, sino modificando su percepción de riesgo, movidos por las acciones previas de otros contactos. Este hecho ilustra y verifica a la vez no solo el fenómeno del contagio de los comportamientos como una de las constantes típicamente observables en los participantes de una red social, sino la facilidad con que estos entramados comunicativos pueden introducir alteraciones en la manera en que conceptualizamos lo que debe ser accesible y lo que no.

Por su parte, y a pesar de las críticas, la compañía obtuvo réditos de la situación: Además de aumentar la desinhibición de los participantes fomentando las mencionadas interacciones, la introducción del canal de noticias consiguió incrementar el tiempo que cada usua-

rio dedicaba a publicar actualizaciones en sus perfiles y revisar las de los demás, suponiendo un valor añadido que rentabilizar gracias a la publicidad. Consiguientemente, y si tenemos en cuenta que el valor de los sitios de redes sociales se mide en función del número de miembros que posee y del tiempo que le dedican al sitio, el precio de Facebook se disparó de manera significativa, convirtiéndose en una plataforma muy apetecible para los anunciantes.

3.2 INTERCAMBIO DE INFORMACIÓN CON TERCEROS

El trasvase de datos puede darse en otros niveles no tan obvios para el usuario, algo que ocurre cuando los contenidos salen de la plataforma de Facebook y se comparten con terceros o viceversa. Esto es lo que sucede cuando entran en juego las empresas asociadas a la plataforma: la citada de nuevo, el intercambio de contenidos personales mediante flujos de información imperceptibles se traduce en pérdida de control y una exposición de la identidad no deseada. Todo ello, envuelto en el entorno altamente voluble y sin fronteras generado por los atributos propios de la Web 2.0, recordemos, la convergencia y la retroalimentación.

3.2.1 **Las aplicaciones de Facebook (Platform Application Programming Interface (API) o Facebook Apps)**

En mayo de 2007, Facebook introdujo su plataforma de aplicaciones, una serie de servicios adicionales para «aumentar la experiencia social en Facebook» [620] incrementando las interacciones entre los participantes. La compañía permitía así que desarrolladores de terceras empresas, ajenas a la red social, crearan funcionalidades adjuntas que pudieran enlazarse a los perfiles de cada participante, toda vez que ofrecía un sinfín de nuevas funcionalidades como añadir contenidos adicionales a sus cuentas, participar juegos en línea con otros contactos o compartir fotos u otros materiales audiovisuales.

---

[620] *Política de privacidad de Facebook, 2007*, en *Archive.org*. Disponible en: http://Web.archive.org/Web/20070118161422/http:/www.facebook.com/policy.php. [27/10/2010].

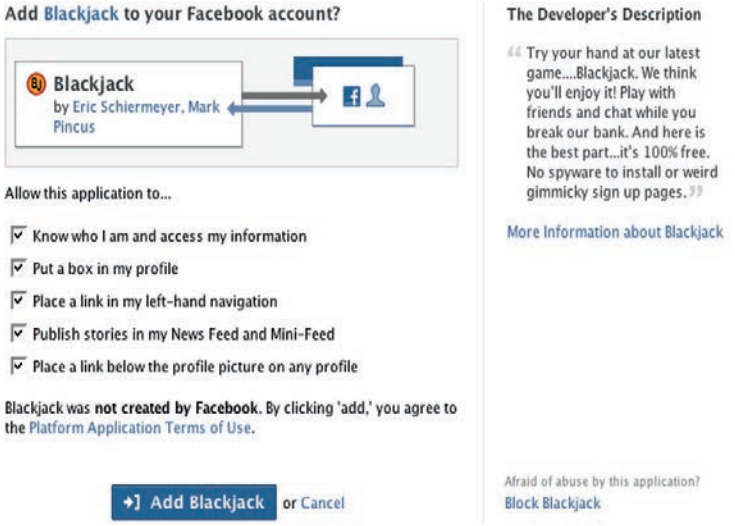

Figura 7.3 Ejemplo de aplicación de Facebook[621]

No obstante, estas aplicaciones que fueron extremadamente exitosas posibilitaban un flujo de intercambio de datos no tan cristalino. De hecho, lo que la generalidad de los miembros de Facebook desconocía era que la plataforma también ofrecía a estos desarrolladores el acceso a la mayor parte de la información del perfil, a excepción de sus datos de contacto.

Más insospechado aún resultaba el hecho de que esta recolección no se limitaba exclusivamente a ese usuario concreto que había decidido usar una aplicación, sino que se extendía al resto de sus contactos. Una fórmula sencilla, en definitiva, para que terceras empresas obtuvieran fácil acceso a una cantidad de datos inusitada, basada en la total e intencionada desinformación de los participantes.

621 Fuente: Facebook.

Figura 7.4 Datos a los que las aplicaciones pueden acceder a través de los contactos[622]

Los creadores de las aplicaciones son totalmente invisibles, lo que oscurece aún más el proceso al ocultar el hecho de que los contenidos están abandonando los límites de la red social y no está fluyendo, exclusivamente, a los contactos seleccionados por cada individuo.

A fin de ilustrar la facilidad con la que nuestros datos pueden ser compartidos por los administradores de estas aplicaciones, nos remitiremos al oportuno ejemplo que, en 2010, plantearon los investigadores Hull, Lipford y Latulipe. Veamos: Cualquier persona puede crear una aplicación que reúna a gente en función de un *hobbie*. Imaginemos, así, que un estudiante alemán desarrolla un juego para que sus participantes elijan qué cerveza les gusta más. Si estos deciden entrar en la aplicación, su información de perfil y la de sus amigos será accesible para el estudiante que creó la aplicación desde su computadora y en su propio dormitorio[623]. Ahora bien, llegados a este punto, el estudiante puede optar por actuar éticamente y no usar los datos para fines ilícitos, pero no hay garantía de ello. Y lo más inquietante es que, como vemos, cualquiera se puede convertir en desarrollador de Facebook y acceder a los datos citados.

La problemática se ve incrementada por el hecho de que, para mantener sus contenidos personales a buen recaudo, los individuos elaboran una serie de estrategias basadas en modelos mentales que, a

---

622 Fuente: Facebook.

623 HULL, G., LIPFORD, H. y LATULIPE, C. (2010): *Op. cit.*, p. 287.

su vez, construyen en función de lo que perciben. Esto es, se guían por la parte visible que les proporciona Facebook, dado que no son capaces de acceder a las dinámicas de datos que se producen bajo su estructura. Se basan, por lo tanto, en las interacciones que llevan a cabo en la red social con sus amigos y en ningún momento son conscientes de que esa información puede ser trasvasada a terceras empresas, dado que todas ellas se integran en un mismo interfaz con la apariencia de ser parte de la propia plataforma.

Para colmo, dichas aplicaciones suelen estar altamente personalizadas, creando una falsa sensación de confianza fundamentada en su supuesta exclusividad y en el ilusorio confinamiento de las relaciones que se desarrollan en ellas. Los usuarios ven como estas aplicaciones usan su nombre y foto, pero ¿por qué preocuparse si también utilizan las de sus contactos? De este modo, recrean la apariencia de un entorno seguro en el que, aunque no conocen qué información están compartiendo, con quién o quiénes son los responsables de que se comparta, tampoco se lo plantean.

Esta donación de información a terceras partes provoca no solo que estas tengan acceso a datos relacionados con la actividad que persiguen, sino a un rosario de informaciones personales de cada sujeto que, por definición, se destinarán a un uso indebido puesto que su utilización no se corresponde con la que motivó su introducción. Una vulnerabilidad que acechó a los usuarios, principalmente, en los primeros momentos de integración de las aplicaciones y que se vio acrecentada por el hecho de que la compañía no ofreció, en ningún momento, información transparente sobre las peculiaridades de la nueva funcionalidad:

> Durante un largo período de tiempo después de que Facebook empezara a publicar aplicaciones en su sitio, se engañó a la gente acerca de cuánta información era compartida con las aplicaciones que usaban. Facebook decía que cuando la gente autorizaba una aplicación, ésta solo tendría la información de los usuarios que requiere para trabajar. [No obstante] las aplicaciones podían acceder a toda la información del usuario, incluso información sin relación con la operación de la aplicación[624].

---

[624] FAIR, L. (2011): «The FTC's settlement with Facebook. Where Facebook went wrong». Federal Trade Commission Protecting America´s Consumers, 29 de noviembre de 2011.

El oscurantismo en el tratamiento de los datos personales motivó que el 31 de mayo de 2008 los investigadores de la Universidad de Ottawa, Lisa Feinberg, Harley Finkelstein y Jordan Eric Plener crearan el proyecto: *Minefield of privacy invasion*[625], bajo el paraguas de la Comisión de Privacidad de Canadá (Canadian Internet Policy and Public Interest Clinic, CIPPIC). Dicho documento especificaba que la plataforma había violado la ley de protección de datos canadiense y lo había hecho hasta en 22 ocasiones. Chris Nelly, por aquel entonces uno de los portavoces de la compañía, intentó quitarle hierro a la denuncia arguyendo que el informe redactado partía de un error de base, ya que «todos los datos de Facebook son intencionalmente compartidos por los usuarios»[626]. Sin embargo, la Comisionada para la Protección de la Vida Privada, Elizabeth Denham, entendió que las quejas eran sólidas pues estaban bien fundadas, por lo que presuntamente la compañía infringía la legalidad con su actividad. De hecho, el 16 de julio de 2009 continuó adelante con la demanda y Facebook resolvió entonces modificar las condiciones del servicio:

> El portal ha anunciado que desde ahora las aplicaciones desarrolladas por terceras partes deberán especificar a qué datos personales acceden y solicitar permiso para difundirlos. Facebook exigirá a las aplicaciones que especifiquen las categorías de información de los usuarios a las que desean acceder y que obtengan el consentimiento de éstos antes de que se compartan esos datos[627].

Empero, los cambios introducidos por la plataforma no resultaban suficientes para asegurar que los sujetos daban, de manera efectiva e informada, su consentimiento expreso tanto al despliegue de sus datos personales, como a su intercambio con terceras partes. Toda vez, que no habían implementado las medidas necesarias para evitar el acceso no autorizado de los desarrolladores a dicha información.

---

625 «CIPPIC files privacy complaint against Facebook», CIPPIC, 30 de mayo de 2008. Disponible en: https://cippic.ca/sites/default/files/NewsRelease_30May08.pdf. [22/05/2012].

626 Chris Kelly citado en MAURIENI, C. (2012): *Facebook is Deception (Volume One)*. Estados Unidos: WSIC Ebooks, p. 37.

627 TOSBACK (2009): *Política de privacidad de Facebook, 29 de octubre de 2009*.

Lejos de acallarse, la polémica se reavivó en 2010, año en que los cambios en la política de privacidad introducidos por Facebook volvían, si cabe, aún más inermes a todos los miembros del sistema que utilizaban aplicaciones y, por extensión, a sus contactos. Bajo el nuevo régimen de 2010, ciertos contenidos cuya visibilidad el individuo podía controlar anteriormente, pasaban a ser tratados bajo una nueva categoría denominada: «Información públicamente accesible» *(Publicly Available information o PAI)*. De este modo, desaparecían los controles de privacidad sin que los propietarios de la información pudieran optar a que esta se mantuviera visible solo para sus enlaces. Y esto, a su vez, suponía que al compartir datos con *Facebook Apps*, la compañía trataría dichos contenidos como públicos, al igual que ya había hecho con otras informaciones.

En la misma línea, la sección en la que se aseguraba que nunca se utilizarían los contenidos privados fuera del servicio de Facebook había desaparecido en la versión actualizada de la política de privacidad y, en lo concerniente al uso de los datos por terceras empresas, el nuevo apartado denominado *Preapproved Third-Party Websites and Applications,* afirmaba:

> Para proporcionarte experiencias sociales útiles fuera de Facebook, necesitamos proporcionar ocasionalmente Información General sobre ti a un sitio Web pre aprobado [sic] o aplicación de terceras empresas que usan la plataforma, al mismo tiempo que tú visitas sus páginas (si estás todavía conectado a Facebook). Similarmente, cuando uno de tus amigos visita un sitio Web pre aprobado [sic] o aplicación, este sitio recibirá Información General sobre ti, dado que tú y tus amigos estáis conectados en este sitio Web (si tú tienes también una cuenta). En esos casos, requerimos que dichos sitios Web pre aprobados [sic] o aplicaciones pasen por un proceso y firmen acuerdos separados destinados a proteger tu privacidad[628].

La razón por la que a pesar de las múltiples quejas de organismos y grupos de usuarios Facebook siguió adelante con su plataforma de aplicaciones y con unos cambios que erosionaban aún más la vida privada del individuo es simple: resulta complicado poner trabas a un negocio que ha engendrado toda una nueva economía. Sólo en Estados Unidos existían, en 2012, más 235.000 puestos de trabajo rela-

---

[628] *Extracto de la Política de privacidad de Facebook, abril de 2010.*

cionados con el sector de las aplicaciones[629], cifra que no ha dejado de aumentar desde la fecha. No obstante, para regatear las críticas la compañía se ha intentado desvincular de las prácticas de estas terceras empresas, apuntando que se tratan de desarrolladores externos y que no puede controlar cómo usan la información personal. A la vez, la red social ha añadido ciertos controles, *a posteriori*, para que sea el usuario el que, una por una, deniegue el acceso a los contenidos por parte de estas aplicaciones, un trabajo ímprobo teniendo en cuenta la multitud de desarrollos existentes en el universo del libro de caras:

> Puedes desactivar todas los sitios Web pre aprobados [sic] o aplicaciones usando tus controles de privacidad del apartado *Applications and Websites*. También puedes bloquear un sitio Web pre aprobado [sic] o aplicación señalando «no gracias» en la barra azul cuando visitas dicha aplicación o sitio Web. Además, si sales fuera de Facebook antes de visitar una un sitio Web pre aprobado [sic] o aplicación, este no será capaz de acceder a tu información[630].

3.2.2 **La publicidad a la carta: Facebook Beacon**

En noviembre de 2007, la empresa de Palo Alto tuvo que hacer frente a una de las mayores crisis de su historia tras la introducción de un sistema de publicidad ultra específico que, finalmente, llevó Zuckerberg ante los tribunales. La funcionalidad en cuestión, *Facebook Beacon*, se convirtió en poco tiempo en uno de los mayores quebraderos de cabeza de los miembros de la comunidad, incluidos aquellos especialmente precavidos y que tomaban más medidas a la hora de mantener sus informaciones a buen recaudo. Mediante este sistema, todas aquellas acciones que el individuo había emprendido en sitios Web de terceros y que aparentemente no tenían nada que ver con Facebook eran compartidas, por defecto, con sus contactos en la red social, siendo publicadas en su perfil. Así, tras realizar comentarios, opinar sobre ciertos servicios o bien comprar en tiendas como Blockbuster, eBay o Travelcity, entre otras, estas empresas adheridas a Beacon podían insertar dichas acciones en la página de inicio de cada usuario, publicitándolas a todos sus «amigos» con frases del estilo:

---

629 ALLAN, R. (2012): *Op. cit.,* p. 164.

630 *Extracto de la Política de privacidad de Facebook, abril de 2010.*

«x se ha comprado unos zapatos en ebay.es». Igualmente, esta notificación aparecía visible en la página de inicio del resto de contactos.

Originariamente, si el usuario no emprendía ninguna medida adicional, la acción era publicada automáticamente, es decir, Beacon no solicitaba consentimiento para plasmar esa información, en forma de noticia, en el muro de cada individuo. Y, si no se frenaba la alerta de manera activa, esta seguía enviándose sistemáticamente a todos los agregados. Por el contrario, si el propio interesado deseaba desactivar dicha opción *(opt-out)* debía acceder a un pequeño menú desplegable que aparecía fugazmente en el interfaz, indicando que no daba su asentimiento para que se enviase dicha información. No obstante, el menú emergía de manera confusa, muchos usuarios ni siquiera se percataban de su aparición y si lo hacían, se veían forzados a accionar en cuestión de segundos la opción «no gracias», lo que conllevaba dificultades más que evidentes para llevar a cabo la denegación de permiso. La complejidad era mayor si tenemos en cuenta que dicha operación debía ser realizada tantas veces como sitios Web externos se visitasen.

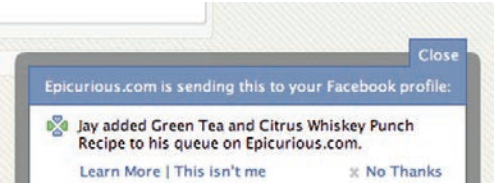

Figura 7.5 Aviso para denegar el envío de información del sistema Beacon[631]

Este hecho generó inmediatamente una reacción en masa contra Facebook en la prensa[632], con quejas de numerosas asociaciones ante la Comisión Federal del Comercio e, incluso, en algunas páginas de la propia red social[633]. Ante el aluvión de críticas, Zuckerberg anunció que la compañía rediseñaría el producto para integrar un sistema de permiso previo (la opción *opt-in*) o lo que es lo mismo: que el programa no mostraría ninguna acción sin el consentimiento explícito por

---

631 Fuente: Facebook.

632 NAKASHIMA, E. (2007): «Feeling betrayed, Facebook users force site to honor their privacy», en *The Washington Post,* 30 de noviembre de 2007.

633 MCCARTHY, C. (2007): «MoveOn.org takes on Facebook's 'Beacon' ads», en *News.cnet.com*, noviembre de 2007.

parte del usuario[634]. Se dio, igualmente, la posibilidad de desactivar el sistema sin tener así que enumerar, una por una, cada Web visitada.

No obstante, Beacon siguió generando dudas. Cada miembro la red recibía poca información y mal contextualizada, y se demostró que la red social seguía recolectando datos incluso si el individuo había optado por no dar su aprobación o aunque ni siquiera hubiera iniciado sesión en Facebook[635]. Esto obligó a la compañía a realizar una segunda aclaración:

> Cuando los usuarios de Facebook realizan una acción posibilitada por el sistema Beacon en uno de los sitios Web participantes, la información es enviada a Facebook para que este pueda operar tecnológicamente con Beacon. Si los usuarios de Facebook señalan «No, gracias» en las notificaciones del sitio Web asociad, Facebook no usará esa información y la eliminará de sus servidores. Separadamente, antes de que Facebook pueda determinar si el usuario ha comenzado sesión en la plataforma, algunos datos pueden ser transferidos desde el sitio asociado a Facebook. En esos casos, Facebook no asociará la información con ninguna cuenta de usuario individual y eliminará los datos, igualmente[636].

En 2008, la plataforma y sus empresas asociadas fueron denunciadas por compartir los datos de los integrantes de la red social sin su consentimiento. Facebook intentó, entonces, limpiar su imagen en la siguiente versión de su política de privacidad, correspondiente a octubre de 2009:

> [Hemos anunciado un acuerdo en un litigio relativo a Beacon: el producto Beacon dejará de funcionar y este término se eliminará de la política de privacidad tras la aprobación de un acuerdo por parte del tribunal.] Facebook Beacon es un medio para compartir las acciones que has emprendido en sitios Web de terceros (por ejemplo, cuando haces una compra o incluyes un comentario) con tus amigos en Facebook. En calidad de usuario de Facebook, para ofrecerte una declaración clara de la

---

634 HANSELL, S. (2007): «Zuckerberg Apologizes, Allows Facebook Users to Evade Beacon», en *The New York Times*, 5 de diciembre de 2007.

635 BERTEAU, S. (2007): «Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking users who opt out or are not logged in», en *CA Security Advisor Research Blog*, 29 de noviembre de 2007. Disponible en: http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s-misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx [09/04/2011].

636 «Thoughts on Beacon», en *Facebook Newsroom,* 6 de diciembre de 2007. https://newsroom.fb.com/news/2007/12/announcement-facebook-users-can-now-opt-out-of-beacon-feature/ [13/04/2010].

> información sobre actividades que se recopila en sitios de terceros y que puede llegar a compartirse con tus amigos en Facebook, recogemos determinada información de dicho sitio y te la presentamos después de haber realizado una acción en el mismo. Tienes la opción de hacer que descartemos dicha información o de compartirla con tus amigos. […] Al igual que muchos otros sitios Web que interactúan con sitios de terceros, podemos recibir cierta información aunque no estés conectado a Facebook o que pertenezca a usuarios que no son de Facebook, desde dichos sitios, junto con el funcionamiento técnico del sistema. En los casos en los que recibimos información de sitios de Beacon sobre usuarios que no estén conectados o sobre usuarios que no son de Facebook, no tratamos de asociarla con cuentas individuales de Facebook y la descartamos[637].

A pesar de la aclaración y tras varios litigios, la empresa resolvió cerrar Beacon en 2009[638]. Durante el tiempo que estuvo activo, más de cuarenta empresas se adhirieron a este sistema de publicidad a la carta. Por su parte, en este periodo Facebook recibió de sus socios los datos personales de individuos que ni siquiera estaban registrados en la red social, toda vez que obtenía información de las compras de los miembros activos. Beacon constituye así un ejemplo ilustrativo no solo de utilización de los contenidos de los usuarios sin su permiso, sino que constituye una muestra palpable de que los datos personales pueden transgredir las fronteras de la plataforma más allá de su propio conocimiento. Una nueva mancha negra en la historia de Facebook que expandió la certeza de que, contrariamente a lo que se asegura desde la compañía, la gente no es capaz de controlar cómo fluye su información.

3.2.3 **Identificación y rastreo a través de lo largo y ancho de la Web: Facebook Connect e Instant Personalization Program**

> «No existe ningún lugar seguro»
> Florian Henckel, *Das Leben der Anderen*[639]

En 2008 y aprovechando las características inherentes a la Web 2.0, Zuckerberg empezó a incrustar Facebook en el lienzo de

---

637 *Política de privacidad de Facebook, revisión de 29 de octubre de 2009*.

638 ORTUTAY, B. (2009): «Facebook to end Beacon tracking tool in settlement», en *USA Today*, 21 de septiembre de 2007.

639 La película de Florian Henckel, *Das Leben der Anderen* (2006) traducida al castellano como: *La vida de los otros*, refleja las prácticas de los últimos días de la Stasi en la ciudad de Berlín.

Internet, introduciendo un cambio fundamental en la plataforma. Tras el descalabro de Beacon, la compañía aprendió la lección sobre lo importante que es dar al individuo la sensación de que ostenta el control efectivo de sus datos, incluso cuando en realidad no lo tiene. Bajo esta premisa, el fundador de la compañía decidió lanzar una tecnología que perseguía algo similar a lo pretendido por el anterior sistema de publicidad: que la gente compartiera en la red social las acciones realizadas en otras páginas Web, con la diferencia de que, en este caso, les ofrecía como moneda de cambio un cierto dominio sobre lo que los demás podían ver de ellos. Así nació el servicio «Conexiones» *(Facebook Connect)*.

Dicho sistema permitía enlazar la cuenta de Facebook a otras de páginas externas con el fin de que los agregados supieran lo que el usuario hacía fuera y dentro de la plataforma, produciendo así una peligrosa simbiosis en la que, cada vez que se accedía registrado en un espacio del universo Internet, también se entraba en la red social. Para ello, *Connect* creaba un sistema de identificación común a todas aquellas Web adheridas, esto es, hacía posible que cada usuario se conectase a estas páginas simplemente usando su cuenta de Facebook. Pero, a la vez, también exportaba sus contactos y otros datos:

> Cuando autorices a uno de estos sitios Web [que operan con Connect] o aplicaciones, nos suministrarán información, incluida la información acerca de las acciones que realizas. En algunos casos, es posible que recibamos una cantidad limitada de información antes de que des tu autorización a la aplicación o sitio Web para poder personalizar el proceso de conexión[640].

Ante cualquier contencioso legal que pudiera derivarse de la actuación de este sistema, como ya sucediera con Beacon la empresa se apresuró en declarar que Connect operaba por cuenta ajena, eximiendo así su propia responsabilidad respecto al trasvase y agregación de datos más allá de sus confines:

> Facebook no posee ni opera las aplicaciones que usas mediante la plataforma de Facebook (como juegos y otros programas) ni los sitios Web con los que interactúas a través de Facebook Connect. Decimos que estos sitios Web y aplicaciones están «vinculados a Facebook» por-

---

640 *Política de privacidad de Facebook, 29 de octubre de 2009*.

> que usan nuestra plataforma para proporcionarte funciones de naturaleza social[641].

En febrero de 2010, ya había más de ochenta mil páginas Web asociadas a *Connect,* lo que se traducía en sesenta millones de miembros de Facebook participando activamente[642], aunque sin saberlo. La cifra no es baladí, dado que entre las empresas participantes se encontraban algunos de los sitios Web más visitados del planeta, entre ellos: *Yahoo,* en aquel momento la mayor página Web de contenidos; medios de comunicación como CNN o Huffintong Post; dispositivos como *iPhone* y la consola de juegos Xbox o herramientas con gran poder para geoposicionar, como *Foursquare*.

No obstante, un número creciente de compañías eludieron adherirse a este régimen al entender que Connect era una maniobra de Facebook para hacerse con el control absoluto de dichas páginas externas, equiparando su estrategia a la del caballo de Troya. De hecho, a esta «conexión universal a Internet» [643] como la denomina David Kirkpatrick, subyacía un intento meridiano de tornar la red social en Google, empresa con la que Facebook siempre ha pugnado por la supremacía. Todo ello, sin contar con los beneficios económicos de su explotación comercial, pues Connect permitiría llegar y definir con precisión un público objetivo que se multiplicaba por momentos.

Una vez más, la peor parte se la llevaban los usuarios. Facebook había transformado su información personal en «conexiones», lo que permitía que otros miembros de la comunidad pudieran acceder a datos como su lugar de trabajo, lugar de residencia, historia laboral o educación, aún cuando esta información no se quisiese hacer pública intencionalmente[644]. Asimismo, el sistema dejaba al descubierto la identidad de muchos de los habitantes de la red social, puesto que todos aquellos que se conectaban para interactuar usando los dispositivos de Connect, lo hacían con su foto, nombre y apellidos, supuestamente reales:

---

641 Ídem.

642 KIRKPATRICK, D. (2011): *Op. Cit.,* p. 365.

643 Ídem.

644 OPSAHL, K. (2010): «Updated: Facebook Further Reduces Your Control Over Personal Information, en *www.eff.org,* 19 de abril de 2010.

> Deja llevar tu identidad a cualquier sitio al que te conectes online. Como puedes decirle a Connect que mande la información de vuelta a tu perfil de Facebook, es una manera de hacer llegar noticias tuyas a tus amigos de Facebook, como si fueran acciones dentro del propio Facebook. También permite que Facebook preste su «viralidad» —su manera eficiente de transmitir información de un usuario a varios— a cualquier página Web que quiera aprovecharla. De este modo, para los usuarios Facebook Connect es como: una conexión universal a Internet[645].

Esta deriva *orwelliana* de la compañía se acentúa a finales de 2009 y, especialmente, a partir de 2010, alimentada por las líneas de actuación subyacentes a las nuevas políticas de privacidad, basadas en una exposición permanente y trasvase de datos creciente a costa de la desprotección del individuo. Como ya hemos mencionado veladamente, resultaba especialmente preocupante la aparición de una nueva categoría denominada: «información públicamente disponible» que, de la noche a la mañana y sin aviso previo, tornaba en públicas informaciones anteriormente introducidas bajo otras configuraciones. La situación de vulnerabilidad de los miembros de la plataforma se vio entonces seriamente acrecentada. Entre otros cambios, esta información, ahora declarada pública por Facebook, podía ser indexada en motores de búsqueda como Google:

> Dicha información puede ser accesible para cualquiera, incluida le gente que no está en Facebook, ser indexada por los motores de búsqueda de terceras partes, ser importada, exportada, distribuida y redistribuida por la compañía o por otros sin limitaciones de privacidad[646].

Como técnica de recolección y agregación de información personal, Connect actuaba mediante el «Programa de personalización instantánea» *(Instant Personalization Program)* un *software* piloto que permitía a sitios externos a la plataforma obtener y usar la información pública de los perfiles tan pronto como el usuario visitaba dichas páginas. Estas conexiones también se creaban tras pulsar el botón «me gusta» sobre un producto o servicio, ya fuera de Facebook o de una página externa, por lo que la plataforma trataba esas relaciones como

---

645 KIRKPATRICK, D. (2011): *Op. cit.,* p. 365.

646 *Extracto de la política de privacidad de Facebook, abril de 2010.*

información pública[647]. La identidad del usuario aparecía entonces enlazada a dicho producto y la Web externa conseguía acceso sus datos. Sólo por citar un ejemplo, el sitio de música Pandora recibía acceso a la lista de artistas musicales en los que cada sujeto había indicado «me gusta» en la red social si este no había denegado el servicio de manera activa[648]. Para los usuarios que no rechazasen el servicio:

> «Instant Personalization» equivale a una filtración instantánea de los datos personales. Tan pronto se visiten los sitios del programa piloto (Yelp, Pandora o Microsoft Docs) dichos sitios Web pueden obtener su nombre, foto de perfil, sexo, ubicación actual, lista de amigos, todas las páginas a las que se les haya dado «me gusta» y todo lo que Facebook clasifique como información pública. Incluso si se opta por rechazar el servicio, aún habría filtración de datos si alguno de sus amigos usa servicios o páginas Web asociadas a Instant Personalization. Sus acciones pueden dar información personal suya a menos que bloquee dichas aplicaciones de manera individual[649].

Denegar activamente el acceso a Connect suponía realizar una serie de gestiones engorrosas, altamente complejas y que no garantizaban el control absoluto sobre las propias acciones[650]. La dificultad para mantener a ralla la propia visibilidad era tal, que hasta el hermano de Zuckerberg se encontró, al intentar gestionar la ambigua configuración del programa, con que una de sus fotos personales estaba siendo publicada entre las actualizaciones de un tercer grado, es decir, un «amigo de un amigo»[651]. Un ejemplo más que flagrante de la complejidad e ineficacia del sistema para denegar el acceso a los contenidos privados.

Por otra parte, esta eliminación no era absoluta ya que en ocasiones estas conexiones seguían siendo visibles una vez borradas, en una dinámica que no parece responder a aquello que Richard Allan enunciaba como «control activo sobre las propias informaciones personales». Este hecho es especialmente sangrante si tenemos en cuenta que estas se crea-

---

647 OPSAHL, K. (2010): «Six Things You Need to Know About Facebook Connections», en *www.eff.org*, 4 de mayo de 2010.

648 RICHARD, E. (2010): «A Handy Facebook-to-English Translator», en *www.eff.org*, 10 de abril de 2010.

649 Ídem.

650 OPSAHL, K. (2010): «How to Opt Out of Facebook's Instant Personalization», en *www.eff.org*, 22 de abril de 2010.

651 «Zuckerberg family pic stirs Facebook privacy debate» (2012), en *CBS News*, 27 de diciembre de 2012.

ban sin consentimiento previo, eran públicas, sin posibilidad de configuración y actuaban sobre publicaciones anteriores que el usuario había realizado bajo una configuración distinta. En pocas palabras, tras la implantación del sistema Connect, se le retiró al individuo la posibilidad de restringir eficazmente el acceso a parte de su información privada. Y lo más preocupante es que las nuevas herramientas propiciaban el rastreo de los sujetos a través de la Web, favoreciendo una dinámica de cruce de datos que, lejos de achicarse, se ha mantenido hasta la actualidad[652]. Este viraje de la compañía ha facultado una vulneración de la intimidad y vida privada sin precedentes, aprovechando la consabida desinformación, ahora alimentada por una falsa sensación de dominio. No obstante, este hecho no ha impedido que Facebook siga lucrándose con los beneficios conseguidos gracias a dicho sistema.

3.2.4 Ponerle «cara» a la información: el reconocimiento facial como culmen del rastreo de la identidad

«Persona».
Del latín *persōna*, máscara de actor,
personaje teatral, este del etrusco *phersu*
y este del griego *πρόσωπον*
Diccionario de la RAE, 22.º edición

En junio de 2011 y haciendo honor a su nombre, el libro de caras aplicó a su plataforma una opción que ofrecía sugerencias de etiquetado de cada uno de los rostros de las personas que aparecían en las fotografías. El sistema, un programa de reconocimiento facial denominado *Deep Face*, consistía en un *software* analítico que actuaba de manera similar a aquellos desarrollados por los servicios de inteligencia: compilaba y comparaba los archivos fotográficos recientemente publicados con todos los registrados anteriormente por el usuario u otros miembros de la plataforma y en los que había sido etiquetado. Cuando el sistema encontraba coincidencias, sugería el nombre de dicho individuo para que cualquiera pudiera añadir una etiqueta que le identificase[653].

---

652 «With new policy changes, Facebook tracks users across the Web», en *epic.org*, 4 de febrero de 2015. Disponible en: https://epic.org/2015/02/with-new-policy-changes-facebo.html [15/05/2015].

653 «In re Facebook and the Facial Identification of Users», dossier elaborado por la EPIC. Disponible en: https://epic.org/privacy/facebook/facebook_and_facial_ recognitio.html [02/01/2012].

Aunque Facebook defendió su uso aludiendo que los miembros de la comunidad eran libres de utilizarlo y que las fotografías podían desetiquetarse fácilmente, las autoridades de protección de datos europeas alertaron de la ilegalidad de este programa. En concreto Alemania, pionera en materia de protección de la vida privada en Internet, denunció en agosto de ese mismo año que el sistema era contrario al derecho europeo, dado que el consentimiento no se daba de manera explícita, ni *a priori;* siendo el propio afectado el que debía denegar su uso, en vez de estar instalada por defecto la revocación del permiso.

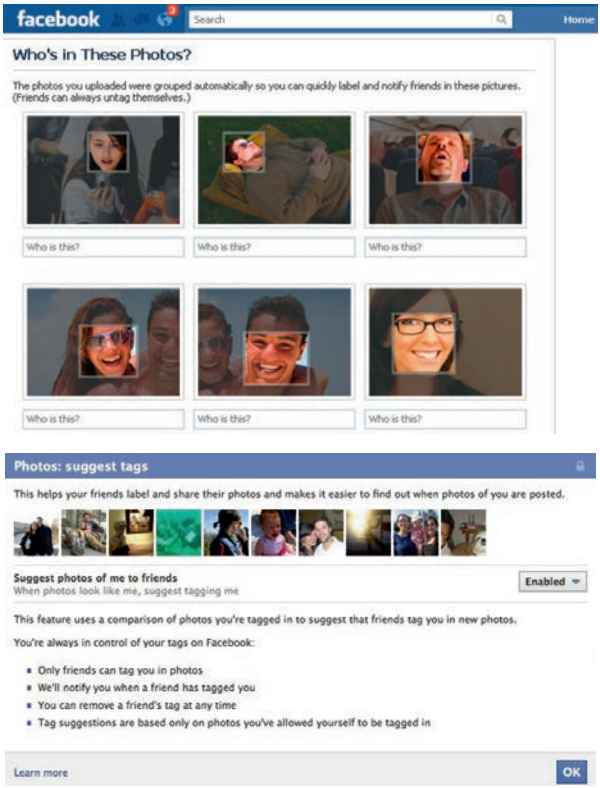

Figura 7.6 Cómo actúa el reconocimiento facial[654]

Tal y como alertó Johannes Caspar, Comisionado en Hamburgo para las libertades informáticas: «el gigante de las redes sociales está

[654] Fuente: Facebook.

recopilando una inmensa base de datos de usuarios ilegalmente»[655]. Este especialista solicitó a Facebook que borrase los datos biométricos almacenados de los perfiles, consciente de que esta función alimentaba en el fondo «una base de datos destinada al reconocimiento físico de millones de usuarios» [656]; y reprochando a su vez el registro de dichos contenidos sin que los protagonistas de las fotos estuvieran capacitados para otorgar su asentimiento. «Si los datos de los usuarios caen en malas manos —advirtió— sería posible comparar e identificar a cualquiera al que se le tome una fotografía con un teléfono móvil»[657].

A pesar de las repetidas reuniones del Comisionado con la cúpula de la compañía, la empresa continuó con el desarrollo de programas específicos destinados a afilar dicho reconocimiento[658]. Así, lejos de contemplar las leyes comunitarias, Facebook anunció en 2014 un nuevo *software* mejorado capaz de identificar a una persona concreta con más precisión incluso que un ser humano[659].

4. LA VULNERACIÓN DE LOS CONTRATOS DE USUARIO: CLÁUSULAS ABUSIVAS Y MODIFICACIONES SIN PREVIO AVISO

Que las políticas de privacidad y protección de datos personales de la compañía están plagadas de potenciales —y no tan latentes— violaciones del ámbito reservado de las personas es un hecho que resulta palmario tras el extenso catálogo de prácticas desleales anteriormente citadas. No en vano, si Facebook ha recibido infinidad de críticas desde que alcanzó difusión global es, en parte, por sus abusivos términos de uso en cuanto a datos e imagen, una vulneración

---

655 O'BRIEN, K. J. (2012): «Germans Reopen Investigation on Facebook Privacy», en *The New York Times*, 15 de agosto de 2012.

656 CASPAR, J. (2011): «Facebook's biometric database continues to be unlawful«, nota de prensa en *Der Hamburgische Beauftragte fürDatenschutz und Informationsfreiheit,* 10 de noviembre de 2011.

657 Ídem.

658 O'BRIEN, (2012): *Op. cit.*

659 TAIGMAN, Y., YANG, M., RANZATO, M. y WOLF, L. (2014): «DeepFace: Closing the gap to human-level performance in face verification», en *Proceedings of IEEE,* Columbus, Ohio, 24 de junio de 2014.

continuada aún cuando el individuo se ha dado de baja[660]. A este respecto, para organismos como la Electronic Privacy Information Center (EPIC) y la Electronic Frontier Foundation (EFF) existe una cláusula de la que parten todas las inquietudes y que, aunque ha sufrido modificaciones con el tiempo, resume a la perfección el espíritu de la compañía:

> [Usted] le otorga a Facebook el derecho irrevocable, perpetuo, no exclusivo, transferible y mundial (con la autorización de acordar una licencia secundaria) de utilizar, copiar, publicar, difundir, almacenar, ejecutar, transmitir, escanear, modificar, editar, traducir, adaptar, redistribuir cualquier contenido depositado en el portal[661].

En otras palabras, en el momento de aceptar el contrato de términos de uso de la comunidad, cada nuevo participante cede la propiedad exclusiva y perpetua de todos los contenidos que agregue a la red social. Y esto a su vez, implica que esas condiciones de licencia ofrecen a la empresa la propiedad comercial de todo lo que tiene que ver no solo con la vida privada de cada miembro de la red, sino con la de sus respectivos allegados, usen o no el sistema; una condición que contraviene, frontalmente, la salvaguarda del ámbito protegido del ser humano. Para el activista de la Electronic Privacy Information Center, Mark Rotenberg, ante este panorama es inevitable que nos cuestionemos el futuro, al fin y al cabo: «¿Es legítimo que una empresa privada se quede con todos los datos que constituyen nuestra identidad digital? ¿Cuánto tiempo deben tenerlos? —Y, sobre todo—, ¿Quién controlará nuestra identidad digital con el tiempo?» [662].

Dicha cláusula, a todas luces indefendible, fue introducida a principios de febrero de 2009 por el departamento legal de Facebook[663]. En realidad, esta afirmación aterradora no presentaba muchas diferencias

---

660 MANETTO, F. (2008): «La cara oculta de Facebook», en *El País*, 27 de enero de 2008.

661 Facebook. *Licencia y términos de uso*. https://es-es.facebook.com/legal/terms?locale=es_ES

662 Mark Rotenberg, declaraciones vertidas en: https://epic.org/privacy/facebook/ [02/01/2012].

663 ORTUTAY, B. (2010): «Facebook Privacy Change Sparks Federal Complaint», en *The Huffington Post,* 13 de marzo de 2010.

con respecto a los términos del contrato anterior, salvo por un pequeño detalle: se había eliminado una aclaración posterior en la que se declaraba que este derecho, es decir, la propiedad exclusiva de los contenidos por parte de la empresa, quedaba extinguido si el usuario eliminaba su cuenta. Bajo las nuevas condiciones, al crear un perfil en la red social, el usuario, sin saberlo, le había otorgado a la empresa el derecho a almacenar sus datos de por vida[664]. Un cambio que pasó totalmente desapercibido hasta que, diez días más tarde, Chris Walters alertó de ello en *The Consumerist*, la bitácora del Sindicato de Consumidores Norteamericanos. El artículo que expresaba su alarma por la cláusula de la discordia, rezaba: «las nuevas condiciones de servicio de Facebook: podemos hacer lo que nos dé la gana con tus contenidos, siempre»[665].

Tras la esperada polémica, Zuckerberg declaró que, si bien desde la red social se arrogaban la facultad de utilizar esta información como quisiesen, «nunca la utilizarían fuera del servicio»[666]; e intentó tranquilizar a los miembros de la plataforma afirmando que al ser ellos los propietarios de los datos, siempre podrían controlarlos: «En realidad la compañía nunca compartiría la información de manera que tú no quisieras»[667]. A ciencia cierta, esta declaración de intenciones no tenía visos de cumplirse por cuanto, en la misma época, la plataforma andaba inmersa en el desarrollo e introducción de herramientas como Connect o el Programa de Personalización Instantáneo, entre otras.

No obstante, dado que las condiciones de servicio seguían estando activas, las aclaraciones del creador de la plataforma no lograban acallar las críticas de todos aquellos miembros que veían como, de la noche a la mañana, habían pasado sin tapujos a ser un activo de la compañía. Ante esta sucesión de acontecimientos, EPIC, junto con otras veinticinco organizaciones de protección del consumidor, resolvieron redactar un documento para demandar a la red social ante la Comisión Federal de Comercio[668]. Zuckerberg anunció entonces que volve-

---

664 Ídem.

665 WALTERS, C. (2009): «Facebook's New Terms Of Service: 'We Can Do Anything We Want With Your Content. Forever'», en *The Consumerist*, 20 de febrero de 2009.

666 «Facebook corrige su cláusula de contenidos tras la polémica», en *El Economista*, 18 de febrero de 2009.

667 CHAN, K. H. (2009): *Op. cit.*

668 ORTUTAY, B. (2010): *Op. cit.*

ría a las condiciones de servicio originales «temporalmente» y mientras desarrollaba unas nuevas cláusulas que permitieran «controlar la información y estuvieran escritas en un lenguaje claro que todo el mundo pudiera entender»[669]. En la misma línea, instauró los denominados *Principios de Facebook*[670] e invitó a todos los miembros del sistema a unirse al grupo denominado *Declaración de derechos y responsabilidades de Facebook*[671] *(Facebook Bill of Rights and Responsibilities)* creado en la propia plataforma para que los participantes diesen su opinión y definir así los nuevos términos de manera conjunta. Invitó, incluso, a los representantes de los grupos de protesta.

La plataforma se comprometió entonces a establecer sus políticas de manera «democrática» «abierta» y, cómo no, «transparente»[672]. A colación de esto y arguyendo que «Facebook es una compañía que introduce nuevas tecnologías potencialmente problemáticas y los usuarios necesitan familiarizarse con los productos antes de ofrecer su aceptación»[673], se anunció que cada cambio se votaría democráticamente y que los resultados serían implantados si conseguían, al menos, un 30% de participación[674]. No obstante, y aunque en un primer momento esta mudanza de talante fue bien acogida por la prensa de todo el mundo[675], más adelante científicos de la universidad de Cambridge[676] y miembros del Open Rights Group[677] tacharon de ficticios estos comicios virtuales: Facebook no publicitaba apenas las votacio-

---

669 CHAN, K. H. (2009): «An update on Facebook governance», en *Facebook blog*, 18 de marzo de 2009.

670 Ídem.

671 Ídem.

672 CHAN, K. H. (2009): «Governing the Facebook Service in an Open and Transparent Way», en *Facebook newsroom*, 26 de febrero de 2009. Disponible en: https://www.facebook.com/notes/facebook/governing-the-facebook-service-in-an-open-and-transparent-way/56566967130 [18/11/2014].

673 Ídem.

674 «Las políticas de privacidad de Facebook cambian», en *Facebook newsroom*, 27 de abril de 2009. Disponible en: https://newsroom.fb.com/

675 CHAN, K. H. (2009): *Op. cit.*

676 BONNEAU, J. (2009): «Democracy Theatre on Facebook», en *Light Blue Touchpaper Security Research*, Computer Laboratory, University of Cambridge, 29 de marzo de 2009.

677 KILLOCK, J. (2009): «Facebook's theatrical rights and wrongs», en *openrightsgroup.org*. Disponible en: https://www.openrightsgroup.org/blog/2009/facebooks-theatrical-rights-and-wrongs [12/11/2012].

nes y, dado que en 2009 tenían doscientos millones de usuarios activos y las votaciones se realizaban en un corto período de tiempo, resultaba altamente improbable que ese 30%, es decir, sesenta millones de personas pudieran votar. A todas luces, se trataba de una nueva maniobra de la compañía destinada a maquillar la flagrante ilegalidad en la que se sustenta gran parte de su emporio.

4.1 LA VIDA PRIVADA SE VUELVE PÚBLICA «POR DEFECTO» Y SIN CONSENTIMIENTO PREVIO

Lo hacemos constantemente: instalamos un programa y damos a «continuar» sin complicarnos, puesto que damos por sentado que las configuraciones por defecto son las más apropiadas para nosotros. Y esto mismo se repite en la red social. Más aún cuando la mayoría de las personas asimilan el uso de Facebook a un instrumento de ocio, por lo que suelen utilizarlo como pasatiempo, de manera más o menos despreocupada y en momentos de cierto esparcimiento. Por ende, el nivel de alerta de los usuarios es, en dichos momentos, bastante bajo y no acostumbran a indagar en las configuraciones que ya vienen predefinidas en el sistema. Del mismo modo, las supuestas garantías que proporciona la simple existencia de dichas opciones por defecto provocan que el usuario se adapte a ellas y se olvide por completo de su existencia, algo que las compañías que diseñan estos sistemas saben de antemano.

La traba, advierte Danah Boyd, es que estas opciones por defecto pueden cambiar y ahí es donde surge el problema[678], especialmente si no se ha informado correctamente de ello. Y eso fue lo que hizo Facebook el 29 de octubre 2009: modificó, sin previo aviso, la política de privacidad, esto es, el contrato firmado entre el usuario y la compañía y que, por aquel entonces, ya habían aceptado 350 millones de personas. Al introducir las nuevas condiciones, la plataforma convirtió de la noche a la mañana los contenidos volcados previamente bajo una configuración más restrictiva, en datos públicamente accesibles, demostrando que se arrogaba el derecho a cambiar las condiciones del

---

[678] Declaraciones de la socióloga Danah Boyd, en HOBACK, C. (2013): *Terms and Conditions May Apply*, documental emitido en *La noche temática - Términos y condiciones de uso*, La 2 TVE, 26 octubre de 2013.

servicio de manera unilateral y en cualquier momento. A este respecto cabe preguntarse: ¿Cómo se consigue violar la legalidad de un contrato firmado por una parte importante de los habitantes del planeta? La respuesta es sencilla: Facebook no lo advirtió y, para cuando los usuarios se dieron cuenta, su información ya era visible para otros miembros de la plataforma e interactores externos.

Zuckerberg intentó entonces maquillarlo como una mudanza de los ideales de la compañía en pro de la soberanía del individuo. En principio, dichas modificaciones estaban dirigidas a simplificar la notoria complejidad de las opciones de privacidad, por lo que servirían para «dar más control a los usuarios sobre las informaciones». No en vano, los cambios aparecen después de que, en 2008, la compañía se comprometiera ante la Comisión de Privacidad de Canadá a desarrollar controles más extensivos y precisos. De este modo y a colación de las críticas recibidas, la red social establecería una nueva arquitectura que permitía limitar el público que podía acceder a cada contenido, introduciendo así una de las peticiones más reivindicadas durante años: la posibilidad de hacer visibles los datos a solo una parte de los contactos, definiendo, mediante un menú desplegable, quien tenía acceso a cada información. Al mismo tiempo, consentía limitar el acceso a la información por parte de los motores de búsqueda y otras herramientas externas.

Para ello, se integró un nuevo mecanismo denominado «herramienta de transición a la privacidad» *(privacy transition tool)*[679] que hacía posible diferenciar entre los materiales mostrados a distintos grupos de contactos; por ejemplo, los accesibles a compañeros de trabajo frente a aquellos mostrados a familiares y amigos más cercanos. Un cambio afortunado, por cuanto propiciaba igualmente que los usuarios estuvieran más pendientes de con quién compartían cada publicación:

> Tú decides cuánta información compartes en Facebook de manera que te sientas confortable y tú controlas como esta es distribuida mediante tus configuraciones de privacidad. […] En Facebook se compartir información con otros —amigos y gente de tus redes— a la vez

[679] «What Does Facebook's Privacy Transition Mean for You?», en *Dotrights.org*, 4 de diciembre de 2009. Disponible en: http://dotrights.org/what-does-facebooks-privacy-transition-mean-you [12/01/2010].

> que te proporcionamos configuraciones de privacidad que puedes usar para restringir que otros accedan a tu información. [...] Puedes controlar quién accede a cierta información que tú has publicado en tu perfil, así como a quién puede encontrarte en las búsquedas a través de tus configuraciones de privacidad. […] Puedes usar tus configuraciones de privacidad para limitar qué información está disponible a «todos»[680].

Sin embargo, bajo este enunciado la nueva política ocultaba algo no tan positivo. Tras el cambio, la plataforma decidió establecer los controles de privacidad en «público» por defecto y lo hizo de manera automática y con efecto retroactivo, es decir, incluyendo publicaciones y otros contenidos que anteriormente los individuos habían decidido no mostrar. Como resultado, miles de informaciones privadas salieron a la luz y los usuarios se volvían cada día más vulnerables, en tanto que no eran conscientes de que todo lo que publicaban a partir de ese momento era visible. Para colmo, la susodicha *privacy transition tool* recomendaba encarecidamente el uso de estas configuraciones públicas. En resumidas cuentas, los nuevos controles no parecían destinados a otorgar más poder a los individuos sino que, por el contrario, los empujaban a compartir públicamente y de manera intensiva su vida privada.

Las críticas no se hicieron esperar. Especialmente sonoras fueron las quejas de la EFF, desde cuya página se invitó a cada miembro de la comunidad a modificar las configuraciones establecidas por la plataforma[681]. Por otra parte, la pretendida simplicidad de los nuevos controles era totalmente ilusoria. Las posibles configuraciones y herramientas para manejar la visibilidad de la información adquirieron una complejidad inusitada para una red social, con cientos de combinaciones imposibles de memorizar por un usuario que se veía abocado a «hacer *click* en más de cincuenta botones de privacidad, eligiendo entre un total de más de 170 opciones»[682].

---

680 *Política de privacidad de Facebook, 29 de octubre de 2009*.

681 BANKSTON, K. (2009): *Op. cit*.

682 BILTON, N. (2010): «Price of Facebook Privacy? Start Clicking», en *The New York Times*, 12 de mayo de 2010.

4.2 LA APARICIÓN DE LA CATEGORÍA «INFORMACIÓN DISPONIBLE PÚBLICAMENTE» *(PUBLIC AVAILABLE INFORMATION, PAI)*

Tras los polémicos cambios introducidos a finales de octubre de 2009, Zuckerberg reformó nuevamente las condiciones del servicio. En esta ocasión y para solventar la controversia de las modificaciones *motu proprio*, la empresa se comprometía a informar, uno por uno, a cada miembro de la plataforma. Así, bajo el título: *Comunicado sobre la privacidad,* una ventana emergía automáticamente en los perfiles para prevenir sobre las nuevas condiciones:

> Si realizamos cambios en esta política de uso de datos, te lo notificaremos (por ejemplo publicándolo aquí [en la página de la política de privacidad] y en la página *Facebook Site Governance*). Si los cambios son sustanciales, mostraremos un aviso prominente según lo requieran las circunstancias. Puedes asegurarte de que recibes notificación directamente haciendo clic en el botón «me gusta» de la página *Facebook Site Governance*[683].

Este cambio de rumbo, aplaudido a partes iguales por interactores y asociaciones, quedó empañado tempranamente debido a las evidentes violaciones que se ocultaban entre el resto de cláusulas de la nueva política. En concreto, la creación de una nueva categoría denominada: «información disponible públicamente» *(public available information, PAI)* estaba en el ojo del huracán. Bajo esta clasificación, cierta información pasaría a ser catalogada automáticamente como información pública y, por tanto, visible a todo el mundo:

> Los cambios que estamos haciendo tienen como finalidad ayudarte a mantenerte en contacto y darte más control sobre la información que compartes […] Al mismo tiempo vamos a mantener cierta información pública (como el nombre o la foto de perfil) para ayudar a que la gente se encuentre y se ponga en contacto. […] Ciertas categorías de información, como tu nombre, foto del perfil, sexo, región geográfica, listas de amigos, redes y las páginas de las que eres fan se consideran información pública y son visibles para todos, incluidas las aplicaciones compatibles con Facebook. Por lo tanto esos datos no tienen configuración de privacidad[684].

---

683 *Política de privacidad de Facebook, revisión de 9 de diciembre de 2009*.
684 Ídem.

Esta disposición, que no aparecía en anteriores versiones, dejaba a los individuos sin posibilidad de manipular los controles de privacidad, haciendo visible datos que anteriormente estaban restringidos. Y lo hizo de manera extensiva, ya que estos controles también desaparecieron del canal de noticias *(news feed)* y de las noticias personalizadas *(mini feed)* por lo que los miembros de la comunidad perdían la posibilidad de mantener cierta reserva sobre las actividades publicadas en sus muros. Tal y como se alertó desde la Federal Trade Commision:

> Algunos datos que los usuarios han designado como privados —como las listas de amigos— han sido hechos públicos amparados por la nueva política […] [Facebook] Ha designado cierta información del perfil de los usuarios como pública, cuando había sido sujeta previamente a los marcos restrictivos de privacidad [a la vez que] ha anulado las decisiones previas de privacidad de los usuarios. Haciéndolo, la compañía ha cambiado materialmente la privacidad de la información de los usuarios y retrospectivamente ha aplicado estos cambios a toda la información previamente recogida[685].

En definitiva, los habitantes de la comunidad se vieron forzados a hacer visibles gran parte de sus contenidos, *hobbies* y quehaceres diarios, incluyendo toda aquella información que previamente habían decidido no publicitar, y todo ello porque la herramienta para restringir dicho acceso había sido eliminada. A este hecho hay sumarle que mediante esta categoría comenzaron a hacerse visibles las páginas Web consultadas por cada miembro, transitando así de una situación en la que el individuo no ostentaba dominio suficiente sobre sus contenidos, a otra en la que la empresa había decidido volver «públicas categorías enteras de informaciones, en una clara lógica de negocios»[686]. De este modo, si una persona deseaba que datos sensibles como, por ejemplo, su residencia, no fueran consultados por terceros, el único remedio eficaz con el que contaba era simplemente no introducirlos y cruzar los dedos para que un tercero no lo hiciera.

Por otra parte, dado que con las nuevas configuraciones todos los contenidos de los perfiles, incluidas las fotografías, quedaban

---

[685] FAIR, L. (2011): *Op. cit.*

[686] OPSAHL, K. (2010): «Facebook's eroding privacy policy: a timeline», *www.eff.org*, 27 de mayo de 2010.

abiertos por defecto, en aquellos casos donde sí se mantenían los controles de privacidad correspondientes, era el usuario el que, expresamente y uno por uno, debía acotar su visibilidad. Como apunte anecdótico, cabe apostillar que tras la entrada en vigor de las nuevas condiciones salieron a la luz más de 300 fotos del fundador de Facebook que anteriormente no estaban disponibles al público. Descuido o estrategia (él mismo se justificó insinuando que quizás lo habría hecho a propósito) lo cierto es que, poco después, Zuckerberg restringió sus fotografías para que no fueran visibles a toda la comunidad de Facebook[687].

Ante esta exhibición gratuita, fomentada por la nueva constitución del universo Facebook, Electronic Privacy Information Center (EPIC) y la Electronic Frontier Foundation (EFF) reclamaron la actuación de la Federal Trade Commission (FTC) así como de la American Civil Liberties Union (ACLU). A estas denuncias se sumaron las de un gran número de grupos de afectados, solicitando medidas para que la empresa explicitara qué información iba a ser compartida y cuál sería su destino. Incluso el periodista Dan Gillmor, figura clave en la divulgación de las bondades de la Web 2.0, decidió borrar su cuenta aseverando que no se podía confiar enteramente en Facebook[688]. Zuckerberg por su parte, defendió los cambios bajo el ya citado *dictum* de que «la época de la vida privada se había acabado» y que estas eran «las normas necesarias para hacer la compañía más social»[689].

La reflexión posterior nos revela que el tema, más allá de las reacciones iniciales, no era en absoluto baladí. Son cuantiosas las investigaciones que alertan de la cantidad de información que se puede obtener de un individuo recolectando todos aquellos retazos de sí mismo que hace públicos en su perfil. Sólo por citar un ejemplo, el Instituto Tecnológico de Massachussets (MIT) llevó a cabo un ensayo bautizado como *Gaydar* para evaluar la cantidad de datos que se podía extraer de un usuario simplemente examinando su lista de amigos. Me-

---

687 «El misterio de las fotos de Zuckerberg en Facebook», en *El País*, 16 de diciembre de 2009.

688 GILLMOR, D. (2009): «facebook-starting-over», en *Mediactive.com*, 12 de diciembre de 2009.

689 KIRKPATRICK, M. (2010): *Op. cit.*

diante dicho estudio, se demostró que era factible predecir, de manera bastante precisa, la orientación sexual de un miembro de Facebook. Y, teniendo en cuenta el cúmulo de contenidos vertidos en la red, la cantidad de información extrapolable no haría sino incrementar con paso del tiempo, lo que permitiría averiguar muchos más aspectos sobre la vida de cada sujeto[690].

Otro aspecto preocupante, según advirtió la Comisión de Privacidad de Canadá, era la cantidad de datos de que disponían ahora los desarrolladores de aplicaciones, ya que no solo recibían información personal de los participantes, sino de todos sus contactos, aún cuando estos habían optado por quedarse fuera del juego. Si bien en la anterior versión de la política de privacidad la plataforma ofrecía la posibilidad de denegar el acceso de dichas aplicaciones, con las nuevas condiciones esta opción había desaparecido y, en consecuencia, los desarrolladores podían obtener las informaciones que quisieran si uno solo de los contactos del usuario había utilizado una aplicación. Para alertar a los ciudadanos, la American Civil Liberties Union (ACLU) promovió un cuestionario que pretendía mostrar a los miembros de la plataforma a qué información podían acceder los desarrolladores de aplicaciones[691]. A buen seguro, los resultados obtenidos por los usuarios no les dejaba indiferentes.

4.3 FACEBOOK RECTIFICA PERO ELUDE CREAR UNAS DIRECTRICES INTERNAS PARA SALVAGUARDAR LA VIDA PRIVADA

Recogiendo una de las peticiones más reclamadas por los usuarios, Facebook añadió nuevas opciones de privacidad que permitían elegir, de manera personalizada, la audiencia de los contenidos publicados. De este modo, las informaciones universalmente visibles serían aquellas que cada sujeto decidía hacer accesibles a sus contactos de

---

690 JERNIGAN C. y MISTREE, B. F. (2009): «Gaydar: Facebook friendships expose sexual orientation», en *First Monday*, vol. 14, n. 10, 5 de octubre de 2009.

691 CONLEY, C. (2009): «Take Our Quiz: See What Do Facebook Quizzes Know About You!» en www.aclu.org, página Web de *American Civil Liberties Union, ACLU,* 26 de agosto de 2009.

tercer grado, es decir, las editadas bajo la configuración «pública» o «todo el mundo»; mientras que los introducidos bajo el epígrafe «amigos» o «amigos de amigos», estarían disponibles solo para los enlaces de primer y segundo grado, respectivamente. Posteriormente, apareció la opción «personalizado» que sucesivamente fue ofreciendo más combinaciones de visibilidad. Estas alternativas no solo restringían qué contenidos eran mostrados en la página de perfil, sino parte de los datos compartidos con las páginas a las que el sujeto se conectaba, incluyendo la información accedida por las aplicaciones y sitios de terceras partes. Igualmente, Facebook restauró los controles de privacidad para las categorías accedidas por Facebook Connect y el Programa de Personalización Instantánea, es decir, para el lugar de residencia, nacimiento, trabajo, educación, gustos e intereses… entre otras, manteniendo algunas como el sexo visibles.

Si bien, a pesar de las mejoras implantadas, la plataforma continuó enfrentando críticas. No solo no publicitó las nuevas opciones tan agresivamente como cabría esperar, sino que los cambios fueron calificados por asociaciones como la EFF, de «insuficientes», dado que la compañía continuaba compartiendo una ingente cantidad de datos personales con otros sitios Web y aplicaciones. Asimismo, cada vez que alguien realizaba un comentario o pulsaba «me gusta» en una publicación o página editada con configuración pública, esta aparecía anunciada a todos sus enlaces en el canal de noticias, incluidos todos aquellos que no eran compartidos. Esta trampa de la que es complicado percatarse a no ser que nos lo comente uno de nuestros contactos, tampoco aparece anunciada en la pestaña «ver cómo», esa función que la plataforma pone a disposición de cada miembro para mostrarle cómo otros usuarios ven su perfil y las informaciones enlazadas a él.

Por otra parte, aunque ahora era posible restringir los contenidos a una audiencia limitada modificando los controles de privacidad, el individuo se topaba con una traba al bucear en la página de configuraciones: la opción para restringir el acceso a los datos personales aparecía desactivada cuando se trataba de aplicaciones utilizadas por sus contactos. En enero de 2011, EPIC presentó una demanda contra la compañía alegando que bajo las nuevas directrices la plataforma compartían con terceras empresas el teléfono móvil y la dirección postal del 0.038% de las personas registradas en la red social, en una práctica «engañosa» que afectaba, particularmente, a los niños me-

nores de 18 años[692]. Facebook resolvió entonces paralizar temporalmente la implementación de los citados cambios, pero solo un mes después anunciaba que reinstalaría las mismas condiciones.

A colación de este hecho, la Comisión Federal de Comercio estadounidense exigió a la compañía que velase por la salvaguarda de la vida privada de los miembros de la comunidad e instó a la empresa de Zuckerberg «a cumplir sus promesas en el futuro, incluidas las de ofrecer a los consumidores información clara y prominente». Más en concreto, en su resolución de noviembre de 2011, la FTC solicitaba a Facebook: «no distorsionar la seguridad que ofrece a la información personal de los consumidores» [693], así como «obtener el consentimiento expreso de los consumidores antes de aplicar cualquier cambio que anule sus preferencias sobre privacidad»[694]. No obstante y a pesar de que la FTC también exigía que crease un programa interno destinado a garantizar la salvaguarda de los datos personales que fluyen por la plataforma, en el presente la compañía sigue anclada en sus prácticas ilegítimas y no ha modificado un ápice sus líneas de actuación más controvertidas.

Paralelamente, en agosto de 2011, la Comisión de Protección de Datos de Irlanda (DPC) comenzó una investigación tras recibir veintidós reclamaciones del grupo de estudiantes austriacos *Europe versus Facebook*. La plataforma, iniciada en 2011 por el ciudadano austriaco Max Schrems junto con otros estudiantes, realizó una petición de acceso a Facebook Ireland solicitando un informe sobre los datos que la compañía había almacenado sobre ellos desde que se habían dado de alta. Para su sorpresa, recibieron 1222 páginas de contenidos por persona, con informaciones catalogadas bajo cincuenta y siete categorías distintas, incluyendo todos aquellos contenidos que habían sido borrados previamente. No obstante, a pesar de la cantidad de documentación, hubieron de realizar una segunda reclamación a Facebook ya que no todos los datos aparecían reflejados: Por ejemplo, no figuraban registros sobre los «me gusta», el reconocimiento facial

---

692 «Facebook Privacy», dossier elaborado por EPIC. https://epic.org/privacy/facebook/ [02/01/2012].

693 Federal Trade Commission (2011): «Facebook settles FTC Charges that it Deceived Consumers by Failing to Keep Privacy Promises», 29 de noviembre de 2011. Disponible en: http//ftc.gov/opa/2011/11/privacysettlement.-shtm [10/01/2012].

694 Ídem.

o páginas de terceras empresas que usaban *plugins* sociales y que los afectados habían visitado habitualmente. Tampoco aparecían incluidos los datos relativos a los vídeos subidos a la página. Este hecho motivó la creación del *Website*: europe-v-facebook.org a modo de protesta. Según el proyecto, actualmente Facebook mantiene, al menos, hasta 84 categorías de información de cada usuario.

La DPC resolvió emprender acciones legales, argumentando ausencia de nitidez y excesiva complejidad en las políticas de privacidad; toda vez que solicitaba a la empresa revisar la protección de los datos personales para los usuarios fuera de Norteamérica. Asimismo, la necesidad de instaurar un sistema para denegar el acceso en el caso de las informaciones compartidas con terceras empresas volvía a hacer aparición por lo que, de nuevo, la polémica sobre cómo otorgar el consentimiento de manera explícita e informada estaba servida. En definitiva, la controvertida cuestión que estaba sobre la mesa era cómo cambiar del sistema de consentimiento *opt-out* al *opt-in*.

En este punto resulta necesario realizar una aclaración: Dado que Facebook posee una sede internacional en Irlanda, responsable de todos los conflictos legales fuera del territorio de Estados Unidos y Canadá, la DPC es legalmente competente respecto a las demandas de los usuarios contra la empresa dentro de suelo Europeo. De hecho, los no residentes de estos dos países firman desde 2010 un contrato con Facebook Ireland, establecida en Dublín. Y puesto que los usuarios reciben este servicio desde una empresa que ha de cumplir con la legislación irlandesa y está bajo el paraguas de la Unión Europea el servicio debe acogerse a las leyes de protección de datos.

Tras la auditoría realizada en diciembre de ese mismo año, la Comisión elaboró un informe no vinculante con las recomendaciones que la plataforma debería adoptar antes de julio de 2012. Richard Allan, Director de Políticas Públicas de Facebook para Europa, defendió la gestión ratificando que cada modificación realizada en las condiciones del servicio partía de la premisa de que es la gente la que «debe controlar el contenido compartido en su cuenta y escoger la audiencia con la que lo comparten»:

> Con los «controles en línea» introducidos en agosto de 2011, cada uno puede escoger fácilmente los ajustes de privacidad, todas y cada una de las veces que publique contenidos, eligiendo la audiencia para la que estos serán visibles. Además, también puede ver las publicaciones ante-

> riores y cambiar los ajustes de privacidad de manera individualizada. Los ajustes de cuenta iniciales recomendados de Facebook se han escogido de manera que las personas puedan encontrar y conectarse fácilmente con sus amigos, al tiempo que protegen la información más sensible[695].

Según Allan, tras la auditoría la empresa salió reforzada, por cuanto se aceptó que:

> En el caso de una red social, el usuario otorga el consentimiento al registrarse en el servicio. Ese consentimiento, combinado con la cantidad de información que Facebook ofrece en su página sobre la forma en que se usa la información y el nivel de control concedido a los usuarios para gestionar los datos, constituye un ejemplo convincente de cómo puede obtenerse el consentimiento de manera firme y muy fácil para el usuario[696].

Aún así, la empresa se comprometió a trabajar conjuntamente con la Oficina del Comisario de Protección de Datos de Irlanda para encontrar la forma de mejorar la información proporcionada a las personas en cuanto a cómo pueden controlar qué datos se comparten al utilizar las aplicaciones[697].

4.4 FACEBOOK ELUDE CREAR UN SISTEMA DE CONSENTIMIENTO Y ADMITE QUE LOS DATOS QUE LOS USUARIOS HAN VOLCADO EN LA PLATAFORMA YA ESTÁN EN INTERNET

A pesar de que la plataforma se vio obligada a colaborar con las autoridades europeas ante la cantidad de quejas recibidas, los cambios para mejorar la seguridad de los individuos no fueron reseñables. Dicha actuación motivó que la Oficina del Comisionado de Protección de Datos de Irlanda volviera a analizar el progreso de Facebook en julio de 2012, redactando un segundo informe en el que se instaba a la plataforma a actuar acorde a la normativa europea.

Entre los deberes que la DPC requería a la red social estaba el de implementar un sistema de consentimiento informado, un punto cla-

---

695 ALLAN, R. (2012): *Op. cit.,* p. 164.

696 Ibídem, p. 165.

697 El Mundo (Ed.) (2012): «Facebook y Linkedin se comprometen a reforzar su privacidad», en *El Mundo*, 29 de junio de 2012.

ve para sustentar la autodeterminación informativa del usuario y a lo que Facebook se ha negado sucesivamente, aludiendo a que la falta de agilidad podría producir una merma en el servicio:

> Aunque el consentimiento es un principio importante, hay que garantizar que no conduce a requisitos demasiado preceptivos que impliquen mecanismos molestos e innecesarios de solicitud de consentimiento para actividades concretas. De ser así, se correría el riesgo de inundar a los usuarios con casillas de verificación y avisos. Esto, aparte de afectar a la experiencia del usuario, conduciría inevitablemente a una posible «devaluación» del principio de control, y podría hacer más complicada la toma de decisiones de los usuarios en lo relativo a cuándo otorgar consentimiento y cuándo denegarlo[698].

No obstante, puesto que la compañía tiene sede en suelo europeo y, por tanto, debe acatar las leyes de protección de datos vigentes en esta región, si desde la Unión Europea se impone la necesidad de integrar un sistema para que el individuo otorgue activamente su permiso, Facebook no tendrá más remedio que amoldar sus prácticas a la legalidad vigente en dicho territorio.

Asimismo, esta no es la única de las recomendaciones realizadas por la DPC que ha quedado en papel mojado. Entre otras reclamaciones se señalaba la necesidad de introducir una herramienta que permitiera a cada miembro ejercitar su derecho de acceso a los datos almacenados y eliminar su huella. Sin embargo, tal y como hubo de admitir finalmente la compañía, borrar totalmente el rastro de los usuarios es misión imposible en tanto que, al ser compartidos con terceras empresas y desarrolladores, no siempre depende de ellos. Y la cuestión se vuelve más polémica «cuando alguien quiere eliminar y ejercer control sobre el contenido que otras personas han publicado»[699].

5. CÓMO USA FACEBOOK LOS DATOS DE LOS PERFILES: LA CREACIÓN DEL SER VISIBLE

En la red social el tráfico de nuestros datos privados sobrevuela todos los puntos del planeta conectándonos con el resto de habitantes

---

[698] ALLAN, R. (2012): *Op. cit.,* p. 165.
[699] Ídem.

del universo Facebook. El pequeño inconveniente es que, a mitad de camino, nuestras acciones, cargadas de imágenes, vídeos, enlaces y otros contenidos, son interferidas, analizadas y, en muchas ocasiones, hasta reelaboradas. Así que, una vez que se ha producido este expolio masivo a través de prácticas hondamente controvertidas, la pregunta de rigor es: ¿Para qué necesita la empresa semejante provisión de retales íntimos? ¿Qué hace tan valiosas nuestras vivencias? La respuesta es bien sencilla: para la plataforma cada persona es un conjunto de datos personales, «me gustas» y demás contenidos muy atractivos para los anunciantes. Este es el verdadero negocio de la red social y la razón por la que cada miembro está pagando un precio más que elevado por usar un servicio que se presupone gratuito.

Esta monetización de los datos personales es el aspecto más preocupante de la red social por cuanto supone, no solo la revelación de informaciones de carácter privado, sino que delinea los contornos de un negocio cuyo provecho económico se basa en una materia prima obtenida sin consentimiento explícito de sus propietarios. Así, lo que la compañía refiere convenientemente como consentimiento, es en realidad un permiso por omisión, en el que si se produce algún cambio en las condiciones del servicio estas se dan por admitidas si el sujeto no las deniega activamente. En resumidas cuentas, se da por entendido que si no dejamos de usar el servicio, nuestra vida privada será susceptible de ser ofertada al mejor postor, sin tan siquiera advertirlo. Y en el otro extremo, el usuario, ajeno a todo ello, no es capaz de otorgar o prohibir de manera explícita dicha utilización ilegítima de sus datos puesto que ni siquiera tiene constancia de ello.

Consecuentemente, conveníamos en afirmar en las primeras líneas de este trabajo que, en la era digital, la información se ha convertido en una variable estratégica muy poderosa para las compañías. Pero los datos por sí solo no valen nada si no se analizan, se les añade significado y se relacionan, y eso es lo que hace de Facebook una empresa tan poderosa, tan bien valorada por los anunciantes y tan agresiva para nuestra intimidad y vida privada. La tendencia a migrar las inversiones publicitarias desde un planteamiento cuantitativo, típico de los medios de masas tradicionales, hacia otro más cualitativo y personalizado basado en el comportamiento, incrementa el valor de los datos, entre ellos, los capturados en los diversos usos y modalidades de navegación. Y que la compañía analiza las conductas de sus inte-

grantes, perfilando su semblanza hasta límites insospechados es, hoy por hoy, un hecho palpable.

Lo que aún no hemos afrontado en este análisis es cómo Facebook consigue integrar a un usuario cualquiera, presumidamente anónimo, en un determinado público. Ni cómo esto puede provocar, por extensión, que su identidad real sea desvelada. Para desentrañar esta incógnita, en el siguiente apartado examinaremos dos de las directrices maestras en torno a las que gira el negocio de la compañía: la creación del público objetivo *(targeting)* y el rastreo *(traking down)*.

5.1 DE LA PERSONA AL PRODUCTO: LA «COSIFICACIÓN» DEL USUARIO MEDIANTE LOS «ANUNCIOS DE COMPROMISO»

Comencemos por una afirmación categórica: La red social simula «el dorado» moderno de los anunciantes, tanto para grandes empresas, como para modestos comerciantes con negocios locales. Ofrece un universo inusitado de posibilidades para la inserción de publicidad, aliñado con promesas de acceso a un público perfectamente definido, aspecto en el que Facebook no tiene rival posible. La propia empresa se lo hace saber a todos los interesados que visiten su página de publicidad: «Los usuarios consideran a Facebook parte de sus vidas por lo que puedes estar seguro de que conectarás con personas con un interés real en tus productos» [700].

Todo ello se consigue gracias a *Facebook Ads* [701], un *software* mediante el cual se puede saber qué usuario ha hecho «clic» en un anuncio concreto y dirigirlo hacia el segmento de mercado más adecuado; siempre en función de una serie de parámetros como son: el sexo, la edad, emplazamiento geográfico, términos clave, nivel estudios, idiomas, situación sentimental u orientación sexual. En consecuencia, la tarta de Facebook se torna muy atractiva para los anunciantes que se topan con un escenario idílico que les permite llegar, a bajo coste, a un público muy segmentado. Y las cifras que mueve este negocio no son triviales: solo en julio de 2009 Facebook y Myspace ofrecían más

---

700 *Política de privacidad 2014.*

701 *Facebook Ads*: https://es-es. Facebook.com/about/ads»

del 80% de los anuncios gráficos en la Red[702]. Centrándonos en la red social, solo en el segundo trimestre del año 2014 obtuvo una facturación de 788 millones de dólares en este concepto[703].

Esta publicidad, altamente personalizada, es efectiva por cómo se integra en los comentarios cotidianos de los habitantes de la comunidad, al no interrumpir el discurso narrativo, ni ser percibida como tal. Así, desde un primer momento la empresa decidió no usar técnicas explícitas como *banners* o molestas ventanas emergentes, sino introducir los anuncios en el propio contenido creado por los individuos, lo que hace que formen parte constituyente de sus propias interacciones:

> Los anuncios deben ser contenido. Tienen que ser solo información orgánica que la gente produce en la página. Mucha de la información que la gente produce es inherentemente comercial. Y si miras en el perfil de alguien, casi todos los campos que le definen tienen algo de comercial: la música, las películas, los libros los productos, los juegos…forman parte de nuestra identidad, como personas a las que nos gusta algo, pero también tiene un valor comercial[704].

Este tipo de anuncios basados en la información orgánica que la gente introduce en la página es lo que Zuckerberg denominó como «anuncio de compromiso», por cuanto genera un mayor vínculo con el individuo y resultan mucho más efectivos que los clásicos enlaces patrocinados en los que el usuario se percata de que se le está mostrando publicidad. Los anunciantes, por su parte, son capaces de interactuar directamente con los potenciales clientes, peguntándoles qué color de móvil deberían usar en los nuevos modelos de determinada marca o cómo quieren que sea el nuevo refresco de cola. Y, dado que es dentro de las fronteras de este gigantesco país virtual donde se producen estas transacciones, la red social, como la banca, siempre gana.

El engranaje del mecanismo funciona a la perfección. Facebook empareja los anuncios con el contexto social, de forma que surgen historias sobre acciones relacionales que cada miembro o sus contac-

---

[702] «Las redes sociales crecen en publicidad», en *CNN Expansión,* 2 de septiembre de 2009 [02/07/2010].

[703] «Facebook aumenta usuarios, ingresos y presencia en el móvil», en *La Vanguardia,* 23 de abril de 2014.

[704] Declaraciones vertidas por Zuckerberg sobre los anuncios en Facebook y recogidas en: KIRKPATRICK, D. (2011): *Op. cit.,* p. 310.

tos han llevado a cabo. Es decir, mediante el uso de los «me gusta» y la lectura de las palabras clave la publicidad de un restaurante puede asociarse con una historia del canal de noticias que indique que a uno de nuestros contactos le gusta esa página. Por ejemplo: si al individuo le gustan los países tropicales, la plataforma obtendrá esta información tras analizar tanto los contenidos que ha introducido, como la información que proviene de sus contactos y de las acciones que ha realizado en otras Web de terceras empresas y, como recompensa, le ofrecerá publicidad de agencias de viajes y hoteles en el Caribe. De este modo, los anuncios aparecen hipercontextualizados por lo que no siempre se identifican los servicios publicitarios como tales. Y da igual si un miembro decide no introducir sus características reales: la empresa se encargará de deducir qué clase de sujeto se esconde detrás de un apodo simplemente con los datos añadidos por sus agregados o analizando sus interacciones. En última instancia: ¿qué más da si un miembro de la comunidad se hace llamar «pepito grillo» si este es susceptible de consumir refrescos azucarados? Una identidad falsa no impide que su catalogación en un determinado público objetivo sea exitosa. Y «Pepito grillo» acabará viendo, insistentemente, el anuncio de ese refresco de cola. En esta mecánica, la plataforma no solo convierte al sujeto en potencial cliente y consumidor, haciendo que las marcas entren a formar parte de las interacciones cotidianas de los individuos, también alimenta una «cosificación» de la persona, que acaba por interiorizar este tipo de actuaciones. Así es como Facebook transforma, en palabras del escritor británico Tom Hodgkinson, «las relaciones humanas en *commodities*. Es la extracción del valor capitalista de las amistades»[705].

5.2 DEL USUARIO AL CLIENTE: USO COMERCIAL DE LOS DATOS PARA CREAR EL PÚBLICO OBJETIVO (*TARGET*)

En los últimos diez años, el fenómeno Facebook ha propiciado la aparición de multitud de monografías destinadas, en su gran mayoría, a desvelar los pasos seguidos para dar a luz a un negocio tan exitoso. Sin embargo, en el relato de los acontecimientos que todas ellas

---

[705] HODGKINSON, T. (2008): «Por qué detesto Facebook y las redes sociales», *Diario Clarín,* 23 enero de 2008.

realizan un dato llama poderosamente la atención: en los primeros momentos de expansión de la compañía Zukerberg rehusó, repetidamente, introducir publicidad para financiar su servicio, intentando diferenciarse así de empresas como Google cuyas páginas se lucraban abiertamente gracias a los anunciantes. No obstante, el rápido crecimiento de la plataforma y las posteriores necesidades de financiación propiciaron que el fundador se replantease cómo convertir en dinero su populosa creación.

El poder en las redes sociales, a diferencia de empresas como Google, es que la materia prima les viene sola. Los programadores ponen el sustrato y los participantes hacen el resto al completar los diversos campos requeridos con sus datos e interactuar con otros miembros de la comunidad. El atractivo de estas plataformas lo constituyen las dinámicas desarrolladas por sus participantes, gracias a las cuales los anunciantes no necesitarán darse a conocer con onerosas campañas promocionales, puesto que los propios miembros de la red social se encargarán de propagarán sus mensajes a todos sus enlaces. La publicidad de Facebook es, por ello, mucho más personalizada y, consecuentemente, más efectiva que la de Google:

> Cuando [el usuario] busca un producto en la ventana de Google, [el buscador] presenta un anuncio que es la respuesta a las palabras que ha anotado en la ventana de búsqueda. A menudo resulta interesante y ese proceso genera millones de dólares a Google. Pero los anunciantes sobre los que acostumbras a clicar son los que ya sabías que buscabas. En jerga publicitaria, la publicidad de búsqueda del *AdWords* de Google satisface a la demanda. La de Facebook, en cambio, generaría demanda […] combinando su capacidad sin parangón de orientar los anuncios basándose en la información de los usuarios, lo que permitiría atraer cada vez más publicidad generadora de demanda. […] Facebook da más opciones a los anunciantes de llegar a un público objetivo. […] Si compran un anuncio en Google que aparece cuando la gente escribe «cámaras», en Facebook pones un anuncio similar para hombres casados de California, con hijos pequeños que aún no han colgado ninguna foto[706].

Los habitantes de la comunidad Facebook ofrecen gran cantidad de contenidos sobre ellos mismos que, a su vez, generan más información personal a través de la confrontación de estos con el comportamiento dentro y fuera de la página. Una veta inagotable que la

---

[706] KIRKPATRICK, D. (2011): *Op. cit.,* pp. 308-309 y 311.

plataforma rastrea en su base de datos, captando pautas de comportamiento y agregando a estas las informaciones recabadas de los perfiles. De este modo, la red social exprime al máximo la esencia de cada uno de sus integrantes para ofrecerles anuncios a la carta, volteando la ecuación del mercado publicitario:

> Para poder mostrarte contenido que sea de tu interés, puede que utilicemos toda la información que hemos recibido sobre ti para sugerirte anuncios que te resulten más interesantes. Esta información incluye, por ejemplo: la información que proporcionas durante el proceso de registro o que añades a tu cuenta o biografía[707].

Así, antes de la llegada de la red social las empresas gastaban grandes sumas en campañas de publicidad, a la vez que intentaban deducir, mediante el seguimiento del rastro de los individuos por Internet, informaciones como su edad, sexo, intereses o páginas que visitaban, entre otras. Ahora Facebook hacía este trabajo por ellas, arrogándose el derecho a usar dichos datos al realizar este filtrado y vendiendo al mejor postor sin que terceras partes tuvieran acceso necesariamente:

> [Mediante] el contenido que compartes y generas en Facebook, como lo que te gusta y tus interacciones con anuncios, socios o aplicaciones, palabras clave extraídas de tus historias y aspectos que deducimos del uso que haces de Facebook. […] Cuando ofrecemos anuncios, no compartimos tu información (información personal que te identifique, como tu nombre o información de contacto) con anunciantes a menos que nos concedas permiso para hacerlo. Puede que proporcionemos a los anunciantes información sobre ti una vez eliminado tu nombre y otros datos personales que te identifiquen o de forma conjunta con otra información para que no puedan identificarte. Por ejemplo, puede que el anunciante reciba información relacionada con el rendimiento de su anuncio o con el número de personas que han visto su anuncio, que han hecho clic en él o que han instalado una aplicación tras verlo[708].

Los anunciantes, por su parte, ven como su trabajo se simplifica sustancialmente. Es más, la propia plataforma pone a su disposición una herramienta a través de la cual pueden escoger el públi-

---

707 *Política de privacidad, 2014.*
708 Ídem.

co adecuado para insertar su publicidad, siguiendo diversos parámetros como la ubicación, los datos demográficos, las preferencias extraídas de los «me gusta», las palabras clave y cualquier otra información que la compañía recibe o deduce de los habitantes de la comunidad.

Sobra señalar que la legitimidad de este lucrativo negocio viene lastrada por las dudosas prácticas que Facebook lleva a cabo para recolectar dichos contenidos, así como por la falta de información que proporciona sobre ello y la imposibilidad de rebatir el consentimiento.

No obstante, que como usuarios nos cataloguen en un perfil determinado y nos sitúen dentro de un grupo concreto de posibles compradores no significa que se conozca nuestra identidad. Dicho de otro modo: la creación de público objetivo, aun cuando esta se realice por medios poco legítimos, no implica, en ninguno de los casos, la revelación de los nombres y apellidos reales del sujeto.

En principio, cuando nos catalogan como público objetivo los usuarios no dejamos de ser un cúmulo de números de serie que representan, a la postre, nuestro identificador virtual. La duda, tanto en el caso de Facebook como de otras muchas redes sociales es si, además de añadir significados como preferencias o lugar de residencia a ese identificador numérico también se agrega un nombre y apellidos, dejando, por tanto, de ser anónimo. Y el hecho de que a este respecto en las políticas de protección de datos se juegue con términos ambiguos como: «puede que otras empresas usen tus datos», no confirma ni desmiente nada. Es por ello que, sin bien desde la red social sí se alude a la creación de ese público objetivo, no aclaran si realizan prácticas correspondientes a la correlación de estos datos con las identidades reales de cada participante. Y ello teniendo en cuenta que, cuando se combinan cuatrocientos millones de informaciones de personas con datos, «no solo sobre dónde viven, sino de quiénes son sus amigos, qué intereses tienen y qué hacen cuando están conectados, potencialmente, Facebook posee el proyecto genoma de Internet» [709].

---

[709] Mike Lazerov, Consejero Delegado de Buddy Media, citado en KIRKPATRICK, D. (2011): *Op. cit.,* p. 318.

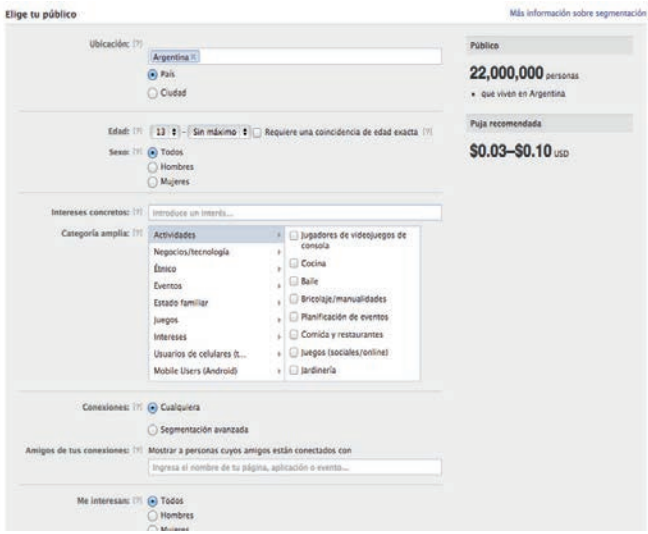

Figura 7.7 Público objetivo[710]

5.3 DEL USUARIO ANÓNIMO A LA IDENTIDAD REAL: USO DE LOS DATOS Y RASTREO DE LA HUELLA DIGITAL CON NOMBRE Y APELLIDOS (*TRACKING DOWN*)

Sabemos que tanto Facebook, como las empresas que actúan dentro de los lindes de la red social, son capaces de rastrear las acciones que llevan a cabo los individuos cuando están conectados. Hemos reseñado igualmente que, aunque estos introduzcan un nombre falso, sus actividades, informaciones agregadas y la contrastación de datos con los contenidos producidos por sus contactos pueden acabar poniendo su nombre y apellidos a su identificador numérico. El hecho es que Facebook posee esta tecnología, sea susceptible o no de usarla, y para muchos grupos y activistas en pro de la protección de los derechos civiles, la gestión de la compañía despierta sospechas, aún cuando desde sus estatutos se declare:

> Solamente proporcionamos datos a nuestros socios publicitarios o a nuestros clientes después de haber eliminado tu nombre y otros datos que puedan identificarte, o bien después de haber combinado tus datos con los de otras personas de manera que no te identifiquen[711].

---

[710] Fuente: Facebook.

[711] *Política de privacidad de Facebook, 2014.*

Es por ello que aunque el rastreo es un hecho evidente no implicaría necesariamente la identificación. Este seguimiento de la huella del individuo se realiza a través de las *cookies*, ya sean de la propia compañía o de terceras empresas: «En ocasiones, los anunciantes y sus socios utilizan *cookies* u otras tecnologías similares con el fin de publicar y llevar un seguimiento de los anuncios y mejorar la eficacia de estos»[712]. Frente a estas *cookies* de terceros, la empresa se autoexime de responsabilidad, aún cuando estas comienzan a actuar dentro de la plataforma Facebook.

Sin embargo, algo que la compañía evita mencionar es cómo gestiona sus propias *cookies,* programas que usa no solo cuando se ha iniciado sesión en Facebook, sino que, según los estudios de Nik Cubrilovic[713], se instalan en el navegador y siguen enviando información incluso después de que el usuario haya abandonado la plataforma. En otras palabras, rastrea el comportamiento de cada individuo a lo largo y ancho de la Web semántica, un ejemplo más de cómo la violación del ámbito privado del sujeto perpetrada por Facebook empaña todo el universo Internet.

Aunque esta no es más que una de las múltiples tácticas de *tracking down* aquí mencionadas y por la cual un grupo de usuarios decidió demandar a la compañía[714], el dato más preocupante sigue siendo la sombra que planea sobre la posible correlación de informaciones con los nombres reales. Y las aclaraciones que ofrece el libro de caras a este respecto son contradictorias. Facebook declara que nunca revela a los anunciantes las identidades reales, sino que trata los datos de manera anónima con el fin de averiguar ciertos parámetros y así orientar la publicidad a una serie de sujetos concretos. Empero, las discordancias imperantes en su propia política de protección de datos se encargan de restar validez a la afirmación anterior:

> Puede que permitamos a los anunciantes llegar a usuarios de Facebook haciendo uso de la información con la que cuentan ya (como di-

---

712 Ídem.

713 CUBRILOVIC, N. (2012): «Facebook and many other sites also bypass Internet Explorer privacy controls», *New Web Order*, 21 de febrero. www.nikcub.com/posts/facebook-also-doesnt-honor-p3p/ [12/03/2012].

714 REISINGER, D. (2012): «Facebook sued for $15 billion over alleged privacy infractions», en *News.cnet.com*, 18 de mayo de 2012.

> recciones de correo electrónico o información relativa a si has visitado su sitio Web con antelación o no)[715].

Centrándonos en este ejemplo, tampoco se especifica en qué momento estas terceras empresas han conseguido las direcciones de correo electrónico, un dato que, como señalábamos al comienzo de este escrito, se considera personal por cuanto puede conducir a la identidad de su propietario.

Por otra parte, las cláusulas que cada individuo acepta al registrarse en la plataforma habrían sido vulneradas en cuantiosas ocasiones, tal y como se desprende de un informe publicado en agosto de 2010 y, según el cual, Facebook habría enviado a sus empresas asociadas los nombres, edades y profesión de todos aquellos usuarios que visitaban sus anuncios[716]. Destaca, especialmente, el período comprendido entre septiembre de 2008 y mayo de 2010, cuando los anunciantes pudieron hacerse, literalmente, con la identidad de todos aquellos que hicieron «clic» en los anuncios[717]. Dicha cesión de información a sociedades con intereses ajenos pasó desapercibida por la generalidad de miembros de la red social que, para colmo, leían en los estatutos de la empresa la negación total de este hecho. Después de que dichos informes saltasen a la luz pública y se hiciesen *vox populi*, la negación inicial respecto a la posible identificación de las identidades reales comenzó a tornarse en cierta ambigüedad discursiva, con menciones confusas, incoherentes e incluso paradójicas en las sucesivas políticas de privacidad. Si bien, ahora sabemos que, además de facilitar estos datos a terceras empresas, Facebook cooperó con los servicios de inteligencia norteamericanos facilitándoles datos identificativos de las personas registradas en la plataforma.

Como corolario, debemos señalar uno de los datos más preocupantes de la Web 2.0 y que ya no constituye una práctica exclusiva de la compañía. Las herramientas de la Web semántica posibilitan un cruce de datos que, en última instancia, puede acabar mostrando nuestra identidad real. No obstante, esta triangulación no tiene por qué ser desarrollada exclusivamente por una empresa como Facebook, sino que puede venir de la mano de cualquier interactor con un

---

715 *Política de privacidad de Facebook, 2014.*
716 KIRKPATRICK, D. (2011): *Op. cit.,* p. 365.
717 FAIR, L. (2011): *Op. cit.*

buen manejo de Internet y la paciencia o curiosidad suficiente para averiguar el nombre y apellidos de la persona que se oculta tras los datos. Y aunque esta identificación no es factible en todos los casos, el hecho de que herramientas como las redes sociales y, en especial, Facebook sean capaces de recopilar, manejar y exhibir tal amalgama de datos, facilita mucho que cualquier usuario pueda descubrir retazos de la vida privada de otros similares, enlazándolos finalmente a sus nombres y apellidos. La Web se convierte así, en un inmenso directorio en el que las interacciones en la red social nos ofrecen muchas pistas acerca de lo que buscamos.

6. REFLEXIONES SOBRE EL CAPÍTULO

Si algo le debemos encarecidamente a Facebook es que gracias a la imbricación de la red social en todos y cada uno de los aspectos de nuestra cotidianeidad, hemos descubierto el valor creciente de nuestros datos. Su capacidad de conexión, la posibilidad de mantener el contacto con viejos amigos y la familia, la atracción de mostrar nuestro día a día y sentirnos arropados por una red de personas entre las que nosotros somos el centro… todo ello engancha a la gente y la compañía de Palo Alto lo sabe bien. Como consecuencia, su *status* de supremacía se debe a que la materia prima, esto es, nuestras informaciones personales, les viene sola: la empresa proporciona el soporte, pero son los propios participantes los que nutren con sus contenidos el mayor banco estructurado de datos personales de todo el mundo.

De entre las redes sociales y otras herramientas relacionales de la Web 2.0, la plataforma se presenta como un valor seguro para los anunciantes y no solo por poseer la comunidad de usuarios más populosa del mundo, sino porque su arquitectura permite obtener muchas más informaciones personales que cualquier otra red social. Este es sin duda el gran salto competitivo de Facebook: la capacidad de conocer al posible consumidor hasta puntos anteriormente inalcanzables para poderle ofrecer una publicidad completamente personalizada y claramente orientada a sus posibles demandas. Así cuando el perfil de las redes sociales, como si de un dossier personal se tratase, está lleno de información de cualquiera de los aspectos del ser humano, este se convierte irremediablemente en reclamo para terceras empresas; emergiendo esa sociedad de exposición continua

en la que todo, hasta la identidad, es susceptible de transformarse en mercancía.

Desde la óptica del sujeto, el panorama es buen distinto. Al registrarse en dicha plataforma da por sentado que su información será confidencial y nunca será utilizada sin su permiso, ni sin ser perfectamente informado. No obstante, dado que no existe consentimiento expreso e informado, sino que cualquier cambio se sobreentiende aceptado por omisión del afectado, averiguar si la confidencialidad de los datos contenidos en el perfil se ha diluido es empresa baldía. Y ello aliñado con el uso de técnicas, no declaradas, para explotar al máximo el valor de cada miembro registrado y reconvertido en potencial consumidor.

En suma, podemos aseverar que la red social por antonomasia ha obtenido una posición de privilegio con respecto a otras herramientas relacionales de la Web 2.0. Sus prácticas abusivas y la violación sostenida de los derechos de los individuos han suscitado que grupos de derechos civiles reclamen un control más estricto desde los poderes públicos.

Por su parte, la compañía ha sabido regatear las numerosas controversias mediante obtusas políticas de privacidad redactadas bajo un lenguaje confuso y en las que se evita mencionar algunos de los aspectos más polémicos. Dichas cláusulas no solo son poco accesibles para el usuario al que, por supuesto, se pretende responsabilizar de la totalidad de interacciones que suceden en la red social, sino que, como evidenciaremos en el próximo capítulo, fomentan la desinformación que le torna más vulnerable.

CAPÍTULO VIII. LAS INTERACCIONES DE LOS USUARIOS EN LAS REDES SOCIALES Y LA PARADOJA DE LA VIDA PRIVADA

SÍNTESIS

Desde la popularización de las redes sociales, son cuantiosas las investigaciones que tratan de dilucidar hasta qué punto los individuos son conscientes de la exposición incontrolada a la que someten su vida privada, cuando interactúan a través de las tecnologías digitales. Es decir, si pueden considerarse los responsables últimos de sus actos, tal y como se apunta desde los estatutos de las grandes compañías que operan en la Red. Dichos sondeos se centran no solo en las percepciones de riesgo de los usuarios, sino en si entienden la idiosincrasia y el funcionamiento de los entornos virtuales y, por tanto, son conscientes del trasvase de contenidos que se da entre los servicios de la Web semántica. En suma, se intenta valorar si los sujetos están en disposición de preservar activamente sus contenidos reservados dentro de esta vorágine de intercambio de datos que constituye el tejido mismo de la Red, ejecutando así su autodeterminación informativa. Partiendo de esta premisa y con la base que otorga haber delimitado las prácticas ilícitas más habituales, en el presente capítulo saltaremos al otro lado del espejo para analizar las motivaciones y planteamientos que hay detrás de las acciones que ejecutan los usuarios en este difuso escenario. Para ello, nos valdremos del análisis de la paradoja de la vida privada, un fenómeno ampliamente documentado en la literatura científica y que arroja considerables dudas sobre hasta qué extremo es el propio sujeto el que controla lo que sucede en estas plataformas.

1. INTRODUCCIÓN: POR QUÉ ESTUDIAR EL COMPORTAMIENTO DE LOS USUARIOS

Los pequeñas teselas que conforman el mosaico de nuestra esfera privada ya están en el escaparate virtual para deleite de todo aquel que desee consultarlas. No se trata de una afirmación descomedida: Tras

la infinidad de interacciones previamente descritas —sazonadas todas ellas con un trasvase de datos que, en parte, no somos capaces conocer, ni controlar— podemos asegurar, sin miedo a equivocarnos, que muchas instantáneas de nuestra existencia ya pueblan la Web en forma de datos personales visibles y accesibles. Y en este universo de significados enlazados a identidades, las redes sociales se han revelado como la fuerza de atracción que nos empuja a exhibir públicamente nuestras experiencias en la vida, algo que, además de erosionar el aspecto más reservado de nuestra persona, nos presenta como el blanco perfecto de la publicidad personalizada.

En consecuencia, es factible pensar que hemos cedido a la mecánica desarrollada por este tipo de herramientas y que esta se ha convertido en una práctica aceptada, en tanto que es más valioso el beneficio adquirido. Ahora bien, ¿Hasta qué punto somos conscientes de este proceso y sus consecuencias? ¿Recibimos la información necesaria para tomar decisiones meditadas, controlar nuestros contenidos y ejecutar nuestra autodeterminación informativa de manera eficiente?

La filosofía defendida por empresas como Facebook y otras populares plataformas propaga la idea de que es dado establecer que si todas las prácticas de las compañías aparecen detalladas en las condiciones del servicio y el individuo es libre de introducir o no sus datos personales, este se convierte automáticamente en el responsable único del control de sus datos y la gestión de su identidad virtual[718]. Y, ciertamente, la transparencia «surge como un elemento imprescindible, acaso en teoría idóneo e insuperable, para permitir al usuario el libre albedrío sobre sus datos personales»[719]. No obstante, antes de estigmatizar al sujeto y culparle de no otorgar el valor suficiente a sus contenidos más privados, Enrique Badía recuerda:

> El argumento de partida suena impecable: en tanto que propietario de los datos que afectan a su intimidad, nadie mejor que la propia persona para determinar y decidir quién, cómo, cuándo y para qué pueda utilizarlos, difundirlos o, en su caso, comercializarlos […] Pero la realidad, en parte de nuevo por imperativo del avance tecnológico, muestra

---

[718] No mencionamos en este ensayo otras compañías como Google, aunque la dialéctica utilizada para justificar sus prácticas es la misma.

[719] BADÍA, E. (2012): *Op. cit.*, p. 19.

> que semejante lectura anda excedida de sencillez. Hay que decir, en primer término, que ningún marco se puede considerar idóneo si su esencia descansa en una suerte de sobrecarga sobre el usuario[720].

El pago que generamos con la exhibición de nuestras informaciones personales es bastante elevado, provocando que multitud de personas se encuentren totalmente desvalidas cuando ciertas consecuencias indeseadas hacen su aparición. No se trata, por tanto, de un hecho aislado: según datos recogidos por el *Eurobarómetro Especial 359*: *Attitudes on data protection and electrones identity in the European Union*, el 74% de los europeos cree que desplegar información personal es una parte creciente de la vida moderna, pero solo un 25% de aquellos que utilizan las redes sociales considera que poseen la potestad completa de sus datos personales mientras que el 43% cree que se les solicita más información de la necesaria. Lo más alarmante es que, a pesar de usar abundantemente estas herramientas comunicativas, el 70% declara cierta inquietud sobre el tratamiento que las compañías dan a sus datos, algo sobre lo que sienten que solo tienen un control parcial, si es que tienen algún tipo de dominio. Esto, sumado al hecho de la complejidad que conlleva averiguar cómo serán gestionadas nuestras informaciones en todas y cada una de las aplicaciones de la Web 2.0, nos incita a desvelar hasta qué punto el usuario es responsable de alimentar el juego de la exhibición.

Por otra parte, indagar en qué motivaciones y creencias guían las conductas de los sujetos nos ayudará a entender mejor esa parte de la ecuación, lugar común de la maraña tecnológica, que sí está en nuestra mano modificar y cuyas acciones se pueden convertir en el mejor arma para evitar las intromisiones. Comenzaremos, así, evaluando las creencias de los interactores y principales prácticas desarrolladas por ellos en estos entornos, con el objetivo de evaluar cómo la información que recibimos modela y condiciona nuestra percepción de riesgo así como las medidas que tomamos para protegernos. En definitiva, si somos conscientes y entendemos correctamente el flujo informativo que se da en la Web 2.0. Realizaremos, para ello, un somero repaso de los estudios de usuarios más reseñados centrados en esta problemática, contenida en parte en el fenómeno denominado como *paradoja de la vida privada* y que explicaremos a continuación.

---

720 Ídem.

2. LOS ESTUDIOS DE USUARIOS

> Debemos ser lo más abiertos posibles
> para romper ideas preconcebidas a la hora
> de acceder a los conceptos sociales.
> Investigación real.
>
> Bruno Latour

Dado que el ser humano es, al fin y al cabo, el epicentro en torno al que pivotan las tecnologías todas, la generalidad de los estudios destinados a desvelar su comportamiento en la Web social ponen su acento en las herramientas más popularmente usadas, esto es, las redes sociales y los buscadores, mayoritariamente representados por Facebook y Google. Dentro de estas, las investigaciones sobre cómo interactúan los individuos se ciñen exclusivamente a las redes sociales, herramientas que suscitan dudas debido no solo a la amplia comunidad de usuarios que pueblan muchas de ellas, sino a que son sus propios participantes los que se encargan de ceder sus contenidos. Es este elemento intencional el que lleva a los eruditos a mover el foco hacia las decisiones de los interactores. Dentro de estas, la plataforma Facebook, con su facilidad para recolectar datos personales e infringir las normativas, alienta una cantidad ingente de investigaciones científicas cuyo fin último es describir las posibles consecuencias indeseadas e intentar aportar soluciones para mitigar los perjuicios derivados.

En este panorama y puesto que también nos proponemos conocer cómo actúa el otro extremo de la ecuación conformado por las plataformas de redes sociales, el análisis de las prácticas, creencias, motivaciones y percepciones de los sujetos constituye una prioridad académica. No en vano, son multitud los estudios que se ha desarrollado desde preceptos tanto cuantitativos como cualitativos, aproximaciones que, en ocasiones, se combinan entre sí o se anejan al uso de programas informáticos de simulación y/o análisis. De este modo, se consigue evaluar no solo cómo actúan los individuos, sino sus percepciones de riesgo y su nivel de conocimiento de los entornos tecnológicos. Entre todos ellos, destacan los llevados a cabo por Besmer y Lipford; Boyd; Brandtzaeg, Lüders y Skjetne; Cunningham y Masoodian; Lange y Nippert-Eng Sleeper y Balebako. La tendencia es usar métodos integrados o complementarios, lo que indica que se desea superar la división inoperante entre ambos métodos, cuya exclusión mutua deja puntos sin tratar.

Dentro de estos estudios, las primeras aproximaciones académicas, nacidas al albor del despegue de la Web semántica, se centran prioritariamente en los jóvenes, un colectivo aparentemente más vulnerable, a la vez que osado, a la hora de apropiarse de las innovaciones tecnológicas. Y aunque, *a priori*, los resultados mostrados señalaban que tal vez la actitud despreocupada de este segmento poblacional provocaba que tomasen decisiones no meditadas en detrimento de la protección de sus propios contenidos, a medida que se expande el universo de las redes y los estudios se abren a otros rangos de edad, se notifican actitudes contradictorias, incluso en aquellos sujetos que desean protegerse proactivamente. Asimismo, se evidencia que la preocupación por el propio control de las informaciones personales es común a la generalidad de los individuos, independientemente de su edad y competencia digital. Así, los denominados: *digital outsiders*[721], o personas no familiarizadas con el lenguaje de Internet y que empiezan ahora a tomar contacto con la Red, declaran sentirse indefensos para afrontar los peligros que puede acarrear su uso. Dicho sector es el formado por los ciudadanos de más edad que se han sumado más tarde al tren de las tecnologías digitales, pero cuyo uso de la Red se ha incrementado considerablemente. De hecho, este subconjunto de la población consulta sus pruebas médicas, realiza transacciones bancarias, visita páginas gubernamentales, llena la cesta de la compra y reserva viajes a través de la Web, pero su desconocimiento fomenta que no adopten las medidas de protección necesarias[722].

Por su parte, los conocidos como «inmigrantes digitales», es decir, todas aquellas personas que se han ido sumando poco a poco a la Red, muestran a menudo cierto escepticismo sobre si sus datos serán gestionados debidamente por las grandes plataformas de servicios digitales. Finalmente, se atestigua que incluso los denominados «nativos digitales», que han nacido inmersos en la era Internet y, presumiblemente, son más diestros en el ecosistema digital que las generaciones

---

721 BUCHMANN, J. (ed.) (2013): *Op. cit.,* p. 30.

722 CHAI S., y RAO, H. R. (2008): «'WiRed' senior citizens and online information privacy», en M., Ward Bynum, T., Rogerson, S., (eds): *Living, working and learning beyond technology* (ETHICOMP 2008), 24-26 September 2008, en Mantua Italia: University of Pavia, pp. 101-110.

precedentes, a menudo admiten sentir miedo de ser monitorizados o identificados por otros usuarios[723].

Muchas de las investigaciones que se llevan a cabo para evaluar esta complicada relación entre protección de informaciones privadas e interacción con las tecnologías digitales hacen hincapié en la idea de que los usuarios son concebidos como consumidores que se ven forzados a realizar decisiones individuales sobre su protección. La premisa sustantiva es, pues, que los sujetos están abocados, en cierta medida, a entrar en el juego de un mercado que les pide traficar con su información privada a cambio de la obtención de beneficios sociales[724], algo que resulta palpable en algunos de los servicios más populares de la Web semántica.

Sin embargo, una corriente comúnmente observada en las distintas investigaciones es la prevalencia de discrepancias entre los deseos de protección y reserva de los sujetos y las medidas efectivas que toman para llevarla a cabo, un fenómeno que se conoce como «paradoja de la vida privada»[725] o «paradoja de las informaciones privadas» *(privacy paradox)* y que fue observado antes, incluso, de la llegada de la Web 2.0. Dichas actitudes contradictorias en lo relativo a la salvaguarda de los propios contenidos se encuentran ampliamente documentadas por un nutrido grupo de investigadores, entre los que debemos citar principalmente a: Sundén, Govani y Pashley, Acquisti y Gross, Barnes, Norberg, Boyd, Young y Quan-Hasse y Tufecki, entre otros. La pervivencia de dicho fenómeno induce a creer que el sujeto no valora, en demasía, la preservación de su esfera privada; o bien, solo se preocupa cuando ya se ha producido alguna injerencia en su ámbito reservado. En otros casos, parece sugerir que los individuos no son del todo conscientes de las posibles implicaciones derivadas de sus actuaciones en la Web 2.0 o que, a pesar de conocer los peligros que entrañan ciertas aplicaciones, no son capaces de evitarlos. Por todo ello, en el *Capítulo VIII* nos serviremos del análisis del citado

---

723 Ídem.

724 GÜRSES, S. y DÍAZ, C. (2013): «Two Tales of Privacy in Online Social Networks», en *IEEE Security and Privacy*, vol.11, n. 3, pp. 29-37, p. 35.

725 Dado que no hemos encontrado estudios en castellano que mencionen el fenómeno y revierte en nosotros la responsabilidad de su traducción, hemos decidido asimilar la voz *privacy* con «vida privada» para evitar el anglicismo. Véase: González Gaitano, N. (1990): *Op. cit.,* p. 16.

fenómeno para arrojar algo de luz sobre las posibilidades reales que detentan los usuarios a la hora de controlar la exposición de los contenidos pertenecientes su esfera privada.

2.1 LA «PARADOJA DE LA VIDA PRIVADA» (*PRIVACY PARADOX*)

Para Petra Ilyes y Carsten Ochs[726], el *leitmotif* de la mencionada contradicción fue formulado en 2003 por Alessandro Acquisti y Jens Grossklags quienes identificaron: «una dicotomía entre las actitudes ya establecidas y el comportamiento real de los individuos cuando debían enfrentar decisiones referentes a su información personal o que afectasen a su vida privada»[727]. Posteriormente, los autores siguieron observando las dinámicas producidas en la interacción entre usuarios y las herramientas de la Web 2.0, especialmente en lo referente al uso de las redes sociales. Así, en 2005, en uno de los primeros estudios sobre las implicaciones de las redes sociales para la vida privada, Gross y Acquisti analizaron los perfiles de Facebook de 4.000 estudiantes inscritos en la Carnegie Mellon University. Ambos autores encontraron que los usuarios estaban continuamente obligados a realizar decisiones racionales[728] para salvaguardar su vida privada. Partiendo de esta premisa, en dicha investigación se comparaban las medidas que los individuos afirmaban tomar para proteger sus datos personales, con la información que *de facto* revelaban sus perfiles sociales. Tras examinar dichos perfiles, los autores describieron los riesgos potenciales para la integridad privada de los participantes de la muestra, derivados de la información propia que ellos mismos habían introducido. Así por ejemplo, fueron capaces de reconstruir sus números de la seguridad social partiendo de datos volcados por los propios sujetos, como la ciudad en la que habitaban o su fecha de nacimiento.

Los hallazgos, de nuevo discordantes, alentaron subsiguientes incursiones dedicadas a desentrañar el por qué de este comportamien-

---

726 ILYES, P. y OCHS, C. (2013): «Sociotechnical Privacy. Mapping the Research landscape», en *Tecnoscienza, Italian Journal of Science & Technology Studies*, n. 4, vol. 2.

727 ACQUISTI, A. y GROSSKLAGS, J. (2003): *Op. cit.,* p. 10.

728 ACQUISTI, A. y GROSSKLAGS, J. (2005): *Op. cit.,* p. 23.

to, estudios que no hicieron sino revalidar la persistencia del fenómeno. En 2006, los investigadores identificaron que los miembros de la plataforma Facebook estaban más preocupados por salvaguardar sus informaciones personales que por otras inquietudes como las relacionadas con el terrorismo o el medioambiente; pero, a pesar de ello y en aparente contradicción, continuaban desplegando una cantidad considerable de datos personales, como sus fechas de nacimiento u orientación sexual, entre otros[729]. Subsiguientemente, autores como Reynolds verificaron que la conducta de los miembros de las redes sociales no coincidía con las preocupaciones previamente declaradas[730]; aunque sería Barnes quien en 2006 bautizara este hallazgo como fenómeno de la «paradoja de la vida privada» *(privacy paradox)*[731] ulteriormente a su observación en otros tantos exámenes.

La idea principal que se contiene bajo la expresión paradoja de la vida privada es que mientras los usuarios de los entornos digitales expresan una amplia preocupación acerca de la posibilidad de que su información personal sea hecha pública, a la vez y en aparente contradicción, continúan construyendo activamente su identidad en dichos entornos mediante el despliegue de considerables cantidades de datos privados. Existe, por lo tanto, un desfase constante entre las inquietudes expresadas por los individuos y su proclividad a exponer sus contenidos de carácter privado.

A este respecto, son cuantiosos los estudios de usuarios que han pretendido identificar cuáles son las variables que influyen en este comportamiento, apoyándose en diversos aspectos como: la confianza que los sujetos asignan a ciertas redes sociales, la percepción de beneficios en forma de capital social por el que merece la pena pagar, el cambio en la concepción en la intimidad y vida privada a lo largo del tiempo, el nivel de percepción de riesgo del individuo o el desarrollo de estrategias defensivas basadas en modelos mentales fallidos. En las próximas páginas, analizaremos detenidamente la evolución y puntos clave en los que recalaron estos trabajos, para intentar definir qué papel desempeña el sujeto en la preservación de su esfera privada.

---

729 ACQUISTI, A. y GROSS, R. (2006): *Op. cit.,* pp. 36-58.
730 REYNOLDS, B. *et al.* (2011): *Op. cit*,. p. 214.
731 BARNES, S. B. (2006): *Op. cit.*

3. EVOLUCIÓN Y ANÁLISIS DEL COMPORTAMIENTO DE LOS USUARIOS A TRAVÉS DE LA PARADOJA DE LA VIDA PRIVADA

Desde que se observan las primeras contradicciones y se describe el fenómeno, hasta el momento actual, la valoración del papel de los individuos respecto a la preservación activa de su intimidad y vida privada ha variado significativamente. Así, los resultados arrojados por los primeros trabajos, centrados en su mayoría en estudiantes universitarios y adolescentes, señalaban que, *a priori,* estos exponían sus datos de manera voluntaria, probablemente, debido a una baja percepción de riesgo. Esta habría sido provocada bien por una absoluta carencia de concienciación y/o conocimiento sobre los peligros de la Web o bien porque no eran capaces de estimar, en su justa medida, el valor de sus propias informaciones.

Con posterioridad, estas conclusiones se matizan recalando en que, aunque los sujetos sí desean proteger sus contenidos de carácter privado, no siempre lo consiguen ya que no poseen herramientas suficientes, no comprenden bajo qué condiciones sus datos se pueden volver accesibles o no interpretan correctamente las dinámicas de flujos de datos de la Web semántica. Son igualmente frecuentes los casos en los que los interactores creen haber protegido sus datos eficazmente mediante el desarrollo de estrategias o la modificación de las configuraciones por defecto, pero ulteriormente descubren que no ha sido así.

Este cambio de perspectiva evoluciona parejo al desarrollo y expansión de las aplicaciones de la Web 2.0, especialmente cuando estas empiezan a atraer a otros rangos de edad y segmentos de la población, y muchas de las consecuencias indeseadas de estas tecnologías relacionales se tornan *vox populi*. Así, resumiendo los hallazgos a los que llegan los estudios de usuario destinados a contrastar y explicar el mencionado fenómeno, podemos indicar tres estadios contenidos en tres proposiciones:

1.º «Los usuarios, en su mayor parte, no valoran la protección de sus informaciones privadas o son muy ingenuos».

2.º «Los usuarios, al menos una parte importante, sí valoran la protección de su informaciones privadas y utilizan estrategias para protegerla».

3.º «Los usuarios, al menos una parte importante, sí valoran sus informaciones privadas y utilizan estrategias para protegerla, pero estas no resultan eficaces».

No obstante, antes de embarcarnos en dicha empresa y transitar estos tres hitos, debemos realizar una aclaración: Si bien es cierto que, a medida que se suceden las investigaciones se abandona mayoritariamente la tesis de que los individuos no se preocupan por mantener a salvo sus informaciones confidenciales, sí debemos admitir que la excepción existe, aunque no relación de causalidad. Es decir, se describen algunos casos en los que los sujetos no mostraron ningún tipo de inquietud respecto a la salvaguarda de su ámbito privado, reflejando una actitud, en cierta medida, ya mostrada en sus interacciones en el mundo físico. En el vértice contrario, no obstante, constatamos que este recorrido resulta interesante por cuanto nos permitirá ver una importante evolución en las destrezas de los usuarios, consiguiendo ampliar su conocimiento a medida que las tecnologías digitales se introducen de manera sustantiva en el quehacer diario. Para guiarnos en el mencionado análisis nos serviremos del siguiente esquema:

Fenómeno de la paradoja de la vida privada

Hipótesis de partida	Indicios	Explicación
– «Los usuarios, al menos una parte importante, no valoran sus informaciones privadas o son muy ingenuos».	– no toman medidas para proteger sus datos personales. – entran en el juego de la exposición. – dejan su personalidad al descubierto.	– equiparan protección de la vida privada a ocultación de la información a ciertos agentes. – equiparan protección de la vida privada a reputación. – poseen una baja o nula percepción de riesgo. – no consideran un valor en sí mismo la salvaguarda de sus contenidos privados, ni le dan importancia a la protección de sus datos personales. – se produce una asimilación de las configuraciones por defecto.
– «Los usuarios, al menos una parte importante, sí valoran sus informaciones privadas y utilizan estrategias para protegerlas».	– cambian las configuraciones por defecto – desarrollan estrategias de autoprotección basadas en modelos mentales – autocensuran sus propias publicaciones	– actúan en relación a posibles intromisiones de otros usuarios. – creen que han preservado correctamente sus contenidos privados mediante las estrategias, la autocensura y los modelos mentales.

Fenómeno de la paradoja de la vida privada		
Hipótesis de partida	**Indicios**	**Explicación**
– «Los usuarios, al menos una parte importante, sí valoran sus informaciones privadas y utilizan estrategias para protegerla, pero estas no son lo suficientemente eficaces».	– se producen los arrepentimientos cuando descubren que ciertos datos pueden ser accesibles – sorpresa al descubrir que las estrategias son limitadas. – intromisiones no deseadas en su intimidad y vida privada – pérdida del control sobre sus propios datos personales – divergencia entre el control que creen tener y los resultados reales.	– discrepancia entre los modelos mentales y estrategias para la protección y el flujo de datos real y de distribución de la información que se da en las plataformas digitales. – los modelos mentales no funcionan porque no están basados en una información clara, ni en la estructura correcta de intercambio de datos que subyace a la red, sino en lo que percibe el usuario. – dificultad para entender los controles de privacidad – dificultad para diferenciar entre espacio público y privado. – dificultad para diferenciar la posible audiencia de sus publicaciones: solo tienen en cuenta las intromisiones procedentes de otros usuarios no de terceras empresas, desarrolladores o la propia plataforma. – asimilación de las opciones por defecto y apropiación de la tecnología. – contagio de comportamientos que alteran la percepción y subsiguiente creación de estrategias.

Tabla 8.1 El comportamiento de los usuarios a través del análisis de la paradoja de la vida privada[732]

3.1 «LOS USUARIOS NO VALORAN SUS INFORMACIONES PRIVADAS O SON MUY INGENUOS»

La emergencia y posterior expansión de las redes sociales aparece ligada, en los primeros años, a una falta de toma de conciencia real por parte de los individuos, quienes no se percatan de que sus datos personales podrán ser accesibles para cualquiera, ni del valor que estos pueden llegar a alcanzar en el mercado. En infinidad de casos, son los propios usuarios los que descuidan la protección de sus perfiles y hacen completamente visibles datos que incluyen características per-

[732] Fuente: elaboración propia.

sonales que serían reacios a exhibir en el espacio público físico, tales como ideología u orientación sexual y religiosa. Así, a finales de 2007, casi la mitad de los miembros de redes sociales observados no aplicaba ningún tipo de restricciones a sus perfiles, cuya información resultaba fácilmente accesible para cualquier persona. En este sentido, según el Grupo Internacional sobre Protección de Datos en las Telecomunicaciones de Berlín, uno de los mayores desafíos que pueden observarse es que «la mayoría de la información que se publica en las redes sociales se hace bajo la iniciativa de los usuarios y basado en su consentimiento» [733].

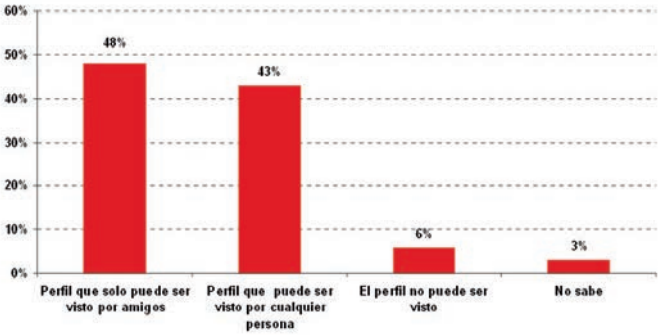

Figura 8.2 Tipo de configuración de perfil aplicado por los usuarios de redes sociales respecto de su visibilidad y nivel de seguridad (octubre-diciembre 2007) [734]

Este es, pues, el escenario primigenio de observaciones, centradas mayoritariamente en los colectivos que más tempranamente se adueñan de las tecnologías digitales, esto es, estudiantes universitarios y adolescentes, segmentos que, por juventud e inexperiencia, resultan altamente vulnerables a pesar de ser más diestros en los entornos tecnológicos. En estos casos, la baja percepción de riesgo que muestran los sujetos se torna en la cara visible del desconocimiento que lastra sus actos, provocando que sean poco cautelosos a la hora de exhibir sus contenidos, bajo la creencia de que si otros lo hacen es porque no existe ningún peligro o bien porque consideran que no tienen nada

---

733 The International Working Group on Data Protection in Telecommunications (2008): *Report and Guidance on Privacy in Social Network Services. «Rome Memorandum»*, aprobado el 4 de marzo de 2008, Roma, Italia.

734 Fuente: AEPD e INTECO (2009): *Op. cit.*, p. 61.

que esconder. El valor de la intimidad y vida privada es un concepto que brilla por su ausencia.

Entre las primeras aproximaciones realizadas a este respecto destacan las anteriormente mencionadas de Acquisti y Gross, llevadas a cabo en 2005 y 2006, los estudios de Stutzman en 2006 y muchos de los trabajos de Boyd realizados entre los años 2007 y 2011, evidenciando, en todos ellos, una amplia discrepancia entre el deseo de protección de los individuos y su conducta real en la red. Igualmente, los resultados parecen señalar la existencia de dos tendencias generales: aquella referida a los individuos que, a pesar de mostrar inquietud por la salvaguarda de sus informaciones personales, continúan alimentando sus redes sociales con una cantidad ingente de datos y la de los que no están realmente concienciados por cuanto no consideran la preservación de la vida privada una necesidad en sí misma. Intentemos ahora desgranar, detalladamente, qué se esconde tras estos primeros hallazgos.

3.1.1 Los usuarios no consideran la protección de su vida privada un valor en sí mismo

Existe un amplio debate acerca de cómo el uso de las redes sociales ha cambiado la percepción de los individuos acerca de lo que es legítimo preservar, así como las acciones que toman para desempeñar dicha protección. En estos recintos del espacio público mediado, los sujetos emplazan a voluntad parte de su información personal con el fin de nutrir sus perfiles y que las redes sean útiles. Pero aun cuando sopesan pormenorizadamente los datos que introducen, deben sacrificar una parte que ellos consideran razonable de su vida privada. A este respecto, estudiosos como Zimmer argumentan que los usuarios de la Web 2.0 mantienen formulaciones particulares sobre lo que es pertinente o no mostrar, esto es, sopesan el valor de sus contenidos privados en función de los contextos. Aunque priman alimentar su círculo social frente al amparo de su espacio reservado, muchos individuos, sabedores del valor de su información personal, comparten solo lo necesario para mantener su red social y alimentan sus diferentes lazos relacionales dentro de este espacio confinado. Esta estrategia les permitiría conectar con toda su red sin ser ni demasiado visibles, ni demasiado reservados.

Dicho comportamiento se articularía a la perfección en el marco teórico de la integridad contextual, según el cual, la pertinencia de los datos de carácter privado debe medirse en relación a su justificación dentro del contexto. Sin embargo, incluso cuando consideramos la noción más contextual de la información privada, el hecho es que los miembros de estas comunidades tienden a compartir una gran abundancia de contenidos en la Web, hecho del que en ocasiones se arrepienten.

¿Qué están dispuestos a compartir?	
Nombre	100%
Imágenes	80%
Amigos	60%
Cumpleaños	60%
Opiniones políticas	36%
Historial laboral	36%

Tabla 8.3 ¿Qué informaciones personales están dispuestos a mostrar los usuarios?[735]

Aunque los sujetos se muestren conscientes de que están sacrificando parte de su información reservada, el hecho de que en las redes sociales formen parte de un espacio público acotado y que en ellas se desarrollen relaciones típicas de la esfera privada hace que, a menudo, sean percibidas como un espacio semipúblico, lo que actúa en detrimento del nivel de alerta del usuario. Dichas actitudes son, por ende, indicios de una percepción distorsionada acerca del valor que los datos privados poseen en sí mismos, dando como consecuencia apreciaciones erróneas entre lo que es razonable mostrar y lo que no. Veamos a continuación una serie de razones que explicarían este fenómeno.

3.1.1.1 *Equiparación entre «vida privada» y «secreto»*

Según las conclusiones obtenidas en algunos de los primeros estudios de Boyd, los adolescentes americanos no consideraban la vida

[735] Fuente propia con datos de: LIPFORD, H. R., *et al.* (2009): «Recovering Reasoning Process From User Interactions», en *Computer Graphics and Applications*, vol. 29, n. 3, pp. 52-51.

privada, en su conjunto, como un valor en sí mismo, sino que solo tenían en cuenta uno de sus aspectos: el referido a «secreto» u «ocultación» de información. La equiparaban, así, a la necesidad de tener un espacio reservado, aunque apartado solo de la audiencia que ellos percibían como peligrosa. En este sentido, los participantes examinados medían la protección que debían otorgar a sus contenidos en relación a condicionantes, como, por ejemplo, la necesidad de mantenerla oculta de sus padres o profesores, así como de las posibles amenazas provenientes de iguales, como aquellas ejercidas por compañeros de instituto. Por ello, usaban las configuraciones de privacidad para que sus progenitores y otras figuras de autoridad no descubrieran qué hacían a sus espaldas, pero no motivados por el deseo real de salvaguardar sus datos. En consecuencia, protegían su información privada de manera selectiva y en función de una determinada audiencia: ciertos actores no debían tener acceso a esta «del mismo modo que no podrían leer su diario privado sin consentimiento» [736]. De esto se deduce que consideraban sus perfiles de redes sociales como ámbitos privados e, incluso, una extensión de su propio dormitorio o sus pensamientos íntimos.

Esta conclusión se asemeja a la ya mencionada en el artículo «Teens Privacy and Online Social Networks» de 2007. Según los autores, Lenhart y Madden: «para los adolescentes no toda la información privada es tratada igual. Para ellos es muy importante entender el contexto en el que será compartida y con quién» [737], subrayando, de nuevo, que no apreciaban explícitamente el resguardo de sus contenidos, sino que intentaban que ciertos actores no tuvieran acceso a ellos. No obstante, esta conducta no les disuadía de seguir introduciendo datos de carácter privado con la intención de alimentar las relaciones establecidas entre su círculo de amistades. Además, en ningún caso consideraban las posibles amenazas procedentes del uso de los datos personales por las propias plataformas o por terceras empresas, es decir, emplazaban sus contenidos en función de su público inmediato o de las personas que ellos creían que verían dichas informaciones. De este modo, la introducción de datos en función de la

---

[736] BOYD, D. y MARWICK, A. (2011): *Op. cit.*
[737] LENHART, A. y MADDEN, M. (2007): *Op. cit.*

integridad contextual del entorno se medía en base a la audiencia percibida como potencialmente peligrosa.

3.1.1.2 *Baja percepción de riesgo*

En muchas ocasiones, los usos de la vida real se han trasladado a las redes sociales, aun cuando las relaciones que se establecen en el mundo físico poco o nada tienen que ver con las interacciones desarrolladas en los entornos digitales. Estas últimas demandan mayor cautela y, tras observar que los usuarios desempeñan una salvaguarda selectiva de contenidos privados en función del público percibido, autores como Gross, Acquisti, Lampe, Ellison, Steinfield, Boyd y Hargittai han convenido en afirmar que el uso de las redes sociales altera la percepción de lo que se considera privado y lo que no.

En este sentido, Zimmer se pregunta si efectivamente las reglas están cambiando en el entorno digital o si, por el contrario, la norma es el exhibicionismo de la información:

> Se ha traducido la popularidad de estas herramientas en unas normas informacionales más amplias —en relación a las normas que imperan en cada contexto y determinan la integridad contextual— ¿Nos sentimos ahora más cómodos con el libre y abierto intercambio de información personal tal y como se describe en la sociedad transparente de David Brin?[738]

En sus trabajos, Zimmer cataloga a los estudiantes universitarios en dos polos en función de la percepción de riesgo que muestran: los que usan las redes sociales y todas sus aplicaciones despreocupadamente, compartiendo infinidad de detalles personales, y aquellos, más tradicionales, que sí valoran su intimidad y vida privada aún cuando no sepan cómo preservarla. Sin bien es cierto que la mayoría de observaciones realizadas durante este periodo coinciden en recalcar la existencia de esta doble tipología, es justo destacar que el exhibicionismo primerizo tiene más de ingenuidad y desconocimiento que de intencionalidad. Por otra parte, según Alyson Leigh Young y Anabel

---

[738] ZIMMER, M. (2007): *Op. cit.,* Zimmer alude aquí al trabajo de David BIRN (1998), *The Transparent Society,* Reading MA: Perseus Books, que versa sobre la erosión del aspecto reservado del ser humano inducido por la sociedad de la vigilancia.

Quan-Haase, la cantidad de información vertida diariamente en las redes sociales es percibida, paradójicamente, como una pantalla de protección, por cuanto muchos sujetos creen que, ante tal maraña de datos, su información no será localizada fácilmente[739].

En cuanto a los individuos que, aparentemente, no mostraban interés por preservar su vida privada, se establecía una relación directamente proporcional entre dicha actitud despreocupada y una percepción de riesgo baja o nula. Como consecuencia, estos son más proclives a entrar en el juego de la exposición continuada de las redes sociales, dejando su identidad virtual, esto es, su persona, al descubierto.

3.1.1.3 *Equiparación entre «vida privada» y «reputación»*

Otro posible escenario es el que apunta a la interpretación de la violación del ámbito privado como una erosión de la propia reputación o del honor. Es decir, los sujetos solo tendrían en cuenta la vulneración de su esfera personal cuando esta puede suponer una brecha en su imagen visible.

Siguiendo esta línea, en un estudio desarrollado en 2010 por Madden y Smith se observó que los participantes analizados controlaban su reputación desetiquetando fotos controvertidas o no favorecedoras, toda vez que borraban comentarios del muro de Facebook que los describían de una manera negativa. En concreto, encontraron que casi el 50% de los usuarios de entre 18 y 29 años habían eliminado publicaciones que otros contactos habían hecho en sus perfiles y las que, aproximadamente un 40% las había desetiquetando su nombre de fotos subidas por amigos[740]. En este sentido, la paradoja de la vida privada responde al hecho de que los individuos solo preservan aquella cantidad de información que creen puede dañar su imagen social, sin contemplar otro tipo de intromisiones. De este modo, dejan una parte importante de sus datos al descubierto con las consiguientes sorpresas cuando descubren que no tienen control sobre sus informaciones o que estas inundan la Red.

Curiosamente, la reputación puede ser también, en sí misma, un factor de riesgo. Los usuarios que priman mayoritariamente su imagen deben mantener vivo su círculo social, nutriéndolo constantemente con infinidad

---

739 YOUNG, A. L. y QUAN-HASSE, A. (2013): *Op. cit.,*
740 MADDEN, M. y SMITH, A. (2010): *Op. cit.*

de contenidos para que siga funcionando. Y, dado que en un amplio número de casos en la batalla entre la salvaguarda de nuestra persona o conseguir más popularidad, esta última arrasa sin contemplaciones, la reputación puede llegar a jugar un papel tan nocivo en la protección como la desinformación. Por otra parte, el control de las opciones de privacidad se relaja a medida que los individuos interactúan con otros y centran su interés en la creación de una determinada presentación pública imbuidos por la urgencia de notoriedad.

Pero además de verificar la existencia de una escasa apreciación de los peligros potenciales, la consideración de la popularidad por encima de la vida privada refleja una cierta ingenuidad o desconocimiento del funcionamiento de los entornos virtuales. En muchos casos, por ejemplo, un número exagerado de «amigos» viene asociado a ese deseo de crear una reputación, esto es, de dar impresión de popularidad; y, sin embargo, esto puede conllevar consecuencias nefastas en lo que a la protección se refiere. Como botón de muestra, rescatemos el experimento realizado por la empresa de seguridad informática *IT Sophos,* en el que la urgencia por ganar contactos a toda costa en la red social Facebook, dejó a muchos usuarios con sus datos a la intemperie.

Para llevar a cabo el ensayo se creó un perfil falso bajo el nombre de Freddi Staur, una pequeña rana verde de plástico que divulgaba el mínimo de información posible sobre sí misma. Con esta carta de presentación, Freddi envió 200 invitaciones aleatorias para tantear cómo respondían los individuos y cuánta información personal era capaz de obtener, y el resultado fue espectacular: 87 personas agregaron a Freddi y compartieron con él datos como sus correos electrónicos (72%) fecha de nacimiento (84%) educación y lugar de trabajo (87%) domicilio o localización (78%) número de teléfono (23%) o alias (26%). En la mayoría de los casos, Freddi fue capaz incluso de conseguir acceso a fotos, familiares y amigos; sin contar con información como gustos, *hobbies* y datos de su lugar de trabajo. Además, numerosos individuos habían introducido el nombre de sus parejas, padres, hermanos y mascotas, datos, estos últimos, que, en aquel entonces, solían solicitarse para verificar la autenticidad de las cuentas y no solo de las redes sociales[741].

---

[741] Es la denominada «pregunta de seguridad» con la que se permitía al individuo autentificar su identidad, en el caso de no poder acceder a su cuenta de correo electrónico u otros servicios.

Consecuentemente, los hallazgos demostraron no solo que, en efecto, es muy fácil obtener información personal de otros usuarios, sino que la mayoría poseía una percepción de riesgo muy baja basada en esa peligrosa mezcla entre desconocimiento y la pretensión de notoriedad.

Bien es cierto que este experimento se llevó a cabo en 2007 y que, probablemente, en la actualidad una rana de plástico verde encontraría más problemas para hacer amigos. No obstante cabe preguntarse: si un perfil con semejante avatar es capaz de hacerse con tamaña cantidad de datos ¿Qué sucede con todos esos contactos, apenas «conocidos», que los sujetos agregan sin miramientos? De nuevo, la necesidad de notoriedad puede jugarnos una mala pasada, especialmente si no somos cautelosos con las opciones de configuración desplegadas.

En resumidas cuentas, las conclusiones obtenidas en estas primeras observaciones revelan que los usuarios primigenios valoraban, en la mayoría de los casos, solo aquella parte de su intimidad y vida privada que aparecía ligada a los conceptos de «secreto» y «reputación», revelando una muy baja valoración del posible riesgo derivado de sus comportamientos. Dichas actitudes además mostraban una cierta ingenuidad y desconocimiento de los entornos en los que operaban.

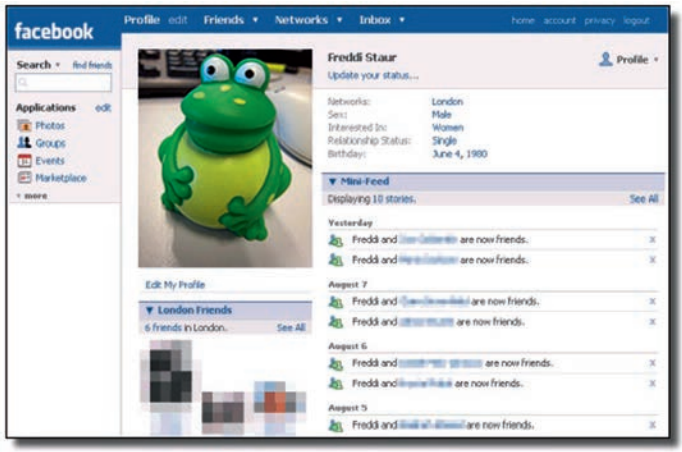

Figura 8.4 Perfil de Freddi Staur[742]

[742] Fuente: Sophos (2007): «Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieve», 14 de agosto de 2007.

3.2 «LOS USUARIOS SÍ VALORAN SUS INFORMACIONES PRIVADAS Y UTILIZAN ESTRATEGIAS PARA PROTEGERLAS»

Esta exhibición voluntaria de lo privado llevó a Stephen Lilley, Andra Gumbus y Frances Grodzinsky a medir la percepción de riesgo de un grupo de estudiantes con perfiles en redes sociales. Los participantes fueron sometidos a un examen cualitativo previo en el que les interrogaban sobre las medidas de protección que habían tomado y si pensaban que sus datos estaban a salvo. Tras el estudio, los autores comparaban las respuestas obtenidas por los miembros de la muestra con la información real que se podía encontrar sobre ellos a través de la red social Facebook, revelando a cada participante la cantidad de datos privados que dejaban al descubierto, ante su consiguiente sorpresa:

> Los chicos y chicas se preocupan por la privacidad, controlando su información personal y su exposición. Sin embargo, por sus reacciones a la controversia sobre el uso de contenido, resulta evidente que no estaba familiarizados con los términos de privacidad de Facebook y no consideraron lo vulnerables que resultaban frente a los administradores de la red[743].

En efecto, a medida que se abandona la ingenuidad que parece acompañar a la adopción de las redes sociales, comienzan a documentarse comportamientos que demuestran que los individuos sí están preocupados por la protección de sus informaciones, aun cuando este canje no se produce en toda la población por igual, ni aparece al mismo ritmo. En este sentido, se puede reconocer cómo ha calado la filosofía Facebook en la sociedad, especialmente en algunos nichos generacionales, entre cuyos usuarios la compañía ha encontrado a los mejores publicistas y defensores de su doctrina del mundo accesible.

Volviendo a las investigaciones, autores como Debatin, Young, Quan-Hasse, Besmer, Lipford, Sleeper, Madden, Smith o Stutzman afirman que existen indicios de que los individuos sí muestran interés en la conservación de su esfera privada por cuanto emplean una amplia gama de estrategias para solventar sus inquietudes. Las prácticas más habitualmente observadas van desde desetiquetar fotos, bloquear

---

[743] LILLEY, S., GUMBUS, A. y GRODZINSKY, F. (2010): *Op. cit.,* p. 278.

peticiones de contacto o configurar las opciones de privacidad, hasta eliminar contenido *a posteriori* para evitar arrepentimientos. Sin embargo, hay una laguna en la literatura acerca de por qué los individuos eligen unas estrategias de protección frente a otras y cómo esas prácticas concretas se utilizan para solventar necesidades específicas de protección.

Dado que estas actitudes se observan una vez que las herramientas relacionales de la Web ya están perfectamente implantadas en la sociedad, todo indica que hay un salto cualitativo entre los individuos con buenas competencias digitales y que, por tanto, pueden entender mejor los entornos digitales y los peligros que estos conllevan, frente a los menos diestros y, potencialmente, más vulnerables. Entre los primeros, las preocupaciones más frecuentemente referidas señalan la enorme capacidad de etiquetar, agregar, buscar, almacenar y reutilizar información como principales desafíos por lo que, en definitiva, no se sienten seguros operando en un entorno con las características de la Web 2.0.

3.2.1 Los usuarios desarrollan estrategias de protección basadas en sus propios modelos mentales

Consiguientemente, los miembros de las redes sociales no son necesariamente *naïve* cuando despliegan tal cantidad de datos personales, sino que toman decisiones racionales en las que sopesan la cantidad de información que deben desplegar para mantener activo su círculo social, toda vez que controlan su *personae* virtual borrando información que pueda dejarles en mal lugar. De hecho, cuando construyen su identidad a través del volcado de información personal, tienden a introducir la cantidad necesaria para alimentar sus lazos sociales sin ser demasiado públicos ni demasiado reservados, dado que perciben las redes sociales como espacios semipúblicos[744]. Esto es, sacrifican una parte que consideran razonable de su vida privada para nutrir las redes y que estas resulten útiles. La literatura sugiere así que los usuarios son activos en la salvaguarda de su vida privada y no actores pasivos como se pensaban en un principio, mostrando

---

[744] BRANDTZAEG, P. B., LÜDERS, M., y SKJETNE, J. H. (2010): *Op. cit.*

una amplia gama de estrategias para manejar su visibilidad, construidas sobre sus propios modelos mentales.

Se señalan dos posibles razones para explicar la evolución observada: la primera indica que, a medida que las personas adoptan más copiosamente las herramientas de la Web 2.0, poseen una visión más contrastada de cómo funciona Internet y, en consecuencia, son más conscientes de los riesgos latentes y de lo fácil que es perder el dominio de los contenidos propios. El segundo motivo aparece enraizado en las experiencias propias de los interactores: Cuando los sujetos sufren una intromisión indeseada en su vida privada o conocen un caso cercano de intrusión, comienzan a ser más precavidos al desplegar y compartir información, modificando, proactivamente, las configuraciones de privacidad. De este modo, cambian sus conductas y alteran la visibilidad de su perfil en respuesta a estas experiencias negativas. En concreto, si han sufrido una mala experiencia en propia persona son más tendentes a modificar las opciones por defecto, que cuando se trata de intrusiones que han experimentado otros. Se desprende así que las personas que más velan por el anonimato de sus informaciones son aquellas que han vivido consecuencias indeseadas. Por el contrario, la falta de concienciación de los sujetos que permanecen ajenos a estas situaciones actúa en detrimento suyo, despreocupación que retroalimenta la desprotección.

En referencia a los interactores más aventajados, Lewis, Kaufman y Christakis identificaron en 2008 los factores que anticipaban la posibilidad de que los usuarios manipulasen su perfil para hacerlo más privado: en primer lugar y debido al citado efecto contagio de las redes descrito por Fowler y Christakis, los individuos cuyos contactos eran más cautelosos con su información y tenían un perfil privado eran más dados a configurar sus opciones de privacidad para que otros no tuvieran acceso a los datos contenidos en sus perfiles. Y en segundo lugar, los miembros más activos resultaban más conocedores de estas configuraciones, por lo que tendían a usarlas más habitualmente, a diferencia de aquellos miembros esporádicos que mostraban mayor visibilidad en sus perfiles. Estos mismos resultados fueron observados por Alyson Leigh y Anabel Quan-Haase al comprobar que, en efecto, las personas que más modificaban las configuraciones por defecto y controlaban el nivel de visibilidad eran las más diestras en el

manejo de las herramientas provistas por la red social[745]. El axioma demostrativo que cabe dilucidar de este hecho es que: «a más uso, entendimiento y conocimiento de las redes sociales, más se activan los controles de privacidad», esto es: «a más conocimiento de este entorno digital, más medidas toma el usuario para preservar sus contenidos privados». En este sentido, Elli Pariser describe como, al igual que sucede con el buscador Google, a través de la modificación de las configuraciones por defecto y de otras prácticas que muestran los individuos, estos son capaces de crear, potencialmente, una «burbuja filtro» (*filter bubble*)[746] que les protege de posibles intromisiones.

Asimismo, dentro del colectivo aparentemente más familiarizado con los entornos digitales, los comportamientos en estos primeros años podían variar de una red a otra en función de la confianza percibida de cada plataforma concreta, así como la satisfacción en el manejo. Los miembros de la comunidad Facebook, por ejemplo, resultaban más dados a compartir contenidos que los de MySpace, toda vez que expresaban mayor confianza en la red de Zuckerberg que estos últimos en la plataforma musical[747].

Demos ahora un paso más para concretar en qué consisten exactamente las tácticas ejecutadas por los usuarios para velar por la seguridad de sus datos.

3.2.1.1 *Estrategias de protección*

Los estudiantes observados en las primeras incursiones emplean una amplia gama de prácticas destinadas a satisfacer distintos niveles de protección. Así, manipulan activamente las configuraciones por defecto para controlar sus datos, alterando no solo la visibilidad, sino el acceso a sus perfiles al restringir la información que es visible a otros miembros. Del mismo modo, muchos individuos efectúan el borrado de datos o comentarios de amigos en el propio perfil, crean listas de contactos o establecen varios niveles de acceso a los contenidos

---

[745] LEWIS, K., KAUFMAN, J. y CHRISTAKIS, N. (2008): «The taste for privacy: an analysis of college student privacy settings in an online social network», en *JCMC*, vol. 14, n. 1, pp. 79-100.

[746] PARISER, E. (2011): *The Filter Bubble: What the Internet Is Hiding from You,* London: Viking.

[747] DWYER, C., HILTZ, S. y PASSERINI, K. (2007): *Op. cit.*

propios. A la vez, usan herramientas privadas de comunicación, como mensajes restringidos, si consideran que el contenido es confidencial, embarazoso o sobreexpone sin tapujos su identidad.

En la misma línea, se observan otro tipo de tácticas basadas en la ofuscación de información (*practical obscurity*)[748] que consisten en mostrar cierto tipo de contenidos más o menos neutrales y, a la vez, ocultar otros más comprometedores. Habitualmente, estos usuarios muestran bastante destreza en el manejo de las herramientas tecnológicas, por lo que utilizan varias redes sociales en función del destinatario de sus publicaciones, bloqueando cierto tipo de público si no se corresponde con la audiencia elegida. De este modo, hacen más difícil el acceso a sus cuentas personales, es decir, aquellas en las que vuelcan más información privada, sin perder por ello los beneficios que les proporcionan estas herramientas sociales. La falsificación de datos también está ampliamente documentada en la literatura como método para proteger la propia identidad,[749] aunque no es la estrategia usada.

Cabe puntualizar, retomando a Elli Pariser, que para muchos sujetos la agregación de datos y el hecho de ser susceptibles de convertirse en público objetivo de la publicidad personalizada se considera como una práctica normalizada en la sociedad, equiparada al precio que es necesario pagar por acceder a esos servicios «gratuitos» [750]. Que esto se haya convertido en una pauta social aceptada, sugiere que los usos referentes a la vida privada y la extracción del significado de los datos personales parecen evolucionar a medida que la gente se comunica mediante redes sociales digitales, algo que enlaza con la concepción de la plasticidad de las normas de comportamiento, anteriormente indicada por Zimmer.

3.2.1.2 *Estrategias de protección frente a otros usuarios*

La expectación de transgresión de la esfera privada a través de iguales se contempla en aquellas personas que solo permiten ver datos

---

748 FREDERIC, S. y WOODROW, H. (2012): «Boundary regulation in social media», en *CSCW '12*, Nueva York: ACM Press: ACM Press, pp. 769-778.

749 GRUBBS, M. y MILNE, G. (2010): «Gender differences in privacy-related measures for young adult Facebook users», en *Journal of Interactive Advertising*, vol. 10, n. 2, pp. 28-45.

750 PARISER, E. (2011): *Op. cit.*

de su perfil a sus contactos. A este tenor, se detallan multitud de casos en los que, nuevamente, son los usuarios que han sufrido intromisiones por parte de desconocidos quienes comienzan a modificar sus configuraciones por defecto de manera activa, para que sus contenidos resulten accesibles solo a sus «amigos». De hecho, una de las mayores inquietudes de los integrantes de las muestras analizadas era ser localizados o molestados por otros miembros del sistema, por lo que intentaban no revelar cierta información a conocidos. Incluso, se detallan casos en las que esta falta de confianza provoca que casi no compartan información. Asimismo, muchos de los sujetos analizados afirmaban «dividir las plataformas», haciendo fragmentaciones entre quién puede ver el contenido y quién no, usando, por ejemplo, de los grupos cerrados de Facebook[751].

Puestas en conjunto, todas estas tácticas verifican que sí existe un interés real en la salvaguarda del ámbito privado, suceso que se torna más palpable a medida que el uso de las tecnologías se expande. No obstante, aun cuando los individuos han hecho un esfuerzo considerable para preservar su espacio reservado, estas actitudes nacen destinadas a protegerse de la intromisión de iguales, esto es, de otros miembros del sistema; pero no tienen en cuenta el uso de sus datos por parte de terceros desarrolladores y otras empresas, algo que además parece no ser percibido. Esto indica que los sujetos no son conscientes de las amenazas provenientes de otros ámbitos y que sus estrategias de protección, basadas en sus modelos mentales, son incompletas por cuanto no contemplan todos los flancos posibles de injerencia.

3.2.1.3 *Estrategias de autocensura*

A medida que avanza el poder de las redes sociales, los usuarios empiezan a ser más conscientes de la amenaza que estas suponen para la integridad de su esfera privada y comienzan a documentarse otro tipo de tácticas. De hecho, cuando la incertidumbre se torna más elevada, se observan casos de autocensura para asegurar no solo le preservación de los propios contenidos, sino los de otros, interactúen o

---

751 LAMPINEN, A., TAMMINEN, S. y OULASVIRTA, A. (2009): «All my people right here, right now»: management of group co-presence on a social networking site», en *GROUP '09*, New York, NY: ACM Press, pp. 281-290.

no en la red. Es lo que denominaremos «estrategias de autocensura» y «estrategias de autocensura responsables».

La autocensura se describe como: «una de las técnicas en las que los usuarios confían para manejar la coexistencia de diversos grupos de contactos en las redes sociales»[752]. De este modo ocultan ciertos contenidos y evitan posteriores arrepentimientos. De hecho, esta estrategia nace como respuesta a una serie de situaciones en las que, a pesar de tener herramientas como controles de privacidad y modificarlos activamente, los sujetos experimentan que la información compartida ha sido vista por una audiencia no deseada.

Dentro de la información censurada, la mayoría de los participantes de los estudios referían contenidos personales para los que no utilizaban las opciones de privacidad, dado que las encontraban «demasiado complicadas de usar y confusas»[753]. Por tanto, a pesar de tener una serie de controles para configurar su visibilidad y la posibilidad de bloquear una parte de la audiencia y compartir así los datos solo con el público elegido, los usuarios prefieren aplicar sus propias tácticas (por ejemplo, no volcar cierta información) antes que fiarse de las opciones proporcionadas por la plataforma. El mero desarrollo de estos efugios indica no solo que la confianza que los sujetos habían depositado en las redes sociales baja en relación inversamente proporcional a su difusión, sino que los individuos no se sienten del todo seguros con las opciones de control que estos espacios proporcionan.

Esta denominada cultura de la autocensura[754] (*self-censorship culture*) deviene de una reflexión previa, que surge en respuesta al malestar que persigue a muchos usuarios cuando descubren que sus contenidos comprometedores han caído en manos equivocadas y cuyas consecuencias van desde el mero arrepentimiento a la pérdida de un trabajo. Coloquialmente hablando, podríamos decir que no es lo mismo criticar a nuestro jefe en un bar, que en la página de Facebook donde queda grabado de por vida; igual que no tiene el mismo alcance que alguien tome una foto nuestra como recuerdo, a que la cuelgue en la Web 2.0 sabiendo que esto va a producir que, al etiquetarnos,

---

752 Ídem.
753 SLEEPER, M., *et al.* (2013): *Op. cit.*, p. 8
754 TEMPLETON, H. (2009): *Op. cit*.

nos identifiquen. Y los ejemplos se mudan más pintorescos en función de lo comprometida que sea la información desplegada. Tempelton recoge la anécdota de un representante de los Estados Unidos que, en febrero de 2009, viajó con una comisión a Iraq y comentó parte del viaje, a modo personal, en su perfil de una red social. Al hacerlo, detalló la ruta seguida no solo por él sino por la comisión entera que, se supone, viajaba en misión secreta[755].

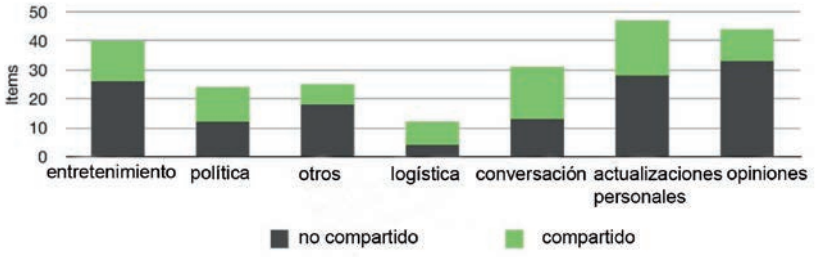

Figura 8.5 Contenido no compartido por los usuarios[756]

Consecuentemente, en la Red no solo debemos considerar la protección de la propia información personal, sino también la de los otros. De este modo, la cultura de la autocensura nace vinculada, particularmente, a las redes sociales, herramientas que han cambiado la ecuación de lo privativo por cuanto los miembros de dichas comunidades se convierten automáticamente en responsables no solo de su propia información personal, sino de la de aquellos con los que, de algún modo, se relacionan. Surgen así las denominadas «estrategias de autocensura responsables».

Para el usuario medio, dichas maniobras constituyen una buena medida defensiva, especialmente en lo que respecta a los contenidos audiovisuales publicados por otros. No en vano, cuando alguien introduce una foto de una fiesta celebrada en un espacio privado, las personas que participaban en ella pasan de ser anónimas a estar catalogadas en el espacio público mediado. Y mientras que aquellos que toman las imágenes pueden mantener su identidad protegida, no ocurre así con los protagonistas de la foto, por lo que la simple acción de

---

[755] Ídem.

[756] Fuente: SLEEPER, M., *et al.* (2013): *Op. cit.*, p. 8.

no aplicarles una etiqueta identificativa puede evitarles consecuencias negativas. El hecho de que muchos usuarios lleven a cabo este tipo de prácticas ya indica, en sí mismo, una cierta reserva en lo que el despliegue de contenidos privados se refiere; un indicio de sus inquietudes respecto a la posible pérdida de control de sus informaciones.

3.3 «LOS USUARIOS SÍ VALORAN SUS INFORMACIONES PRIVADAS Y DESARROLLAN ESTRATEGIAS, PERO ESTAS NO SON LO SUFICIENTEMENTE EFICACES»

Los estudios reseñados anteriormente revelan que los sujetos sí poseen inquietudes respecto a la salvaguarda de su esfera reservada, interés que se acrecienta a medida que las herramientas de la Web 2.0 aparecen más imbricadas en el tejido social. Como hemos reseñado, manipulan los controles por defecto, realizan determinadas prácticas e incluso desarrollan estrategias de autocensura, es decir, en mayor o menor medida, desempeñan un papel activo. Y esto, en principio, les permitiría introducir la cantidad de datos que desean a la vez que se sienten seguros sabiendo que ostentan el control. Sin embargo, estas tácticas no siempre resultan efectivas, llevando al usuario desde el arrepentimiento breve a otras intromisiones más graves, habitualmente reseñadas tanto en trabajos científicos, como en medios de comunicación. En este sentido, en los últimos años han proliferado multitud de investigaciones que evalúan la eficacia de dichas estrategias, a la vez que comparan las decisiones que los sujetos afirman haber tomado, con la cantidad de datos personales que, de manera efectiva, introducen en sus perfiles. Examinan, en definitiva, sus modelos mentales.

Para observar detenidamente el papel que dichas abstracciones especulativas ejercen a la hora de decidir cómo preservar de manera proactiva nuestra integridad privada, nada mejor que detenernos en un ensayo destinado a documentar las percepciones de los miembros de una red social y en el que pudimos tomar parte durante la elaboración de la presente tesis. Nos referimos a DIPO, proyecto que detallaremos a continuación y que fue elaborado entre el Instituto Fraunhofer para la Seguridad de la Información (Fraunhofer-Institut für Sichere Informationstechnologie, SIT) sito en Darmstadt, en conjunto con la Universidad Goethe, Frankfurt am Main.

3.3.1 Los modelos mentales y la falta de conocimiento: ejemplo de estudio sobre usuarios DIPO

El punto de partida del proyecto *Software Design for Interactional Privacy within Online Social Networks (DIPO)* era la necesidad de conocer mejor el comportamiento de los individuos en entornos mediados para desarrollar así herramientas efectivas y sencillas capaces de ayudarlos a salvaguardar sus contenidos personales. De este modo, serían capaces de llevar a cabo sus deseos de «vida privada interaccional», lo que Andreas Poller, uno de los investigadores principales del proyecto, define como: «la protección de la esfera privada de los usuarios en escenarios digitales sin perjuicio para la interacción con otros»[757].

Durante cinco años, el estudio se propuso crear nuevos métodos de recogida y evaluación de información sobre los hábitos de los miembros de las redes sociales, centrándose originalmente en Facebook. (Posteriormente, al constatar la eficacia de la técnica aplicada, se usó la misma aproximación para abordar la relación entre las interacciones de los individuos y la visibilidad de sus informaciones privadas en Google). El proyecto partió de una nueva perspectiva en la que se combinaron dos técnicas: el análisis cualitativo y la recogida de registros mediante un *software* analítico. Dicho programa, denominado *Research Tool for Online Social Environments (ROSE)*[758] documentaba, con el consentimiento de los participantes, las acciones que estos llevaban a cabo en la red social. Los registros obtenidos se ceñían a datos de carácter técnico, por lo que no se grababan los contenidos de dichas acciones para evitar injerencias en su ámbito privado.

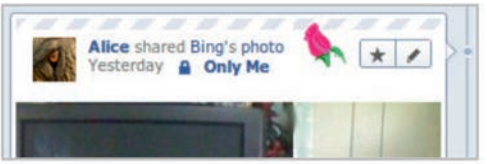

Figura 8.6 Icono del programa ROSE en el interfaz de Facebook[759]

---

[757] Andreas Poller, investigador en el Fraunhofer Institute for Secure Information Technology SIT. Entrevista realizada en el citado instituto, en Darmstadt, en mayo de 2013.

[758] https://dipo.sit.fraunhofer.de/rose-2-is-coming/

[759] POLLER, A.; ILYES, P. y KRAMM, A. (2013): *Op. cit.*

Esta metodología combinada aporta dos ventajas principales frente a otro tipo de aproximaciones: En primer lugar, los resultados no se encuentran condicionados. El *software* se instala en la computadora de cada miembro de la muestra y no en un servidor externo, «para asegurar que no se influye en el comportamiento del usuario, tal y como sucedería, por ejemplo, si un participante del estudio siente que está siendo controlado por el programa»[760]. Para ello, aclara Poller: «el programa está intencionalmente diseñado para dar a los participantes un control total sobre sus datos»[761]; se ejecuta un *pluging* en el buscador, pero la recolección de información solo tiene lugar en el ordenador del participante.

Del mismo modo, los datos no se transmiten automáticamente, sino que son los sujetos los que deben enviarlos a los investigadores. Y dado que el contenido no se conoce, pues solo se capturan las funciones técnicas (eventos como los «me gusta», comentarios, mensajes del *chat* o contenido compartido) el programa incorpora de *facto* la denominada «protección desde el diseño» (*privacy by design*) de la que hablaremos más adelante. Por último, al adaptarse a todas las versiones y cambios en la plataforma Facebook, el sujeto puede seguir adelante con sus actividades normales, sin tener que realizar engorrosas actualizaciones que condicionarían el fluir normal de los acontecimientos a analizar.

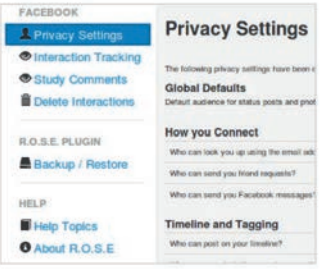

Figura 8.6 bis Controles de usuario[762]

---

760 Poller, entrevista realizada en el Instituto Fraunhofer para la Seguridad de la Información (SIT).

761 Ídem.

762 Fuente: POLLER, A.; ILYES, P.; KOCKSCH, L. y KRAMM, A. (2014): «Investigating OSN Users' Privacy Strategies with ROSE- A Research Tool for

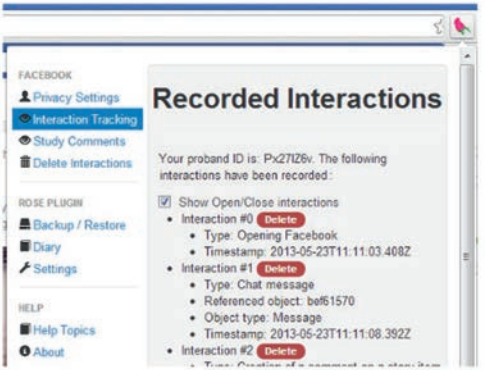

Figura 8.7. Interacciones registradas[763]

Si además durante el uso de Facebook los participantes necesitan aportar algún comentario sobre sus experiencias, el programa contiene una funcionalidad que permite enviar sus impresiones. En este sentido, la segunda ventaja que aporta la yuxtaposición de estos dos métodos es que permiten observar la problemática desde los ojos de los individuos, «al interpretar las distintas aplicaciones técnicas desde su perspectiva» [764].

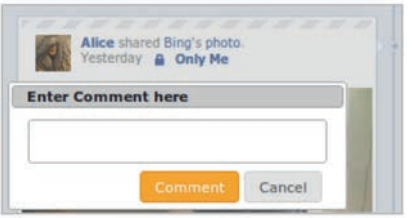

Figura 8.8. Pestaña envío de comentarios[765]

En un primer estadio del proyecto se marcó como objetivo la recopilación de información directa e indirectamente sobre el comportamiento de los individuos. En este sentido, se realizaban entrevistas en

---

Online Social Environments». *CSCW'14*, Poster, Companion, Baltimore, 2014.

763 Fuente: Ídem.

764 Poller, entrevista realizada en SIT.

765 POLLER, A.; ILYES, P. y KRAMM, A. (2013): *Op. cit.*

profundidad a los miembros de la muestra, anotando todas y cada una de las acciones que los sujetos declaraban realizar; a la vez que el programa informático recogía las interacciones que, efectivamente, llevaban a cabo. De este modo, además de evaluar las medidas ejecutadas y la conducta general de los individuos respecto a la protección de su vida privada en Facebook[766], se valoraba el manejo y la eficacia de las herramientas provistas por la plataforma para gestionar la visibilidad de la información.

En una segunda fase se comparaban los registros recogidos por el programa informático con las respuestas ofrecidas por los participantes. Los resultados señalaban disparidades entre el nivel de confidencialidad que presuponían estos y la visibilidad real de sus datos, revelando dos conclusiones: que las medidas tomadas por los sujetos para salvaguardar sus contenidos no resultaban tan efectivas como ellos creían y, en consecuencia, que no contaban con la información suficiente, ni entendían en qué momentos la confidencialidad de sus datos podía ser contravenida. Los hallazgos del estudio verificaron, por tanto, la persistencia de la mencionada paradoja de la vida privada, achacándola no ya al desinterés de la población analizada como sucedía en las primeras observaciones, sino a la dificultad para entender las dinámicas de flujos de datos de esos entornos mediados que son las redes sociales. Esta dificultad se une al total desconocimiento de dicha situación por cuanto, incluso los participantes con mayor nivel de competencias digitales se mostraban confusos y no entendían cómo, ni por qué, sus datos eran accesibles.

Esta misma reacción fue observada en los participantes de otras investigaciones similares. Heather Lipford, de la universidad de Carolina del Norte, averiguó, mediante un programa de simulación, que los usuarios sabían muy poco sobre lo que compartían en redes sociales, razón por la que en ocasiones ni siquiera modificaban los controles por defecto[767]. Cuando estos eran interrogados, afirmaban que habían tomado medidas para que sus datos resultasen inaccesibles por terceros; sin embargo, los hallazgos revelaron no solo que no

---

[766] Proyecto: Privatsphärenschutz in Online Social Networks / Estudio de la protección de la esfera privada en redes sociales. para más información: https://www.sit.fraunhofer.de/

[767] LIPFORD, H. R., *et al.* (2009): *Op. cit.*

eran plenamente conscientes de lo que sucedía en la red social, sino que estaban bastante confundidos. En un alto número de casos, los participantes habían olvidado las configuraciones de privacidad previamente establecidas por ellos. Y, cuando se les revelaba que sus datos resultaban visibles para otros miembros del sistema, se mostraban estupefactos; especialmente, al descubrir que otros actores que no habían tenido en consideración, como son las aplicaciones de terceras empresas, también habían tenido acceso.

No obstante, el acierto más notable de este ensayo es que los autores consiguieron revertir la situación introduciendo más información para asesorar la toma de decisiones. Bajo estas condiciones, los participantes variaban notablemente su comportamiento, suministrando menos contenidos privados y más apropiados al contexto. De este modo, consiguieron establecer una relación directa entre lo que percibían los usuarios y la cantidad de datos privados desplegados por ellos.

Por su parte, otras investigaciones como la de Young, Gurzick y Quan-Haase, documentaron la misma dinámica:

> Durante las entrevistas, se realizó el análisis de perfiles que consistía en pedir a los participantes que entrasen en Facebook y comentasen la información revelada en sus perfiles así como las estrategias de protección que habían empleado. Esto permitió a los participantes elaborar y ampliar la información ya proporcionada en las entrevistas. El análisis de perfiles mostró que los estudiantes no eran a menudo conscientes o habían olvidado qué información habían desplegado y qué opciones de privacidad habían activado [768].

Todo ello refleja la dificultad que tienen los individuos para crearse modelos mentales acordes a la mecánica de funcionamiento de las redes sociales, derivando este fenómeno en los consiguientes errores de cálculo a la hora de emprender estrategias proactivas de protección.

---

[768] YOUNG, A. L., *et al.* (2011): «Online multi-contextual analysis: (re)connecting the social network site user with their profile», in B. K. Daniel (ed.): *Handbook of Research on Methods and Techniques for Studying Virtual Communities: Paradigms and Phenomena*, Hershey, PA: IGI Global, pp. 542-554.

3.3.2 Las estrategias fallan porque los modelos mentales de usuarios no reflejan correctamente el flujo de datos de la Web

Cuando comparamos las medidas que los participantes de los estudios declaran haber tomado, con las acciones que efectivamente han ejecutado, observamos no solo una discrepancia que bien podrían explicar la paradoja de la vida privada, sino que avistamos un vacío en cuanto a percepción y cognición que se plasma en que los individuos no saben qué contenidos han preservado y cuáles no. La razón de este desfase se explicaría porque las personas tienden a crear sus estrategias en función de sus modelos mentales y estos, a su vez, aparecen condicionados por el lienzo visible del interfaz de las redes, percepción simplificada que no representa, ni mucho menos, toda la dinámica que en ellas tiene lugar. Así, las actuaciones de los sujetos analizados erraban al no tener en cuenta los flujos de información que subyacen a la Red, ni entender las condiciones en que se produce el intercambio de datos.

Esto indica que, si bien al menos una parte importante de los usuarios sí valoran su vida privada y utilizan tácticas para manipular la accesibilidad de sus contenidos, ciertas características de las redes sociales, inherentes a la Web semántica, así como el hecho de que el trasvase de datos que se da en ellas no sea visible, constituyen factores que aumentan los errores de apreciación. Para clarificar este punto, a continuación mencionaremos algunos aspectos que propician fallos en la creación de los modelos mentales de los usuarios.

3.3.2.1 *Apropiación de la tecnología y dificultad para diferenciar entre espacio público y privado*

Que las nuevas comunicaciones mediadas, bien sean estas sociales o personales, se desarrollen en infinitud de ocasiones en el interior de nuestros hogares o en momentos de retiro, propicia una mezcolanza de espacios en la que intimidad y vida privada de un lado y esfera pública y profesional de otro, se alternan a un mismo tiempo y en un mismo canal. Nuestras interacciones digitales se desarrollan en un amasijo de escenarios muy diversos, que hacen su aparición de manera yuxtapuesta e independientemente de su naturaleza, y esta característica novedosa de las comunicaciones mediadas que propicia escenarios ambivalentes, hace posible que el espacio en el que se ubica el

sujeto no siempre comparta características similares al entorno donde se desarrolla la comunicación. Esta capacidad de las tecnologías digitales nos permite, por ejemplo, realizar transacciones públicas en el más reservado de los recintos y, en este sentido, no habría diferencias notables con otras tecnologías de comunicación precedentes como es el teléfono. No obstante, la diferencia recala en que nos encontramos ante una amalgama de planos distintos de exposición y visibilidad alternante y canalizada a través de un mismo dispositivo electrónico, lo que se presenta como un terreno propicio para los errores de percepción por diversos motivos: En primer lugar, porque al carecer de especialidad, los seres humanos tienden a realizar inferencias entre el entorno digital en el que operan y el espacio físico que les rodea en ese momento, entendiendo los ordenadores y dispositivos móviles no solo como una parte constituyente de este, sino, por extensión, las páginas a las que acceden, aun cuando este espacio no les pertenezca, ni esté contenido en su recinto. Íntimamente ligado a este punto, se puede perfilar otra equiparación: la de las herramientas de la Web 2.0 a momentos de ocio, puesto que el uso de estas se enlaza habitualmente a situaciones de relax y al abrigo de una cierta intimidad. En ambos casos, se evidencia como, de algún modo, la realidad tangible engulle a lo virtual, evitando el conflicto y la sensación de incertidumbre que resultan tan complejos de gestionar para el cerebro humano, más dado a actuar con representaciones analógicas que con abstracciones. Esta doble asimilación provoca que muchos usuarios no se percaten de que sus datos pueden volverse visibles cuando interactúan en el espacio digital, bajando considerablemente la guardia y olvidando, por tanto, muchas de las estrategias de autoprotección.

Así pues, la falta de materialidad del universo digital provoca que el espacio físico que rodea al digital donde se produce el intercambio de informaciones influya decisivamente en el diseño de los modelos mentales. Empero, no es el único factor que torna complicado distinguir la naturaleza del medio en que navegamos, sino que las propias herramientas sociales se encargan de alimentar estos errores de percepción. En este sentido, basta citar un ejemplo: es muy probable que si le preguntamos a alguien sobre su perfil en una red social responda que este un espacio privado. Y es algo totalmente lógico. A diferencia de las aplicaciones anteriores a la Web 2.0, las nuevas herramientas relacionales explicitan no solo la red del usuario, sino su propia personalidad. Quiénes somos, quiénes son nuestros contactos o, por

omisión, quiénes no, son representaciones siempre presentes en el interfaz de Facebook, una página que, recordemos, «te ayuda a comunicarte y compartir la vida con las personas que conoces». Y, dado que esta parte del espacio público se presenta acotada y en ella se desarrollan relaciones típicas de la esfera privada, los usuarios acaban percibiendo las redes sociales como un espacio reservado o semipúblico que les es propio y que, por tanto, controlan a su antojo. No obstante, ni nuestro muro de Facebook es la pared de las fotografías del pasillo de nuestra casa, ni podemos actuar en MySpace como lo haríamos en la soledad de nuestra habitación.

Todo ello fomenta una cognición distorsionada, hecho ampliamente sustentado por toda la parafernalia que rodea al acto comunicativo, ya que no solo las tecnologías permiten personalizar al máximo las comunicaciones, sino que el propio ordenador se presenta, cada vez más, como un apéndice de nuestro cuerpo recubierto con diseños acordes a la forma de ser de cada cual; al tiempo que las relaciones tradicionales se han ido perdiendo la esencia humana. No está de más señalar, que esta extensión de nosotros mismos y que creemos controlar está gestionada en realidad por agentes externos que consiguen que el usuario se olvide de la mediación e interiorice los nuevos usos digitales.

En consecuencia, las redes sociales no solo se perciben como un espacio privado, sino que fomentan una identificación y apropiación tal, que es capaz de crear la ilusión de propiedad, idea que aparece siempre tan ligada a la de esfera privada. Baste un ejemplo: cada vez que Facebook renueva su aspecto, miles de usuarios abren páginas del tipo *Queremos que vuelva el viejo diseño de Facebook*, dado que sienten melancolía de «su» vieja página en la red social. Esta apropiación de una herramienta controlada por un ente exógeno induce a la creación de modelos mentales erróneos, por cuanto el control que presupone el usuario, en realidad, no existe.

3.3.2.2 *La relación hábitos y tecnología: la asimilación de las configuraciones por defecto*

La apropiación anteriormente citada posee otra lectura negativa: la asimilación de las opciones por defecto. A pesar de que los estudios de comportamiento demuestran que los usuarios desempeñan tácticas para preservar de manera activa sus contenidos privados y, entre

estas, detallan el uso de las configuraciones de privacidad proporcionadas por las plataformas, a la larga estas conductas parecen relajarse. Consecuentemente, una de las posibles explicaciones a la permanencia de la paradoja de la vida privada deviene del hecho de que los usuarios tienden a asimilar las configuraciones predeterminadas, adaptándose a ellas e, incluso, olvidándose de que están disponibles. Y cuando las opciones predefinidas cambian, surge el dilema.

Existe, por tanto, una articulación entre tecnologías y hábitos, hecho que Eva Aladro aborda retomando las reflexiones de Alva Noë: «cuando la mente humana automatiza una conducta, disminuye la consciencia de ella para favorecer la acción inmediata. Nuestra consciencia automatiza imágenes y conductas y les concede tal autonomía que llegamos a considerarlas ajenas a nosotros» [769].

Este «saber pericial», en palabras del propio Noë, supone «prescindir de la consciencia de las reglas, normas o elementos constituyentes, es más amplio que el pensamiento y usa la economía y la relajación» [770]. Y una vez que se han interiorizado, desprogramar esas acciones automáticas resulta complicado, algo que plataformas como las redes sociales comprueban cada día en sus millones de usuarios.

A este respecto, resulta interesante mencionar cómo las estructuras digitales que soportan la vida del ser humano han mutado nuestro comportamiento social, así como nuestros usos y costumbres. Una transformación recíproca, en la que tecnologías y personas se influyen mutuamente, hecho que nos impele a revisar los dictámenes de las teorías coevolutivas.

3.3.2.3 *Dificultad para diferenciar la posible audiencia de nuestras informaciones*

La abstracción que envuelve la comunicación asíncrona de las herramientas sociales digitales alimenta el hecho de que exista un diferencial no percibido entre la audiencia contemplada por los usuarios

---

[769] NOË, A. (2010): *Fuera de la cabeza,* Barcelona: Kairós, p.145. Citado en Aladro Vico, E. (2012): «Cultura y distribuciones humanas», en *Estudios sobre el mensaje periodístico,* vol. 18, número especial, octubre de 2012, pp. 35-43, p. 35.

[770] Íbíd., p. 36.

y la que, en efecto, verá sus informaciones. Los individuos tienden a infravalorar, significativamente, la magnitud que sus actuaciones pueden alcanzar en la Red, creándose esquemas sobre cómo podrá ser distribuida su información, pero sin tener en cuenta todos los factores de la ecuación.

A este tenor, una de las conclusiones señaladas por los estudios anteriormente citados señala que los participantes -en este caso concreto, estudiantes- tienden a ver la audiencia en términos de varios grupos de semejantes y no consideran las intrusiones provenientes ni de otros usuarios ajenos, ni mucho menos de los administradores del sistema y/o terceras empresas asociadas. Así, retomando la distinción enunciada por Raynes-Goldie entre «vida privada social» (*social privacy*) concebida como: «la preocupación por evitar el acceso de otros individuos a nuestros datos personales» y «vida privada institucional» (*institutional privacy*): «la preocupación de que empresas ajenas usen nuestros datos personales», esta última no es ni tan siquiera considerada por los individuos[771]. Es más, habitualmente, son poco conscientes de la cantidad de datos recopilados por las plataformas de Internet, por lo que sus estrategias no actúan en esta dirección.

Es coherente certificar, por tanto, que los miembros de las redes sociales no son conscientes de las amenazas provenientes de otros ámbitos y que sus estrategias de protección son incompletas por cuanto dejan una parte de su vida privada al descubierto, dado que no contemplan un posible flanco de injerencias. Y lo mismo que se observa en los estudiantes, se reproduce en otros rangos de edad: crean sus estrategias sobre la audiencia a la que quieren destinar sus publicaciones y manipulan activamente la accesibilidad de estos contenidos, pero sus modelos mentales fallan al no tener en cuenta este tipo de intromisiones.

Una primera lectura de este hecho nos induce a creer que, puesto que los usuarios desconocen cómo funcionan los flujos de datos en la Web 2.0, bien no perciben las intromisiones o bien no las consideran en absoluto peligrosas. En términos del interaccionismo simbólico de Blumer, esto es, «de acción y reacción», el hecho de que los individuos realicen un menor número de interacciones con estos agentes provoca

---

[771] RAYNES-GOLDIE, K. (2010): «Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook», en *First Monday*, vol. 15, n. 1.

que estén poco pendientes de sus posibles actuaciones[772]. Esto crearía puntos ciegos en las medidas de protección tomadas por los sujetos, especialmente si tenemos en cuenta que en servicios como las redes sociales la sustracción de información personal por terceras empresas que permanecen ocultas va más allá de los límites de la plataforma.

Otra posible respuesta es la que señala que estos agentes no son contemplados como peligrosos. En el caso de las plataformas, los usuarios parecen atribuirles el *role* de árbitros del sistema, por lo que consideran que en ningún caso actuarían en detrimento suyo. Y en lo que respecta terceras empresas y plataformas de desarrolladores, pueden llegar a pensar que merece la pena pagar con algunas informaciones privadas en pro del beneficio adquirido. En cualquier caso, dado que en ambos escenarios no se contemplan los posibles daños derivados de la actuación de estos agentes, los modelos de protección desarrollados por los sujetos resultan sesgados desde el inicio.

3.3.2.4 *La viralidad, el efecto contagio y la percepción de riesgo*

Otra explicación factible de la paradoja de la vida privada tendría que ver con el efecto contagio que se produce en las redes sociales. La percepción de lo que es aconsejable revelar varía mucho de un individuo a otro y no solo en función de la edad, destrezas tecnológicas o experiencias del usuario, sino también de cómo se comportan sus contactos. En este sentido, la «viralidad» que caracteriza a las herramientas de la Web social provoca que los modelos mentales de los sujetos se transformen, influidos por las actitudes de aquellos contactos con los más interactúan. Un contagio que, a diferencia de lo que ocurre en el mundo tangible, provoca que personas que no se conocen de nada puedan condicionarse mutuamente, dado que este fenómeno llega hasta el tercer grado. Y los miembros de las redes sociales raramente reflexionan sobre ello, de la misma manera que, en el mundo real, raramente el individuo tiene momentos para cavilar o modificar sus actos.

Como consecuencia de este cambio de régimen experiencial, copiamos los comportamientos de otras personas de forma casi gregaria y la inercia resultante propicia que esa imitación incluya también

---

[772] BLUMER, H. (1986): *Symbolic Interactionism: Perspectives and Method*, Berkeley: University California.

conductas despreocupadas, aunque estas contradigan nuestro ideario original. De este modo, las tácticas acometidas por los individuos pueden relajarse si la mayor parte de sus contactos han desarrollado estrategias de protección más laxas. Y estas conductas pueden contagiarse de manera instintiva, pero también conscientemente bajo el axioma demostrativo: «si otros se exhiben y no les ha pasado nada, yo también puedo exponer mi vida privada sin problema».

Instintivamente, la falta de concienciación de nuestra red cercana puede generar una sensación de seguridad errónea alimentada incluso por diversos sentimientos, dado que el efecto contagio es tan poderoso que es capaz de alterar el estado anímico de la persona. De hecho, en un estudio realizado en marzo de 2014 y suscrito por autores afiliados a Facebook, se afirmaban que la plataforma había experimentado con 689.003 miembros para identificar la prevalencia del: «efecto contagio emocional»[773]. En el ensayo, desarrollado entre 2011 y 2012, se alteraba la cantidad de contenido emotivo que aparecía en la sección de noticias, sin que los usuarios fueran avisados explícitamente de ello. Implicaciones éticas aparte, sí se pudo constatar cómo los individuos mostraban un estado de ánimo en consonancia con las sensaciones que percibían de su red cercana, modificando sus actuaciones al respecto.

Factores, en definitiva, todos ellos que alteran nuestra percepción de riesgo y, por extensión, la base sobre la que construimos nuestros modelos mentales, lo que explicaría por qué los sujetos toman decisiones erradas o que contradicen sus propios deseos. Y aunque este efecto tendría una parte positiva, en tanto que pueden contagiarse igualmente los buenos hábitos sobre protección, este extremo no parece darse frecuentemente, dado que dicha actitud necesita de un mayor esfuerzo por parte del individuo.

3.3.2.5 *Los usuarios no entienden los controles de privacidad*

Hemos visto como muchos de los problemas para la protección de la vida privada están íntimamente ligados a la tendencia de las redes

---

[773] KRAMER, A. D., GUILLORY, J. E., y HANCOCK, J. T. (2014): «Experimental evidence of massive-scale emotional contagion through social networks» en *PNAS*, vol. 111, n. 24, p. 8788-8790.

sociales de alimentar errores en la percepción de riesgo. Los usuarios se sienten confusos ante la audiencia a la que destinan sus publicaciones por lo que desarrollan estrategias, autocensuran informaciones e intentan adaptar sus contenidos en función del grupo al que va dirigido. Sin embargo, no siempre confían en las herramientas que ofrecen las redes sociales para crear diversos grupos de audiencia; es más, en muchas ocasiones, ni siquiera intentan crearlos previamente. Siguiendo esta tónica, tienden a no leer las advertencias, ni los diálogos de seguridad y cuando deciden hacerlo, dado que estos están escritos en un lenguaje engañoso, no comprenden el alcance las advertencias. En consecuencia, los sujetos prefieren crear sus propias tácticas, ya que encuentran problemas para entender las configuraciones de privacidad, por lo que no suelen examinarlas una vez que ya están establecidas. Igualmente, no entienden los flujos de intercambios de información que se dan en las redes sociales, toda vez que estos no son visibles o están ocultos de manera intencionada. De este modo, no comprenden el alcance de las advertencias, lo que incide significativamente en la toma de decisiones que realizan al introducir sus datos.

En definitiva y conjugando todos los factores analizados, parece existir una clara desconexión entre el funcionamiento de las redes sociales y lo que los usuarios perciben, origen de todos los problemas referidos a la dificultad para conciliar la salvaguarda de la esfera privada con el uso de las tecnologías digitales. En suma, a pesar de que los modelos mentales surgen para satisfacer las expectativas personales de los individuos, estos no alcanzan los niveles de protección deseados, hecho que, en un número elevado de casos, parece estar en el epicentro de la nombrada paradoja de la vida privada.

4. REFLEXIONES SOBRE EL CAPÍTULO

Que el usuario juega un papel primordial en la salvaguarda de sus informaciones privadas es un hecho indiscutible. A este respecto, dos parecen ser las claves capaces de motivar una actuación más o menos sensata al respecto: una percepción no desvirtuada de lo que ocurre en la red y un correcto manejo y entendimiento de las tecnologías y entornos digitales. Abandonada la idea de que las intromisiones en la intimidad y vida privada se deben exclusivamente a las acciones despreocupadas de los sujetos y su bajo nivel de cautela, cabe pre-

guntarse si estos se hallan en disposición de alcanzar los niveles de protección deseados con las herramientas proporcionadas por las plataformas y con la información de que disponen.

Y en este trance, el estudio del comportamiento de los usuarios a través del análisis de la paradoja de la vida privada revela que, a pesar de que las plataformas intentan responsabilizar a los individuos de sus actos en las redes, estos no siempre entienden la mecánica de su funcionamiento, ni ostentan el control sobre sus datos. Así, hemos dado cuenta de cómo incluso los sujetos más aventajados tienen problemas para preservar contenidos inicialmente destinados a una audiencia finita y que, a la postre, acababan siendo fácilmente accesibles para el usuario universal. Y es esta imposibilidad de ejecutar sus pretensiones de protección de manera activa y consciente lo que vulnera su autodeterminación informativa.

Todo ello, nos lleva a pensar que existe un factor condicionante que propicia esta dinámica, por cuanto se repite a escala cada vez que se realiza una medición en diversas muestras. Asimismo, este hecho, sumado a los hallazgos relatados en capítulos anteriores, apunta a que el epicentro se encuentra en la desinformación que lastra el quehacer del sujeto, una situación de la que las plataformas sacan provecho, fundamentando que las inquietudes por defender la esfera privada sean lugar común de la generalidad de navegantes de la Red.

Por otra parte, el que los individuos no sean capaces de interpretar correctamente los flujos de datos que se dan bajo la estructura de la Web 2.0, nos incita a preguntarnos cómo interpretarán la integridad contextual de los escenarios digitales, algo necesario para decidir qué datos personales introducir en cada contexto pero cuya correcta ejecución no parece garantizada en condiciones de desconocimiento. De este interrogante, crucial en la empresa que nos ocupa, daremos cuenta en el siguiente capítulo.

PARTE IV

DISCUSIÓN Y ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

CAPÍTULO IX. COMPROBACIÓN DE LAS HIPÓTESIS DE PARTIDA

SÍNTESIS

Mediante el análisis realizado en los capítulos precedentes, hemos constatado cómo el escenario dibujado por las redes sociales genera una coyuntura perfecta para la emergencia y prevalencia de multitud de conflictos referidos a la protección de la intimidad y vida privada. De hecho, estas herramientas relacionales no parecen diseñadas para que la salvaguarda de los datos privados constituya una prioridad, erosionando el poder de autodeterminación de los usuarios que no controlan, en un alto número de ocasiones, las gestiones que se llevan a cabo con sus contenidos reservados. Por todo ello, retornaremos a las hipótesis que motivaron la presente investigación, para debatir y esclarecer si estos problemas son inherentes a la naturaleza de las aplicaciones sociales y a la Web semántica, qué papel juega el nivel de conocimiento del interactor y, si bajo estas condiciones, está en disposición de aplicar fielmente las leyes de Nissenbaum que velan por el respeto a la integridad contextual.

1. INTRODUCCIÓN: EL RESPETO DE LA INTEGRIDAD DEL CONTEXTO EN LOS ESPACIOS PÚBLICOS MEDIADOS COMO BASE PARA PROTEGER LA ESFERA PRIVADA DE LOS USUARIOS

Comenzábamos esta disertación aludiendo a la teoría de la integridad contextual como marco para evaluar la pertinencia de los datos privados en los espacios mediados creados por los entornos digitales. Así pues, para facilitar la lectura crítica de la presente discusión, conviene recordar ahora, brevemente, cuáles son los pilares en los que se fundamenta dicha aproximación.

La premisa sustantiva de la teoría enunciada por Helen Nissenbaum parte de la creencia de que todos los aspectos del individuo están gobernados por una serie de convenciones inherentes a cada contexto. Estas reglas actúan como pautas sociales compartidas por toda una comunidad y, de este modo, ante las mismas situaciones

hay un abanico de posibles acciones y conductas que, se considera, no vulneran nuestra esfera privada.

Estas pautas se hacen palpables en nuestro quehacer diario. A modo ilustrativo, Nissenbaum explica cómo no revelamos ni la misma cantidad, ni el mismo tipo de datos personales en una entrevista de trabajo que en una conversación con nuestros amigos. Y esta dinámica se repite en la totalidad de situaciones que puede enfrentar un ser humano, ya que, recordemos, no hay dimensiones de la vida humana que no se desarrollen de acuerdo a estas normas de información.

En este sentido, la protección de las informaciones privadas en un escenario determinado se sopesa en función del mantenimiento de la integridad del contexto, entendiendo que es apropiado que exista un determinado flujo informativo acorde a dicha situación y que el despliegue de ciertos datos personales puede estar justificado e, incluso, resultar necesario para satisfacer la interacción comunicativa.

Esta dinámica se repite en el caso de los espacios públicos mediados, en los que, al igual que sucede en los intercambios comunicativos desarrollados en entornos físicos, la comunicación estaría condicionada por una serie de pautas consignadas a preservar la coherencia de los flujos informativos que dan forma a cada escenario. Estas reglas informativas constituyen cánones no estáticos que se adaptan, son plásticos y evolucionan con el tiempo, los usos sociales, las costumbres, las distintas culturas o los agentes implicados en la comunicación, entre otros muchos factores. Y, por supuesto, también se modifican en función de las necesidades personales del individuo que es quien, en última instancia, decide qué información muestra para posibilitar la interacción social.

Observemos el siguiente ejemplo para ver cómo actúan las citadas pautas: si un servicio de Internet requiere posicionarnos, las normas de propiedad indican que la obtención y utilización de nuestros datos geográficos estará justificada mientras dure la prestación de dicho servicio. Por su parte, las normas de distribución impedirán que esos datos sean enviados a empresas situadas en dicha localización, para que estas nos envíen anuncios personalizados. Del mismo modo, si nuestros datos se almacenan tiempo después de dar de baja el servicio o se comparten con terceras empresas sin que nosotros lo hayamos decidido, esto es, sin nuestro consentimiento previo e informado, la

integridad del contexto habrá sido vulnerada y se habrá producido una intromisión en nuestra esfera privada. De esta manera, al respetar las pautas de distribución, conoceremos la finalidad que se dará a los datos que introducimos en Internet y, al aplicar los usos de pertinencia, sabremos que nuestros contenidos solo serán emplazados en aquellos escenarios en los que realmente son necesarios.

Para satisfacer las premisas de la integridad contextual, el usuario necesita entender cómo funciona el contexto donde se desarrolla el intercambio de datos, esto es, requiere información concisa para concretar los atributos de cada escenario comunicativo, comprendiendo el alcance y las posibles consecuencias de mostrar ciertos contenidos. A diferencia de un intercambio de datos en el espacio tangible, en el caso de las herramientas relacionales de la Web 2.0 el individuo debe tener en cuenta que esa información será emplazada en un espacio público mediado, por lo que deberá conocer si es susceptible de distribuirse más allá de su voluntad y a otros agentes o si será almacenada por tiempo indeterminado lo que, en efecto, vulneraría las normas de distribución y de propiedad.

En este sentido, la aproximación teorética de la autora resulta inestimable en tanto que entronca con dos conceptos clave para la salvaguarda de las informaciones personales en los entornos mediados: de un lado, respeta la capacidad de decisión del individuo, subrayando su autodeterminación informativa. De otro, pone en valor la importancia de que este reciba un flujo de información adecuado, que arroje luz sobre las características del entorno digital en el que opera y le muestre todos los vértices de la ecuación, capacitándole, a la postre, para tomar decisiones críticas.

1.1 LOS USUARIOS Y LA INTEGRIDAD CONTEXTUAL EN LA WEB 2.0

En el análisis precedente, hemos visto como los individuos mantienen formulaciones específicas sobre cómo preservar su información personal en las redes sociales. Manejan así sus distintas relaciones emplazando una serie de datos privados en estos espacios para mantener la interacción social sin perjuicio para su esfera privada. Y esta mecánica varía de unos individuos a otros y en función de sus expectativas de visibilidad o reserva.

Siguiendo pues la lógica del planteamiento de Nissenbaum, cuando nos preguntamos qué lleva a los usuarios a mostrar unas informaciones y a ocultar otras llegaríamos a la conclusión de que es la cantidad de datos privados que ellos consideran necesarios para hacer funcionar sus redes sociales, satisfaciendo sus necesidades comunicativas y la interacción social. De este modo, operan bajo el marco del mantenimiento del contexto cuando introducen, con arreglo a las normas de propiedad: datos de contacto como el correo electrónico para que la plataforma les comunique cualquier cambio; información identificativa para que otros miembros los encuentren; datos para validar o asegurar la cuenta de una sustracción o suplantación de personalidad o contenidos para dotar de sentido una conversación entre amigos. Y, a la vez, controlan su visibilidad en términos de distribución, modificando las opciones de privacidad para que esa información sea sólo visible a amigos o no sea indexada por buscadores.

Sin embargo, a pesar de haber verificado la existencia de estas formulaciones destinadas a preservar parte de los contenidos privados, lo cierto es que los usuarios siguen volcando una cantidad importante de información en la Web y no siempre lo hacen de manera consciente, hecho que, en no pocas ocasiones, degenera en consecuencias indeseadas. Y esta problemática parece mantenerse aun cuando las redes sociales llevan ya diez años entre nosotros. Todo indica que, aunque la concepción de Nissenbaum ofrece un valioso marco de referencia para la salvaguarda de lo privado, desde el punto de vista de su realización práctica aplicar las medidas contextuales no resulta tarea llana.

2. DISCUSIÓN

La teoría de la integridad contextual surge de la pretensión de dar herramientas al sujeto para alcanzar su autodeterminación informativa, toda vez que le posibilita para operar en espacios públicos donde la incursión de datos privados resulta integrante del acto comunicativo. Pues bien, tras arrojar luz sobre los flujos de información y traspaso de datos que se suceden en las redes sociales, y nos referimos tanto a aquellos declarados y visibles para los individuos como a los que permanecen ocultos en la estructura y dinámicas propias, observamos que existen una serie de prácticas habituales que contravienen

seriamente las leyes de Nissenbaum. Dichas actuaciones quiebran las dos normas de la integridad contextual, tanto las de propiedad o pertinencia de la información, como las de distribución, y se concentran en los siguientes casos:

— Apropiación de informaciones de los usuarios para crear y ofrecer publicidad a la carta.

— Utilización de datos de geolocalización para otros fines no justificados o referidos a la obtención del servicio.

— Trasvase de datos con terceras empresas y viceversa (Facebook Conect, Instant personalization, Beacon…)

— Recopilación de contenidos por desarrolladores de aplicaciones.

— Utilización de datos para realizar el seguimiento del usuario dentro y fuera de la plataforma.

— Aumento de la visibilidad y accesibilidad de los contenidos al cambiar los contratos de usuario sin previo aviso. Estos datos pasan al torrente de la Web 2.0 y ya no habrá posibilidad de restitución.

— Hiperexposición de los contenidos del usuario para aumentar las interacciones.

— Centralización de todos los datos e imposibilidad de crear círculos de atribuciones distintas para manejar las diversas relaciones y el flujo de datos destinados a cada una de ellas.

En todos estos casos se vulneran ambas normas de información, en tanto que los datos introducidos son destinados a otros fines y distribuidos más allá de lo inicialmente estipulado por las condiciones del contexto. Estas acciones poseen un denominador común: el usuario sufre las consecuencias de una desinformación que le despoja de todo control. Se utilizan informaciones que él previamente ha volcado, pero no es capaz de otorgar su consentimiento para que se introduzcan en otros escenarios, ya que esta solicitud de permiso ni siquiera ha sido informada.

En otras ocasiones, hemos visto cómo es el propio individuo el que, movido por la necesidad de alimentar su reputación o mantener su círculo de contactos pasa por alto su propia salvaguarda. Esta coyuntura aparece por la falta de entendimiento de la estructura de las

redes, la baja percepción de riesgo y la apariencia inocua de los flujos visibles del interfaz, lo que produce que los sujetos no se percaten de que sus datos pueden ser copiados, distribuidos y almacenados más allá de sus deseos. Lo hemos observado al estudiar la paradoja de la vida privada, del mismo modo que hemos acreditado que dicho fenómeno nace ligado al desconocimiento y al hecho de que resulta altamente complicado acreditar las particularidades de los escenarios creados por las redes sociales.

En resumidas cuentas, la aplicación de la integridad contextual aparece lastrada por la susbtancialidad novedosa de los flujos de información que conforman las redes sociales y, por extensión, la Web relacional. Vayamos más allá y analicemos por qué los agentes que operan en los escenarios digitales, así como los flujos informativos que conforman la estructura subyacente no siempre actúan acorde al mantenimiento del contexto. En otras palabras, describamos detenidamente las trabas que lastran la ejecución de la integridad contextual por parte del propio individuo, así como del resto de actores implicados.

2.1. LA EJECUCIÓN DE LA INTEGRIDAD CONTEXTUAL POR PARTE DEL USUARIO

2.1.1 **La mediación como obstáculo al mantenimiento de la integridad del contexto**

Como dominio público mediado, el flujo de datos que se produce en los entornos digitales poco tiene que ver con el que se da en las interacciones emplazadas en el universo tangible. En este sentido, una de las principales trabas que lastran la comunicación a través de la tecnología se debe, paradójicamente, al mecanismo que la posibilita, esto es, la mediación. Gracias a ella, en vez de interactuar directamente con otras personas, tal y como sucede en el espacio físico, podemos intercambiar datos en la distancia a través de los canales proporcionados por las herramientas comunicativas. Empero, en los ambientes mediados tecnológicamente esa comunicación aparece empobrecida por cuanto no genera la suficiente información como para distinguir las condiciones en las que se produce el trasvase de contenidos. Así, no se especifica, por ejemplo, las barreras entre lo que se considera

espacio privado y lo que no lo es. Y este no es el único inconveniente con el que nos topamos.

La mediación se genera en dos fases. En primer lugar, surge aquella que capacita al ser humano para operar con las herramientas tecnológicas, es decir, la que traduce la abstracción del lenguaje informático que sustenta el interfaz visible y lo convierte en una imagen analógica capaz de ser percibida por los ojos y entendida por el cerebro humano. La segunda es un producto de la anterior y es la que permite a las empresas de Internet dar forma a sus páginas, así como herramientas a sus intereses. Es decir, que procede de cómo las plataformas modulan una determinada zona acotada de la Web; proceso que conlleva una intencionalidad clara por cuanto nace orientado a la consecución de ciertos objetivos específicos.

Si vamos más allá, observaremos que, a diferencia de una charla entre amigos en un espacio corpóreo, ya sea este público o privado, el escenario digital aparece condicionado no solo por esa mediación primaria que posibilita la salida y recepción del mensaje, así como por la secundaria proveniente de las plataformas que en él operan; sino que está además «hipermediado» y «remediado»[774]. Como consecuencia, debido a la utilización integrada de las diversas formas de representación, todo lo que se hace en un soporte se reproduce por otros, aumentando su visibilidad[775] y alternando necesariamente, en cada representación, las condiciones del escenario primigenio que justificaron el despliegue inicial de las informaciones. Este fenómeno se opondría, en sí mismo, a las leyes de propiedad y distribución de Nissenbaum.

Pero si la hipermediación y la remediación son atributos propios de las tecnologías digitales, el salto a la Web semántica acelera de manera exponencial los procesos reproductivos de informaciones y contenidos que se representan una y otra vez. Y, en estas circunstancias, resulta altamente complicado, si no ilusorio, conservar la integridad contextual de los escenarios digitales. Más aún cuando «la realidad virtual es inmersiva, un medio cuyo propósito es desaparecer»[776]. Ante semejan-

---

[774] BOLTER, D. J. y GRUSIN, P. (2011): «Inmediatez, hipermediación, Remediación», en *Cuadernos de Información y Comunicación*, vol. 16, pp. 19-57.

[775] Bolter y Grusin citados por CASTAÑARES, W. (2012): *Op. cit.,* p. 22.

[776] Ibídem., p. 21.

tes condiciones, la imagen superficial a la que se enfrenta el interactor no permite sospechar la dinámica que se da bajo el interfaz.

A modo ilustrativo, una de las violaciones serias de las normas de la distribución vendría condicionada por existencia de unos desarrolladores detrás de las aplicaciones y otras herramientas, que son invisibles para el usuario, oscureciendo el hecho de que nuestra información está abandonando los límites del contexto en el que introdujimos dichos datos y fluyendo a otros escenarios y agentes. Este hecho, cuya prueba más palpable sería la indexación de informaciones personales por los buscadores o la recolección de datos por las terceras empresas que actúan sobre las plataformas de redes sociales, vulneraría la ley de la distribución y, consecuentemente, las normas de propiedad, por cuanto el nuevo contexto no justificaría la utilización de los contenidos recolectados. Este «daño colateral»[777] en la terminología de Hull, Lipford y Latulipe, quebrantaría en definitiva la finalidad inicial por la que los datos fueron revelados, coartando, bajo la bandera del desconocimiento, el poder de decisión que el ideario de Nissenbaum otorga al usuario.

Tanto la remediación como la hipermediación poseen su epicentro en la convergencia que alimenta y sostiene las múltiples representaciones cuando, por ejemplo, la concomitancia de todas las herramientas permite, a través de identificativos comunes como las etiquetas, encontrar multitud de información sobre un mismo usuario.

Por otra parte, las leyes de propiedad y distribución varían con el tiempo por lo que el hecho de que los datos pervivan por un período indeterminado en la Web también podría quebrantarlas. En este sentido, los individuos deberían considerar qué contenidos deciden exhibir, ya que, aun cuando estas informaciones hayan desaparecido de su fuente inicial, la memoria caché[778] de los buscadores puede guardarlas y exhibirlas perpetuamente, habiendo perdido su propietario cualquier control sobre estas. Supongamos, por ejemplo, que alguien pone una foto o comentario en una red social y, a los pocos días, piensa que es mejor quitarlos. Si este

---

[777] HULL, G., LIPFORD, H. R. y LATULIPE, C. (2010): *Op. cit.,* p. 292.

[778] En informática, la palabra de procedencia inglesa y francesa «*cache*» o «memoria caché», tal y como la denomina la RAE, denomina a aquella memoria de acceso rápido de una computadora que guarda, temporalmente, los datos recientemente procesados. *Diccionario de la Lengua Española* (22.ª ed.), Real Academia Española, 2001.

material ha sido atrapado por la memoria caché de Google, se volverá públicamente accesible durante un tiempo determinado. Pero si además entran en juego los denominados «agregadores de datos», motores de búsqueda específicos que se dedican a rastrear Internet y reunir las informaciones personales dispersas por la Red sin una contextualización adecuada[779], dicho contenido estará siempre disponible para el usuario universal, aunque la fotografía o el comentario hayan sido eliminados de la fuente inicial. De este modo, esa información nuestra que no queremos que sea pública y sobre la que ya no tenemos ningún tipo de control, puede ser sucesivamente remediada aunque la hayamos borrado hace años.

Si bien es cierto que existe la posibilidad de pedir que dichos contenidos se retiren de buscadores y otras páginas con sede en suelo europeo haciendo uso del derecho al olvido, poco tenemos que hacer con la generalidad de los agregadores de datos, empresas cuyas matrices tienden a asentarse en países con legislaciones más permisivas. Esto obliga a los individuos a una reflexión inicial, un esfuerzo previo para evaluar si de verdad necesitan introducir o no determinada información y, en caso de duda, seguir los consejos de autores como Parrish, para quien la mejor manera de evitar arrepentimientos es, sencillamente, no introducir dichos datos[780].

2.1.2. **Los usuarios no tienen herramientas para entender, visualizar y comprender los flujos de distribución de la información en la Web 2.0.**

Los entornos virtuales en los que operan las tecnologías digitales no siempre ofrecen la información necesaria para interpretar los escenarios, lo que provoca que el usuario no identifique correctamente en qué condiciones se realiza el intercambio de datos y no sepa por qué leyes guiarse. Desde la perspectiva propuesta por Nissenbaum, en la vida diaria la inserción de contenidos privados viene determinada por entornos sociales altamente granulados. No obstante, en los espacios públicos mediados esta granularidad no se produce, ni es explícita por lo que no es sencillo interpretar qué normas deben usarse en cada

---

[779] Algunos de los servicios que actúan como agregadores de datos más populares son: 123people.com, yaasni o date check.

[780] PARRISH, J. L. (2010): *Op. cit.,* p. 193.

situación concreta para desplegar o no datos privados con arreglo a la integridad contextual. Es decir, el individuo no siempre identifica claramente la naturaleza normativa del medio en el que se requiere su información personal, por lo que no está en condiciones de sopesar, en consecuencia, el despliegue de dichos contenidos. Es más, dado que el cerebro automatiza los contextos y, por tanto, las normas informativas que atribuye a cada uno de ellos, si el sujeto no ha interpretado bien el escenario puede usar normas contraproducentes que dejen su vida privada totalmente al descubierto.

En este sentido, las redes sociales y otras aplicaciones relacionales no aportan herramientas suficientes de contextualización. De hecho, la generalidad de los individuos interpreta, por mencionar un ejemplo recurrente, que su muro Facebook es un espacio privado que les es propio y creen que tienen el poder de decidir con qué contactos comparten o no la información. Sin embargo, cualquier cambio en la política de privacidad de la compañía o, simplemente, las acciones desempeñadas por pares, influirán decisivamente en la visibilidad de sus acciones, en muchas ocasiones, sin que ellos se percaten siquiera de que su información privada se ha vuelto visible.

Esta dificultad para «leer» correctamente el escenario provoca incoherencias contextuales que son endémicas en las redes sociales y una fuente sustancial de problemas para proteger el anonimato de las personas. Un buen ejemplo lo encontramos en los resultados alumbrados por los estudios citados en el capítulo anterior y en los que, cuando a los participantes se les enseñaba cuáles de sus datos resultaban visibles para otros usuarios o para terceras empresas, estos mostraban su asombro e incapacidad para entender cómo dichos agentes habían obtenido acceso. Este hecho, sin embargo, alumbra un cierto optimismo pues en el extremo contrario autores como Lipford demostraban que esta situación se podía invertir al introducir más información para asesorar la toma de decisiones.

En suma, queda delineada una relación directa entre lo que perciben los usuarios y la cantidad de contenidos privados desplegados, esto es, entre la información con la que cuentan para interpretar el contexto y la eficacia y pertinencia de las medidas de protección que ellos mismos desarrollan.

2.1.3 Dificultad para distinguir entre espacio privado y público, así como el alcance y las consecuencias derivadas de las publicaciones

Las estrategias mencionadas en el capítulo anterior permiten a los usuarios conectar con todo su entorno social sin ser ni demasiado públicos, ni demasiado reservados. Con todo ello, la realidad es que estas tácticas defensivas no siempre dan los resultados deseados. Por citar un ejemplo, el hecho de que las redes sociales formen parte de un espacio público acotado y que ellas se desarrollen relaciones típicas de la esfera privada hace que sean percibidas como un área semipública o incluso privada, lo que actúa en detrimento del nivel de alerta del usuario. Esta indefinición torna inútil la aplicación de las normas de la integridad contextual.

A este respecto, existe un amplio debate acerca de cómo el uso de las herramientas relacionales de la Web 2.0 ha cambiado la percepción de los individuos sobre las informaciones que se deben preservar y las que no, así como las acciones que toman para protegerlas. En este sentido, la aproximación de la integridad contextual sostiene que las normas son cambiantes, algo que no es necesariamente dañino, siempre que se respete la voluntad del sujeto y la coherencia del escenario. Pero incluso cuando tenemos en cuenta esta capacidad de adaptación de las normas y usos ligados a los contextos, lo cierto es que las interacciones en la Web social conllevan en ocasiones consecuencias indeseadas e intromisiones que pasan inadvertidas. Incluso si los propios usuarios mismos modelan las normas para satisfacer una necesidad relacional propia, lo más probable es que estén bajando la guardia, en tanto que la información que reciben del contexto no les permite tomar decisiones acordes a la realidad del escenario.

Por otra parte, sabemos que toda la extracción de significado a la que el sujeto está expuesto, use o no las plataformas de redes sociales, se traduce en una minería de datos en la que se obtiene el valor monetario de sus informaciones. Podemos creer, al respecto, que la mecánica desarrollada por este tipo de herramientas se ha convertido en una práctica aceptada, puesto que es más valioso el beneficio adquirido. Pero en suma el resultado es el mismo: lleva aparejada la pérdida de dominio de los propios datos, dado que no son los usuarios los que deciden el alcance de las interacciones.

En consecuencia, estos tres factores: la divulgación ampliada, la no granularidad de los espacios digitales y la dificultad para entender la naturaleza, condiciones y alcance del medio pueden contravenir decisivamente los preceptos de la integridad contextual, factores que no son exclusivos, ya que, no podemos olvidar que en el espacio digital nunca actuamos solos.

Demos ahora unas breves pinceladas sobre la incidencia de otros actores.

2.2 EL RESPETO A LA INTEGRIDAD CONTEXTUAL POR PARTE DE OTROS ACTORES

Dado que en el mundo digital nuestras acciones aparecen interconectadas, focalizar toda la atención en el sujeto aislado nos llevaría a olvidar extremos fundamentales de la ecuación: Las acciones del resto de agentes, también interactores, pueden dificultar seriamente que el individuo preserve su persona de manera efectiva. En este sentido, cabe puntualizar que para que la integridad del contexto se mantenga, todos los componentes de la cadena deben velar por el cumplimiento de las normas imperantes en cada escenario y esto, como veremos, no siempre se cumple.

La realidad a la que nos enfrentamos es que la protección de nuestra información personal no dependerá solo de nuestras acciones, por lo que estaremos al vaivén de los actos intencionados, cavilados o meramente casuales de los otros usuarios y agentes. Tan es así que independientemente de nuestro nivel de conocimiento, entendimiento de los contextos y manejo de las herramientas informáticas e incluso si decidiéramos no usar ninguna de las herramientas digitales, el hecho palpable es no podemos controlar que otro individuo publique una información personal sin nuestro consentimiento. Y lo mismo sucede con las compañías que recaban nuestros datos como activo para su negocio, siendo este un punto especialmente escabroso debido a la magnitud e invisibilidad que adquiere. De este modo, las expectativas de protección que podemos esperar pueden verse empañadas cuando no todos los agentes implicados en la comunicación respetan las «normas de propiedad» y «distribución» que guían el correcto flujo de información. Desgranemos este punto con algo más de detenimiento.

2.2.1 Multitud de servicios sustentan su desempeño en el no respeto a las normas contextuales para agregar y vender informaciones

Tal es el caso de diversas prácticas llevadas a cabo por las plataformas de redes sociales y cuya conjunción con otros servicios de la Web 2.0 provoca que nuestra identidad virtual se vuelva fácilmente accesible. Recordemos simplemente cómo actúan las aplicaciones de terceras empresas dentro de Facebook o aquellos servicios conocidos como «agregadores de datos» que son capaces de reconstruir nuestra personalidad, añadiendo significados a nuestro nombre. El simple hecho de que los buscadores ofrezcan estas páginas en sus resultados o arrojen información que hemos vertido en otro continente, como son las redes sociales, ya implica una descontextualización importante. Especialmente, si sumamos el hecho de que en estas páginas se agregan informaciones de muy distinta naturaleza (personales, laborales, registros públicos…) que fueron introducidas bajo condicionantes bien distintos.

Las posibilidades de ejercer el derecho de rectificación *a posteriori* de la información recabada y publicitada por estas empresas es algo, por lo general, casi anecdótico. En principio porque muchas de las grandes plataformas de Internet tienen su sede en países donde puede operar bajo legislaciones más laxas. Y aun cuando estas se atienen a las leyes del país donde ubican sus oficinas regionales, si el marco normativo es más restrictivo suelen aparecer conflictos de competencias que, en el mejor de los casos, se traducen en una demora en la solución de la problemática, retraso que siempre actúa en detrimento del ciudadano afectado. Además, se da la particularidad de que se trata de datos personales a los que en el momento de publicación no se les ha dado el tratamiento de reservados, puesto que el sujeto los introdujo bajo circunstancias distintas, hecho que puede lastrar su posibilidad de amparo. Así, en ocasiones son los propios usuarios los que sin saberlo otorgan esa visibilidad a sus contenidos, otrora reservados, cuando desconocen, por ejemplo, que sus perfiles en determinadas redes sociales están siendo indexados públicamente.

En esta coyuntura, el ejercicio de la potestad de control sobre las propias informaciones es casi inexistente. A modo ilustrativo, poco se puede reclamar en el caso concreto de los agregadores de datos, pues las informaciones que agrupan ya eran públicas previamente. Este es tal vez el mejor ejemplo de ruptura de la integridad contextual en la

Web 2.0: Basta con poner nuestro nombre y apellidos en Google y consultar los resultados que ofrecen estos agregadores para verificar que muchas de las informaciones que nos imputan se corresponden con la imagen o las acciones de otra persona. Y ello sin tener en cuenta que se exhiben datos que anteriormente habíamos destinado a otros menesteres, pero que ahora aparecen recopilados a modo de dossier personalizado.

2.2.2 **La tecnología no siempre tiene por qué ser neutral, ni ética**

Las redes sociales están diseñadas para conseguir el máximo posible de informaciones personales, lo que las convierte en el instrumento perfecto para la minería de datos. No en vano, uno de los pilares clave de estos negocios es el mantenimiento de una inmensa base de datos con la que atraer anunciantes, por lo que el respeto a la integridad del contexto en la que el sujeto, voluntaria o involuntariamente, vuelca sus contenidos, no representa una prioridad empresarial. De hecho, hemos visto como muchos de los problemas de protección están relacionados con la tendencia de estas plataformas a alimentar errores en la percepción de riesgo. Sus prácticas e, incluso, sus políticas de privacidad y condiciones de uso, inciden en la desinformación del individuo que no siempre entiende cómo funcionan muchos de los controles de privacidad, ni comprende el tratamiento que se dará a sus datos. Asimismo, no son conscientes de los flujos de intercambios de contenidos que se dan bajo dichas plataformas, pues estos no son transparentes o están ocultos de manera intencionada en la estructura de la red.

Nissenbaum arguye que el marco de la integridad contextual está diseñado para considerar cómo la irrupción de una nueva tecnología modifica las normas que condicionan el flujo informativo. Del mismo modo, si la acción de esta se encuentra en contradicción con las pautas que imperan en el contexto recién creado, sabremos que la integridad contextual ha sido violada. No obstante, en el caso de la Web 2.0 esa contradicción nunca es perceptible para los interactores que no tienen constancia de dicha vulneración por cuanto esta se produce en una total ausencia de conocimiento. Como botón de ejemplo, baste mencionar los innumerables casos detallados en el apartado *Análisis* en los que se verifica que el traspaso de datos que tiene lugar entre las

plataformas y las terceras empresas asociadas a ellas es una constante, cuya negación de las normas contextuales nunca es conocida.

Una vez analizados los inconvenientes que la estructura y dinámicas de las redes sociales añaden para el mantenimiento de la coherencia los flujos informativos del contexto, veamos ahora si los usuarios están en disposición de proteger sus informaciones reservadas. Procedamos, para ello, a la comprobación de las premisas de partida.

3. COMPROBACIÓN DE HIPÓTESIS

> Estamos hechos de tal manera que no solo necesitamos una determinada proporción de verdad y error como base de nuestra vida, sino también una cierta proporción de claridad y oscuridad en la imagen de nuestros elementos de vida.
>
> Georg Simmel, *Sociología*[781]

El *corpus* del estudio realizado se ha centrado intencionalmente en una de las herramientas paradigmáticas de la Web 2.0: las redes sociales, encarnadas en Facebook. Tal elección se perpetró por entender que los dilemas planteados por la compañía contenían los patrones de vulneración de la esfera privada que más habitualmente hacen aparición en estas plataformas. De su observación, enmarcada por diferentes acontecimientos que han condicionado la defensa de la vida privada, hemos inferido casos concretos en los que el nivel de conocimiento del individuo, esto es, la información que recibe y su capacidad para entender e interpretar correctamente los entornos digitales donde opera, juega un papel primordial en la salvaguarda de su intimidad y vida privada. Si rememoramos ahora cuál era nuestra premisa de partida, advertiremos no solo que nuestra suposición se ha verificado, sino que, en efecto, los flujos informativos ostentan un papel clave en el dilema que nos ocupa.

La hipótesis sustantiva con la que comenzábamos la presente disertación partía de la consideración de que: «el usuario no obtiene información suficiente para comprender los escenarios de la Web 2.0 en los que opera e introduce sus datos privados y, consecuentemente, no puede interpretar la integridad contextual».

---

781 SIMMEL, G. (1986): *Op. cit.,* p. 404.

Como suposiciones derivadas de la anterior se plantean las siguientes presunciones:

— Tras la llegada de la Web 2.0, la información y la formación del individuo constituyen su mejor defensa *a priori* para proteger su intimidad y vida privada.

— La estructura y diseño de algunas de las herramientas arquetípicas de la Web 2.0 contravienen la integridad del contexto y favorecen, por tanto, la aparición de escenarios en los que se producen estas intromisiones.

— Muchas de las plataformas de la Web 2.0 sacan provecho o incluso basan su negocio en este desconocimiento del usuario.

Desmenucemos, paso por paso, cómo quedan contrastados nuestros postulados.

3.1 LA RELACIÓN ENTRE LA INFORMACIÓN QUE RECIBE EL USUARIO, EL MANTENIMIENTO DE LA INTEGRIDAD CONTEXTUAL Y LA SALVAGUARDA DE LA ESFERA PRIVADA

La hipótesis de la que partía este trabajo se resumen en la premisa de que el conocimiento constituye la mejor herramienta que posee el ser humano para prevenir injerencias en su intimidad y vida privada. En efecto, el individuo necesita información para interpretar los escenarios de la Web 2.0 y entender los distintos flujos, así como el trasvase de datos que se da en su estructura, decidiendo conscientemente cuándo introducir sus contenidos, con quién compartirlos y qué visibilidad otorgarles. Es decir, necesita partir de concreciones y certidumbres para percibir las atribuciones del contexto y actuar conforme a su integridad.

Se subraya así el hecho de que para garantizar la defensa de la vida privada a través del respeto a la integridad contextual, el interactor debe conocer no solo cómo funciona dicho entorno digital, sino recibir información concisa y «transparente», esto es, fácil de entender, aunque rigurosa, sobre el escenario digital, algo que no sucede en un alto porcentaje de los casos.

Sin embargo, dado que los sujetos no reciben dicha información y, consecuentemente, tanto sus decisiones como sus modelos mentales

no siempre se desarrollan acorde a la realidad del escenario en cuestión, las posibilidades de ejecutar su autodeterminación informativa descienden abruptamente. Este hecho alerta de que cuando hablamos del amparo de la vida privada no debemos verter toda la responsabilidad en las acciones y las medidas que toman los individuos ya que, en un alto grado, sus decisiones se encuentran lastradas por la falta de información que reciben sobre el entorno.

De nuevo, la palabra «transparencia» nos juega una mala pasada cuando lo que se torna visible es el usuario y la mediación, tan condicionante, consigue desaparecer logrando así no ser tenida en cuenta por el sujeto.

La complejidad aumenta si tenemos en cuenta que las características propias del entorno digital provocan que el individuo no sea capaz de establecer y mantener la cantidad de esferas distintas, en ocasiones superpuestas, que definen a las relaciones del mundo físico. Cuando se produce tal mezcolanza de ambientes, los límites se tornan difusos, las normas que actúan en un determinado escenario pueden diluirse instantáneamente y se crea una amalgama de coyunturas de atribuciones indefinidas, cuya única certeza es que aparecen contenidas en la carcasa del dispositivo electrónico. Y cuando esas esferas se tornan fluidas, es muy difícil crearlas explícitamente en sitios Web determinados, por lo que manejar los flujos de información entre ellas se vuelve muy complicado.

En este sentido, las redes sociales carecen de la granularidad que distingue a los escenarios que se crean en la realidad tangible, lo que provoca que en el universo digital se mezclen las normas que imperan en situaciones distintas y hasta contradictorias. Argumento, este último, que lejos de suponer un obstáculo en la evolución de la Web semántica o prevenir al sujeto de usar sus servicios, se interpreta como una feliz conquista de la filosofía 2.0, dado que se asume que los usuarios quieren proyectar una imagen unificada al mundo. Sobra indicar que este hecho supone, en sí mismo, la ruptura total de la integridad.

3.2 LA ESTRUCTURA DE LA WEB 2.0 COMO OBSTÁCULO PARA ENTENDER Y MANTENER LA INTEGRIDAD DE LOS ESCENARIOS DIGITALES

Otra de las premisas que estamos en disposición de verificar es que las propias herramientas relacionales obstaculizan que el sujeto pueda tomar decisiones informadas, en tanto que no conoce qué su-

cederá con sus datos una vez introducidos, cuáles serán las posibles consecuencias de sus acciones o cómo actuarán los otros agentes que entran en juego.

Puesto que los contextos en la Web 2.0 son altamente cambiantes y las fronteras fluctúan, la información que, en un momento dado, se introduce puede ser distribuida más allá de nuestro propio dominio y conocimiento, esto es, emplazada en nuevos escenarios, enlazados a un tipo de visibilidad distinta al original. Este hecho, sin duda, impide la correcta aplicación de las normas de propiedad y distribución.

Por otra parte, la propia estructura reticular de la Red que permite comunicar «de muchos a muchos», genera «agujeros contextuales» [782], dado que las intromisiones pueden venir de una infinidad de actores que, en ocasiones, ni siquiera contemplamos. Así, la comprobación de hipótesis dibuja un discurso meridiano: la Web semántica no está diseñada para respetar la coherencia del contexto, ni para satisfacer plenamente los deseos de protección de la información y autodeterminación informativa de las personas.

Y todo ello porque su estructura permite acceder a multitud de datos pero no percibir perspectiva, es decir, no podemos «ver a través». Percibimos una imagen que, a pesar de su dinamismo, solo es la superficie de las corrientes de datos que encierra. Por hacer un símil pictórico, las tecnologías digitales no permiten dar el salto de lo figurativo a lo abstracto, dado que solo podemos leer la información del contexto que se nos presenta de modo analógico, esto es, mediante el interfaz o «cara visible» de los dispositivos de acceso.

3.3 EL PROVECHO DEL DESCONOCIMIENTO

Que el cerebro humano no esté diseñado para descodificar lenguajes binarios no es excusa alguna para no enviarle información. No significa esto que debamos acostumbrarnos a interpretar el lenguaje informático de la mediación que posibilita la comunicación, ya que, no es esa mediación la que nos inquieta. Tampoco necesitamos manejar los códigos y combinaciones numéricas que facultan la transmisión. Lo verdaderamente preocupante es esa confección intermedia

---

[782] HULL, G., LIPFORD, H. R. y LATULIPE, C. (2010): *Op. cit.,* p. 292.

que proviene de las empresas de Internet: A través de ella, se oscurece el intercambio comunicativo, y ello, auspiciado por políticas de privacidad, protección de datos o condiciones de uso que no revelan, adecuadamente, cuáles son los procesos seguidos en esa segunda mediación generada por ellas.

Esta desinformación actúa en detrimento del usuario, tornándole inerme, a la vez que alimenta un negocio fundamentado en la monetización de sus datos personales. Así, si el individuo no se percata de que sus informaciones están siendo recolectadas, no podrá tomar decisiones informadas y conscientes sobre sus actos. Y no siempre es cuestión de ingenuidad, es que ni el interfaz con el que operamos ofrece la información suficiente, ni las políticas y aplicaciones diseñadas por las compañías parecen tener el entendimiento del usuario entre sus objetivos.

En consecuencia, podemos señalar que la propia naturaleza de la Web 2.0 provoca que sea muy complicado aplicar las leyes de la integridad contextual, en tanto que los datos introducidos para un contexto concreto pueden ser repetidos hasta la saciedad y emplazados en otros escenarios, sin que medie consentimiento expreso alguno del propietario de las informaciones.

4. ENTONCES, ¿CÓMO PROTEGER A LOS USUARIOS?

> Los efectos positivos de los nuevos medios y de las Tecnologías de la Información pueden ser ampliados y sus consecuencias negativas mitigadas gracias a un sentido de la responsabilidad y consciencia, al ejercicio de derechos y deberes, y a la capacitación de las gentes todas.
>
> Ricardo Díez Hochleitner, presidente del Club de Roma[783]

En el presente escrito ha quedado demostrado que los individuos no son plenamente conocedores de todo el traspaso de datos que se da bajo la capa visible de la Web 2.0, ni por supuesto, reciben información sobre ello. Ya se ha visto cómo determinados servicios como las redes sociales exigen, en sí mismos, la captura y gestión de datos

---

[783] Ricardo Díez Hochleitner, citado en Cebrián, J. L. (1998): *La Red*. Madrid. Santillana, p. 9.

de carácter privado. Y cómo en multitud de ocasiones las prácticas desleales de las compañías, la estructura difusa y afortunadamente ácrata de Internet y la desinformación que envuelve las acciones tomadas por los usuarios contribuyen a que estos no sean capaces de ejercer sus derechos de autodeterminación informativa.

Así, la realidad es que, a pesar de que en estas plataformas los sujetos introducen contenidos de manera voluntaria, esta sustracción va más allá de su dominio; sin mencionar aquellos casos en que los datos son volcados por otros agentes. A este respecto, sabemos que si la información privada no es hecha pública por el propio individuo, bajo su conocimiento y consentimiento, es la propia naturaleza de la intimidad y vida privada la que impide, al hacerse visible, que exista un resarcimiento pleno, por cuanto, por definición, algo que se ha hecho público no puede volver a su estatus anterior. Lo que sí parece inalterable es que las múltiples caras de esta nebulosa difusa y enmarañada parecen haberse conjurado para tornar más vulnerable al verdadero protagonista de la tecnología digital y agente más frágil de la cadena.

Nos encontramos así con un dilema de hondo calado y complejidad específica, por cuanto se trata de una realidad poliédrica, creada por tres dimensiones: la legislativa, la técnica y la social. Las dos primeras nos restringen el marco de actuación al impulso de leyes, creación de unas directrices suscritas por las grandes corporaciones y otras empresas que operan en la Red, así como la implantación de estándares técnicos y herramientas respetuosas con la esfera privada del individuo. La realidad social, por su parte, nos compele a nutrir al interactor con información clarificadora acerca del funcionamiento de los entornos digitales y ofrecerle herramientas para denunciar posibles abusos. Comencemos abordando la primera dimensión.

4.1 LA DIMENSIÓN NORMATIVA

Existe la necesidad, casi urgencia, de modificar la normativa vigente dado que la actual regulación ha dado muestras de estar obsoleta y no satisface los desafíos surgidos en el entramado digital. A este respecto, reforzar las autoridades nacionales de protección de datos, certificar el cumplimiento de unos mínimos en la custodia y tratamiento de nuestros informaciones, desarrollar el derecho al olvido o imponer herramientas para garantizar la seguridad de los contenidos

privados desde el diseño y por defecto, se consolidan como medidas, todas ellas, esenciales y que representan pasos de gigante para solventar una buena parte de las incompatibilidades que se presentan.

No obstante, Internet está muy lejos de poder ser regulado eficientemente. En primer lugar, porque no se trata de poner parches a cada situación novedosa que pone en peligro nuestra esfera privada. Entraríamos así en una dinámica inagotable en la que nos veríamos constreñidos a disponer normativas para cada caso concreto, a sabiendas de que, al día siguiente, surgiría una nueva problemática. Sería, en definitiva, como poner vallas al campo.

Igualmente, aunque la actualización de la reglamentación acorde a los desafíos actuales constituye, sin duda, una necesidad en nuestros días, debemos señalar que no se debe volcar en el legislador toda la responsabilidad en lo referente a la presente problemática. Debido a la naturaleza propia de los entornos digitales, la ley no siempre llegará a tiempo para remediar ciertos casos. Asimismo, presentará un carácter limitado, por cuanto: «establecer un exceso de complejidad o una sobrecarga de limitaciones podría devenir en hacer inviable la puesta a disposición del mercado de innovaciones potencialmente contributivas al progreso económico y el bienestar» [784].

4.2 LA VERTIENTE TÉCNICA

Respecto a la realidad técnica, creemos en la pertinencia de imponer ciertas directrices compartidas, requisitos regulados por ley que obliguen a los agentes que nutren de herramientas a la comunicación digital a garantizar la protección de las personas desde el diseño y mediante la introducción de mecanismos para preservarla por defecto. En este sentido, un acuerdo de mínimos sería deseable y, a todas luces, necesario para que la implantación de esos requerimientos fuese realmente eficaz. Sin embargo, dado que las compañías que operan en el universo digital no están sujetas más que a las leyes del mercado y al marco legislativo de su país, nos veríamos impelidos a hablar de este punto casi en términos de utopía. Por ello, se trata de establecer la obligación de estos estándares en todas aquellas empresas que cuenten con sede en

[784] BADÍA, E. (2012): *Op. cit.*, p. 19.

regiones enlazadas a normativas más restrictivas, tal y como sucedería con las compañías con delegaciones sitas en suelo europeo.

4.3 LA REALIDAD SOCIAL

A pesar de la urgente actualización de la normativa y la acertada aplicación de las citadas recomendaciones técnicas, como los son estándares de protección por defecto, no podemos obviar que la estructura y desconocimiento de las dinámicas que sustentan la Web alimentan problemas de interpretación que dificultan la toma de decisiones críticas por parte del interactor. Todo ello, sin olvidar que, en muchas áreas, la competencia de los usuarios y la información proporcionada pueden no ser suficientes para garantizar un adecuado nivel de protección; así como, en última instancia, las acciones de los individuos no siempre responden a la lógica de la pertinencia. Teniendo todo esto en cuenta, resulta evidente que verter toda la responsabilidad en el usuario es injusto e irrealista.

Es por ello que, asentados ya en el factor social, nos preguntamos: ¿Qué acciones podemos tomar para asegurar un nivel de garantía deseable en la integridad nuestra vida privada, a la vez que disfrutamos del beneficio que aportan las tecnologías digitales? El camino a desbrozar nace de la evidencia de que buena parte de las intromisiones se dan en escenarios en los que el flujo de información que recibe el usuario no permite la valoración crítica del contexto. El desconocimiento conllevaría así una mayor vulnerabilidad del sujeto, en una situación que se torna exponencialmente peligrosa en la medida en que parece retroalimentarse. ¿Cómo combatir dicha vulnerabilidad?

Afirma, con su habitual claridad de ideas, el autor de «Nativos e inmigrantes digitales» [785], Marc Prensky, que si trabajamos para crear y mejorar el futuro, necesitamos imaginarnos un nuevo sistema de distinciones valores: ya no debemos pensar en lo que distingue a unos usuarios de otros, sino que tenemos que centrarnos en nuestro denominador común: debemos pensar en términos de «sabiduría digital». En la actualidad, el conocimiento de los entornos tecnológicos, esto

---

[785] PRENSKY, M. (2001): «Digital Natives, Digital Immigrants», en *On the Horizon*, vol. 9, n. 5, pp: 1-6.

es, la información pero también la formación en competencias digitales, constituye un elemento central, clave para la sociedad entera:

> La tecnología digital puede hacernos cada vez más sabios. La sabiduría digital es un concepto doble: se refiere, en primer lugar, a la sabiduría que se presenta en el uso de la tecnología, con el que nuestra capacidad cognoscitiva llega más allá de nuestra capacidad natural. En segundo lugar, a la sabiduría en el uso prudente de la tecnología para realzar nuestras capacidades[786].

Su antagónico, esto es, la desinformación, es el epicentro en torno al que pivotan las injerencias en la esfera privada. Así, dado que sabemos que la carencia de información conforma uno de los vértices más recurrentes de la citada problemática y que dicho extremo constituye una constante que afecta a todos los usuarios de manera universal, nos vemos impelidos a actuar en dicha dirección, reforzando la defensa del usuario, objeto común de las intromisiones.

Es por ello que, desde el presente texto, creemos firmemente en la conveniencia de establecer mecanismos para reforzar el papel decisorio del sujeto frente a ese desconocimiento que va más allá, incluso, de lo que sucede en la Red. Y esta no es una afirmación azarosa; tal y como nos recuerda Enrique Badía:

> La mayoría de usuarios de Internet carece de la debida conciencia de cuáles son sus derechos, qué grado de protección han asumido —o renunciado— y, lo que es todavía más relevante, cómo y ante quién deberían reclamar la protección de sus derechos y, en caso de violación, cuáles son las instancias y los procedimientos que tienen a su alcance para reclamar ser resarcidos[787].

Realidad constatada por los datos recogidos en el *Eurobarómetro Especial 359*: *Attitudes on data protection and electronic identity in the European Union* y en el que se muestra que solo una tercera parte de los europeos son conscientes de la existencia de una autoridad nacional pública de protección de datos[788].

En consecuencia, se torna ineludible actuar en dicha constante que es la información y en el agente de la cadena que sí está en nuestra

---

786 Ídem.
787 BADÍA, E. (2012): *Op. cit.* p. 19.
788 EUROPEAN COMMISSION (2011): *Op. cit.*

mano reforzar: el usuario. Es decir, debemos trabajar en su capacitación digital para ayudarle a entender las herramientas comunicativas y la mecánica de los entornos digitales; así como en su formación, facultando la comprensión de las implicaciones de las acciones que desempeña en Internet. Inquietudes, todas ellas, que deben tener presencia en la vida académica y en los medios de comunicación, con el fin de que calen profundamente en la sociedad. Y, dado que divulgar la información necesaria se constituye en imperativo para cualquier agente implicado, y toda investigación que se precie debe intentar ofrecer respuestas para solucionar la problemática que aborda, destinaremos las siguientes páginas a delinear los principios de actuación de una propuesta, encaminada a minimizar las posibles injerencias en la esfera privada del sujeto.

5. PRESENTACIÓN DE LA PROPUESTA

Debemos crear el mundo en el que nos gustaría vivir.
Richard Mason, *Four ethical issues of the information age* [789]

Comenzaremos, en primer lugar, incidiendo en una advertencia: sería del todo ilusorio afirmar que podemos controlar todas las intrusiones en la esfera privada generadas en los entornos mediados de la Web. Por ello, no perderemos la ocasión de insistir que la aplicación de la presente propuesta no exime a los agentes implicados en la comunicación de mantener y desempeñar acciones destinadas a una protección activa. Si bien, es cierto que podemos realizar una serie de actuaciones para minimizar los efectos negativos de ciertas herramientas relacionales. Para ello, es necesario dejar a un lado las negras profecías futuristas que auguraban un futuro *orwelliano*, comparación que, además de no corresponderse con la realidad, aporta pocas soluciones.

Una vez aclarado esto, nos centraremos en la presentación de nuestra proposición. En el siguiente capítulo y tras señalar las principales conclusiones de nuestra investigación, presentaremos un plan de actuación elaborado sin desdeñar la importancia capital de im-

---

[789] Mason, R. O. (1986): *Op. cit.,* p. 12.

plantar determinados elementos legislativos y técnicos, pero centrándonos en la pieza clave de la interacción comunicativa, esto es, el ser humano, al que nos proponemos nutrir de armas suficientes para incrementar su capacidad crítica a la hora de operar en la Red. Así, como ya hemos expuesto, en esta tesis pretendemos actuar desde la óptica del individuo, denominador común de la ecuación comunicativa y donde sí podemos controlar, en cierto modo, que las acciones realizadas no promuevan situaciones potencialmente peligrosas.

El avance de las Tecnologías de la Comunicación y la Información hace que sea imposible contemplar todos los posibles escenarios en los que se vulnera el derecho a la intimidad y vida privada de los ciudadanos, si no es *a posteriori* y como respuesta a situaciones de transgresión ya observadas. Se legitima, así, la necesidad de contemplar las potenciales intromisiones desde dos perspectivas complementarias: la que nos urge a disponer nuevas normativas y estándares técnicos que velen por la seguridad de los ciudadanos y la que habla de la necesidad de facultar al usuario y fortalecer su papel activo a la hora de ejercer su autodeterminación informativa.

Es en ese punto en el que deberíamos considerar la importancia de una actuación más global que la que se propone exclusivamente desde el ámbito jurídico, insuficiente, a todas luces, dado que no operamos en un entorno sujeto a limitaciones geográficas. Si bien es cierto que sería más efectivo imponer una serie de políticas comunes en las empresas que gestionan las plataformas de la Web, dado que la disparidad de marcos jurídicos existentes avala comportamientos divergentes e, incluso, contradictorios sobre la protección de datos, este extremo es, hoy por hoy, inviable. Por otra parte, en la actualidad es complicado imaginar un horizonte en que dichas compañías decidan renunciar, voluntariamente, al tan lucrativo negocio que la vulnerabilidad del individuo alimenta. Todo ello, induce a actuar sobre las mejoras basadas en lo que puede controlar el individuo y lo que son capaces de fomentar los poderes públicos.

A este respecto, debemos destacar la urgencia de una actualización normativa como la relatada a principios de esta tesis y referida al futuro Reglamento de Protección de Datos en Europa, cuyos cambios constituirían un buen punto de partida para solventar parte de la problemática. De hecho, en nuestra proposición citaremos cómo dos de sus medidas resultan vitales, por cuanto, por primera vez, se imple-

mentaría la protección *a priori:* Nos referimos a la obligación de introducir estándares de preservación de los datos por defecto y desde el diseño, así como la implantación de herramientas para asegurar que el consentimiento sea informado.

Por otra parte, en numerosas partes de este trabajo hemos enumerado que las claves de la defensa activa que puede llevar a cabo el usuario se basan en dos factores: el conocimiento, esto es, saber a qué finalidad se destinarán los datos, durante cuánto tiempo se almacenarán o los perjuicios derivados con la interacción de otras herramientas, entre otras cuestiones; y el consentimiento, estando, este último, condicionado al anterior factor. De este modo, la finalidad podría justificar la utilización de ciertos datos personales, hecho que implicaría, necesariamente, el conocimiento previo del propietario de dichas informaciones. A este respecto, uno de los hallazgos más interesantes y en el que coinciden muchos de los estudios citados en el anterior capitulo, es la importancia que los sujetos dan al hecho de ser informados correctamente sobre ciertas prácticas.

Nuestro cometido a este respecto no es otro que centrarnos en cómo capacitar al usuario para que sea capaz de entender el alcance de sus acciones y obtenga herramientas para otorgar dicho consentimiento. Y lo más complicado: cómo hacerlo para una inmensa parte de las personas que se encuentran bajo marcos normativos distintos e interactúan con empresas de alcance multinacional. Recordemos que Internet es una globalidad y no podemos dar soluciones parciales o parchear problemáticas concretas.

Todo lo expuesto nos compele a atajar la problemática a través de mecanismos exógenos, mediante la educación y el aporte de información suficiente para ampliar las competencias digitales y el conocimiento del entorno Internet. Pero también, otros internos incluidos en el propio interfaz de la Web 2.0 y destinados a asesorar al usuario para que pueda tomar decisiones críticas sobre el volcado de sus datos o denegar el uso de los mismos *a priori.* Con este objetivo en mente, surge la propuesta que culmina el desarrollo de la presente tesis y que detallaremos en el siguiente capítulo, junto a las conclusiones más relevantes del estudio.

6. REFLEXIONES SOBRE EL CAPÍTULO: EL PAPEL DETERMINANTE DEL CONOCIMIENTO

Información, conocimiento, formación, contextualización, contexto… Qué duda cabe que estas nociones han sido lugares comunes en la presente investigación, certificando que, en la generalidad de los supuestos, la violación de la intimidad y vida privada se ha producido en entornos difusos, marcados por la desinformación, por el desconocimiento o ingenuidad del usuario o, directamente, por la vulneración de sus derechos, aprovechando su debilidad. En el capítulo que ya toca a su fin, hemos averiguado, igualmente, que al no ofrecer dicha base, esto es, al no concretar las atribuciones de los escenarios ni ofrecer información sobre el contexto, las tecnologías 2.0 contradicen el paradigma de la protección de la intimidad y vida privada mediante el respeto a la integridad contextual, por cuanto los datos que se introducen son usados para otros fines que los notificados al usuario (normas de propiedad) y son compartidos hasta la saturación con terceros (normas de distribución).

Esta difusión de nuestra vida privada constituye una suerte de intromisión no informada que no siempre ha tenido la misma intensidad, la misma dirección, ni los mismos agentes involucrados. Hemos resaltado así el papel de una de las herramientas 2.0 cuyas prácticas oscurecen ampliamente las dinámicas que tienen lugar bajo la estructura que soporta la Red, contradiciendo, consecuentemente, los dictámenes del marco enunciado por Nissenbaum. Y, puesto que los casos analizados representan muchas de las situaciones propiciadas por otras herramientas relacionales con las que además se entrelazan, esto nos lleva a certificar que la Web semántica auspicia coyunturas contenidamente dañinas para la salvaguarda de nuestra esfera privada, dado que, en ningún momento, se respeta un flujo informativo apropiado.

Por otra parte, sabemos que la maraña de redes que es Internet constituye un reflejo de la vida real, como ya avisara Castells, pero conforma, a la vez, un universo novedoso marcado por la descontextualización, unos límites desdibujados y, en definitiva, un entorno inestable en el que todavía estamos aprendiendo a movernos. Así, en las interacciones en espacios físicos la información que nos ofrece el escenario nos da una serie de pautas que nos ayudan a decidir qué datos son apropiados desvelar y cuáles no. Del mismo modo, la difu-

sión de estos posee un carácter finito: entre nuestro círculo de amigos, compañeros de trabajo, ante un auditorio… Si no media la tecnología, esos contenidos no serán transportados a otros contextos, por lo que si decidiéramos contar con una difusión mayor o incluso mundial, nos veríamos abocados a acudir a un medio de comunicación de masas, de otro modo, sería imposible.

En los entornos digitales, sin embargo, somos capaces de extraer menos información del escenario en contraste con una mayor visibilidad o publicidad *quasi* total de nuestros actos. Y, dado que operar en términos infinitos es algo para lo que el cerebro humano no está diseñado, concretar las atribuciones de esos recintos digitales semiacotados y mediados constituye una necesidad.

Como corolario, nos acogeremos a la capacidad de divulgación ampliada y la mencionada indefinición de los escenarios en los que se dan los intercambios de información, como elementos que fomentan una indeterminación capaz de contravenir, radicalmente, el mantenimiento de la integridad del contexto, volviendo altamente factible la violación de las normas que regulan el despliegue de información. Es por todo ello, que en este mundo interconectado el conocimiento se torna en virtud esencial, en tanto que se encuentra en la substancialidad misma de la problemática que ha protagonizado nuestro estudio.

PARTE V

CONCLUSIÓN DE LA INVESTIGACIÓN

CHAPTER X. CONCLUSIONS AND PROPOSALS[790]

SUMMARY

This thesis has underlined an alternative approach to address the problem of privacy protection on the Internet focusing on the essential role that knowledge plays both in order to prevent breaches taking place and to ensure that users are capable of exercising their informational self-determination. In the following chapter, we make some recommendations for improvements and put forward the importance of carrying out educational measures in conjunction with other instruments such as «privacy by design» and «informed consent». Finally, we present a proposal on a new model of «informed consent» which aims to deal with the complex issue of how to supply users with the amount of information they may need to satisfy their desires for data protection whilst, at the same time, to fulfil their requirements for social interaction on SNS.

1. INTRODUCTION

Privacy rhetoric often focuses on the individual (…)
Models that go beyond the individual often focus on groups (…)
or articulated lists of others (…)
But what are the implications of privacy in a networked world
where boundaries aren't so coherently defined
and when entities aren't so easily articulated?

danah boyd (2013) *Networked Privacy*

The protection of personal data in Internet has gained significant attention since the increased collection of private information online and the superior capabilities for searching, tagging and aggregating this data Information and Communication Technologies (ICT) provides. This is not a minor issue therefore it is not surprising that in

[790] Este capítulo, que responde a los requerimientos de la mención europea, se ha elaborado gracias a una beca otorgada por el Deutscher Akademischer Austauschdients (DAAD).

recent years there has been a lot of interest in studying issues relating to privacy concerns that users have and how these might impact their online activities. Governments from several democratic countries as well as public and private institutions are forced to face these new challenges for data protection, underlining an urge for a new set of rules and technical improvements aimed principally to enforce users' control over data and enhance their informational self-determination.

In line with it, in 2011 the German National Academy of Science and Engineering (ACATECH) launched a project that focuses on the privacy dilemmas associated with the Internet, developing recommendations for a «culture of privacy and trust», core values and conditions to increase a safer use of ICT. The term «culture» has not been chosen at random. It is used to emphasize that dealing with the privacy dilemmas requires a complex approach that combines education and good practices with appropriate legislation and technology. Culture allows users to assess and choose the suitable degree of control about their personal data depending on their preferences and the respective context, hence its importance. Within this culture of privacy, education, good practices, law and technology are developed in such a way that this choice becomes possible[791].

Addressing the translational dimension of this issue, in 2012 the European Commission proposed a major reform of the European Union (EU) legal framework on the personal data protection[792]. The current EU Data Protection Directive 95/46/EC does not consider important aspects like globalization and some ICT developments, therefore, a proposal for a regulation was released on 25 January 2012, published in 2013 and it is expected to be finally adopted in 2015.

This reform aims to unify data protection with a single law, the General Data Protection Regulation (GDPR). This new draft European Data Protection Regulation strengthens individual rights and tackles the challenges of globalization and new technologies, seeking to extend the scope of data protection legislation beyond the EU bound-

---

[791] BUCHMANN, J. (ed.) (2013): *Op. cit.*, p. 19.

[792] EUROPEAN COMMISSION (2012): Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses. Available at: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htmeuropeancommission [27/12/2013].

aries for the first time. The changes introduced will help to improve personal data protection for individuals in the following ways:

— Reinforcing the role of National Data Authorities.

— Imposing the «Right to be Forgotten» to allow people to delete their data if there are no legitimate reasons for retaining it so that third persons can no longer trace them. Although the concept described is derived from several pre-existing European ideals, the term «Right to be forgotten» is relatively new. It was on May 30, 2010 when the European Court of Justice legally solidified that it is a human right when they ruled against Google in the Costeja case[793]. The 2012 draft European Data Protection Regulation Article 17 details the «Right to be Forgotten» for the first time. Under Article 17 individuals will be able to:

> Obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child or where the data is no longer necessary for the purpose it was collected for, the subject withdraws consent, the storage period has expired, the data subject objects to the processing of personal data or the processing of data does not comply with other regulation[794].

— There will be increased responsibility and accountability for those processing personal data. At this point new regulation introduces a notably innovation: People will be able to refer cases where their data has been breached or rules on data protection violated to the Data Protection Authority in their country, even when their data is processed by an organization based outside the EU. Additionally, it will apply in those cases where personal data is processed abroad by companies that are active

---

[793] Court of Justice of the European Union (2014): *Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*. Available at: http://europa.eu/rapid/press-release_CJE-14-70_en.htm [12/12/2014].

[794] European Commission (2012): *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data (General Data Protection Regulation)*. 2012/0011 (COD).

in the European Market. This will give people in the EU confidence that their data is still protected wherever it may be handled in the world.

— People will have easier access to their own data and be able to transfer personal data from one service provider to another more easily.

— Introduction of «privacy by default» and «informed consent». Much research into ICT users' behaviour shows they are usually unaware of how their information is being stored, and the purpose of this collection.

However, in this essay we have outlined the necessity of regulation working hand in hand with other improvements. Therefore, in this final chapter we underline the main conclusions of the present research, focusing on the key role played by education and user's knowledge to prevent violations of privacy. Within this framework, it aims to explain, firstly, the key importance of educational measures as well as technical improvements such as «privacy by design» and «informed consent» as instruments to supply users with the suitable information to protect their privacy. Subsequently, we present a proposal on a new model of «informed consent», underlining the suitability of its implementation as «opt-in» model by layers.

2. CONCLUSIONS

2.1 THE IMPORTANCE OF USER'S KNOWLEDGE TO PROTECT THEIR PRIVACY AND DEVELOP THEIR «INFORMATIONAL SELF-DETERMINATION»

An updated regulation in conjunction with knowledge and digital competences play an essential role to mitigate privacy breaches in online mediated environments. They both represent common themes linked to user's necessities to understand the functioning of digital environments in order to evaluate the possible repercussions their actions may involve for their privacy. Therefore, knowledge in the form of a correct flow of information becomes necessary to understand correctly the contextual norms governing in this scenery, indicating the quantity of personal information it is necessary to display in each

context to satisfy social interaction[795]. At the same time, it helps users to evaluate the privacy expectations when posting their personal data in mediated public spaces. For that reason, it has been frequently mentioned Nissenbaum's «contextual integrity» theory since it provides a useful framework to consider the preservation of privacy on digital environments. In addition, it is able to deal with many different conceptions of privacy enrooted in every culture[796]. As well as the dynamic process of boundary negotiation that distinguishes privacy and publicity according to circumstances[797]. Furthermore, it links with essential concepts concerning the protection of personal data on mediated environments: the necessity of a correct flow of information in order to identify every context and respect the contextual integrity, as well as the suitability of improving an active role of users to enforce their decisional autonomy.

From this premise, users may be able to choose which data display depending on the context and thus privacy protection could be translated as «the ability for people to choose and control what they disclose and what the hide»[798]. As a result, privacy is closely connected to the basic right to «informational self-determination» and consequently, knowledge about digital environments becomes an essential requirement to enable citizens to exercise their privacy rights.

As Rössler points out protecting privacy may take into account at least three different dimensions: «decisional privacy», «informational privacy» and «local privacy»; three necessary areas for individuals to control aspects of themselves, to be able to express themselves and to act accordingly to their own values and plans[799]. On her view, the contravention of the right to privacy is a violation to the person's autonomy since «privacy protects autonomy in those respects in which the exercise of autonomy is dependent upon my control of the

---

795 NISSENBAUM, H. (2004): *Op. cit.*

796 CAPURRO, R. (2005): «Privacy. An intercultural perspective», *Ethics and Information Technology*, vol. 7, n. 1, pp. 37-47, p. 37.

797 ALTMAN, I. (1975): *The environment and social behaviour*. Monterey, CA: Brooks/Cole.

798 BUCHMANN, J. (ed.) (2013): *Op. cit.,* p. 14

799 RÖSSLER, B. (2005): *The value of privacy*, Cambridge, MA: Polity Press.

access of others to me, to my person, to my (reflects on) decisions and to information about me»[800].

The connections between privacy, autonomy and democracy are so close that it does not seem accurate to say that one is instrumental to the other. As Deborah Johnson outlines «privacy, autonomy and democracy are so intertwined that one is inconceivable without the other. Privacy is not just instrumental to autonomy or democracy; it is essential to both»[801]:

> The idea of democracy is the idea that citizens have the freedom to exercise their autonomy and in so doing develop their capacities to do things that have not been thought of before. Democracy requires citizens who are capable of critical thinking, individuals who can argue about the issues of the day and learn from the argument so that they can vote in. [...] The argument for privacy is, then, an argument for the space that individuals need to develop autonomy.[802]

2.2 USER'S KNOWLEDGE, A KEY CONCEPT TO MAKE CONSCIOUS DECISIONS IN SNS AND OTHER WEB 2.0 SERVICES

A correct flow of information about the possible repercussions of posting personal data in some of the contexts created by ICT plays an essential role both, to ensure informational self-determination and to avoid breaches on the contextual integrity. Therefore, receiving transparent information becomes fundamental to prevent users from suffering infringements of privacy. From this premise, Nissenbaum's theory provides a valuable framework to mitigate privacy breaches on mediated environments. Nonetheless, from the point of view of its practical execution applying contextual norms is not so simple, especially since the arrival of some Web 2.0 tools. Within this framework, one field of study that has drawn particular concern is the provision of personal data on Social Network Sites (SNS).

---

[800] Ibídem, p. 73.
[801] JOHNSON, D. (2009): *Computer Ethics*. Pearson, New Jersey, p. 97.
[802] Ídem.

Users may find several difficulties to understand and control data flows in these mediated environments. Moreover, contextual integrity depends on the contextual information and whereas offline privacy is mediated by highly granular social contexts, digital communication, especially SNS, lack much this granularity and thus, users find themselves incapable of exercising their right to informational self-determination[803]. Furthermore, the ambiguity of some SNS such as Facebook, make it difficult for users to determinate whether it is a public space[804] or not and even when users are aware of that, third developers create added functionalities that may break the contextual norms prescribed by Nissenbaum. As a result, online tools seem to create a new environment characterized by the collapsing of contexts[805].

Therefore, despite developing a more suitable regulation the main drawback we find when trying to protect users is the ambiguity inherent to Web 2.0 tools such as SNS. Thus, the challenge we may face is how to proportion Web 2.0 users enough information to become them capable of deciding which and how many private information is needed to display in each context in order to both protect them and, at the same time, satisfy social interaction.

3. **RECOMMENDATIONS**

3.1 EDUCATION

In light of the conclusions underlined, information has a key role to play as far as privacy protection is regarding. By providing users with a flow of information about the risky characteristics of each context created by SNS we could prevent some of the unexpected consequences from taking place. For that reason, we place emphasis on the need to equip everyone with extensive knowledge and skills required to protect their personal data. These Internet competences are essential, in particular in order to enable free self-determination and democratic participation; therefore, the goal of education should be developing these skills.

---

803 HULL, G., LIPFORD, H. R., and LLATULIPE, C. (2010): *Op. cit.,* p. 289.
804 YOUNG, A. L. and QUAN-HASSE, A. (2013): *Op. cit.*
805 BOYD, D. (2008): *Op. cit.,* «Taken out of...»

The afore-mentioned competences would improve the ability users have to understand digital contexts, to evaluate the relevant risks to their privacy and to operate in a safer way. This includes ensuring that they are capable of interpreting the relevant flows of information which make up the contexts created by SNS platforms and other Web 2.0 tools. Once they have this knowledge, they will know the available options and thus will be in a position to modify their privacy preferences whenever they wish to. Additionally, they will know their duties and responsibilities towards themselves and others —We must remember that privacy is not an individual issue. As a result, by developing Internet competences users will be able to manage Internet privacy issues in an informed manner, providing them with a huge array of options.

As it is essential that everyone possess Internet competences, the suitable educational provision should therefore be available for a wide variety of age groups. These include not only children and young people, but also university students and adults of all ages and educational levels, regardless of whether they are frequent Internet users or not.

Finally, we make especial mention of other targets in order to ensure that every user has knowledge and skills required to protect their own data as well as taking advantage of the benefits of Web 2.0 tools. Parents and teachers need to gain an understanding of how young people behave on the Internet, but also retired people and those so called «digital outsiders» who needs special training.

3.2 TECHNOLOGY AND REGULATION

Education should be supported by updated regulation and the implementation of in suitable technologies. From a legal point of view, we have underlined the importance of improving measures such as «privacy by design» —or «privacy by default»— and «informed consent», particularly in order to increase users' privacy protection as well as to satisfy their needs for informational self-determination. We must admit, however, that new EU Draft Data Protection Regulation introduces other useful measures such as the «Right to be forgotten» we must put apart. Nonetheless, in this essay we have focused on those measures capable of preventing privacy breaches *a priori*, that

is to say, before such violations taking place. In line with it, the following pages aim to delineate the main points of a proposal which introduce a new model of «informed consent» able to ensure the preservation of privacy from the very beginning.

4. PROPOSAL

The suggestions presented in the following section are geared towards developing educational measures as well as technology improvements —both working in conjunction with regulation— in such a way to enable privacy protection whilst, at the same time, ensuring that the Internet can fulfil its potential for supporting users' informational desires and democratic participation.

4.1 WHY INFORMED CONSENT

From the point of view of legal theories, the right to privacy is considered a personality right, directly pointing at «informed consent» as the specific tool to draw the line between the legitimated or unauthorized use of personal information. In addition, since one of the key concepts for data protection is the purpose given to our data after collection, wherever consent is required for data to be processed, it will have to be given explicitly, rather than assumed as is sometimes the case now.

For that reason, it is common to see calls for «informed consent» from National Data Protection Authorities, organizations and several groups of citizens. Focusing on Europe, according to *Special Eurobarometer 359* from European Commission, over 70% people said they were concerned about how companies use their data and over 74% wanted to give their specific consent before their data is collected and processed on the Internet[806].

The acquisition and use of personal data requires the informed and voluntary consent. In fact, the current Data Directive ensures that processing of personal data meets three conditions: «transparen-

---

[806] EUROPEAN COMMISSION (2011): *Op. cit.*

cy», «legitimacy» of purpose and «proportionality»[807]. «Transparency» means that a person is explicitly informed of the specific purpose when their personal data is processed. «Legitimacy» of purpose means that the purposes for which personal data are processed are legitimately related to the business needs of the data controller. «Proportionality» means that personal data must be processed only to extend compatible with the explicitly stated purpose[808]. «Informed consent» comes to fulfil these three requirements, therefore most probably new Data Protection Regulation will include this measure.

This implementation is a technical tool aimed to explain users how their data will be used and with whom will be shared, as well as the use given by third companies' applications. In other words, it is an imposition upon actors who collect or use information to provide and explain users the purposes of such data collection and how they will manage it[809]. After receiving the information, users being aware of the possible consequences of disclosing personal data on the Internet (informed) are supposed to be capable of deciding whether they display personal information or not (consent).

The implementation of «informed consent» may prevent people from suffering much of the privacy violations they experiment when interacting with some ICT, in particular as far as SNS are concerned. Among them Facebook, created in 2004 by Mark Zuckerberg, has received criticism on a wide range of issues relating to privacy, including targeting and tracking down users and using tricky privacy policies. Besides, there is a huge amount of research showing that users do not understand completely the implications of some actions even after having read security dialogs and warnings, usually due to the misleading statements writing on these texts.

For that reason and to verify the efficiency of «informed consent», it should be obtained in such a way as to ensure that users know exactly what they are consenting to. Therefore, it has to be easy enough to be understood by the whole audience in contraposition to those

---

807 European Parliament and the Council of the European Union (1995) «Directive 95/46/EC», *Official Journal of the European Union*, L 281, 0031-0050.

808 Ídem.

809 NISSSEMBAUM, H. and BAROCAS, S. (2009): *Op. cit.*

illegible privacy policies or the current SNS «Terms of Use» written in a tricky and complex language.

4.2 PASSIVE «INFORMED CONSENT» OR «OPT-OUT» MODEL REGIME

The moral legitimating of informed consent stems from the belief that it respects individual autonomy, specifically, that it reflects rational and informed decisions as far as the manage of personal data is concerning. If the social contract signed by all the actors involved in the digital world become a moral imperative to certificate a correct functioning of the ICT[810] it seems to be logical that a tool to give freely and informed permission might solve the majority of the privacy infringements produced.

Nonetheless, much of the controversy that surrounds «informed consent» derives from the competing views of the proper implementation of this tool. This controversy refers to hegemonic approach to informed consent as an «opt-out» model, forming it as a defensive tool based on a passive role of users. That really means that it is the user who constantly is forced to refuse the permission in order to prevent their data from being public whilst, at the same time, default settings provide the minimum level of protection. Accordingly, «opt-out» model is based on a notion of passive consent with opportunities for revocation and users are forced to deny predefining actions which aim to confer the higher level of visibility to their data. In light of this fact, it seems clear that «opt-out» models are though to give users false expectations of privacy control. Hence, this passive consent is, in all likelihood, a tricky *manoeuvre* carried out by Internet companies to extend the mistaken belief that people have informational self-determination.

We have mentioned many examples of this fact on *Chapters VI*, *VII* and *VIII*. For instance, on its implementation over Facebook's Beacon, «opt-out» regimens were also a factor for controversy. Beacon was a part of Facebook's advertisement system which worked sending data from external Websites to Zuckerberg's SNS, for the purpose of allow-

---

[810] MASON, R. O. (1986): *Op. cit.,* p. 11.

ing targeted advertisements. The system reported to Facebook on its member's activities on third party sites that also participated. As a result, this Facebook's advertisement program announced to one's friend what one had just bough using «opt-out» model to agree o decline permission. However, if users had forgotten to deny sharing something, the application still went ahead and shared it with their friends[811].

These reasons come to underline the fact that thought «informed consent» might assure a safer navigation as far as ICT are concerned, it is fundamentally inadequate under the technical conditions that it currently holds. Consequently, we must rethink this tool which could become much more effective under a necessary redefinition and working in conjunction with the implementation of «privacy by default».

4.3 PRIVACY BY DEFAULT AND ACTIVE INFORMED CONSENT

«Privacy by design» means that data protection is designed into the development of business processes for products and services and therefore, privacy settings are set at a high level «by default»[812]. Within this framework, «informed consent» would be improved as an «opt-in» model and under the conditions we suggest in the following lines.

4.3.1 **Privacy by default / by design**

«Privacy by design» and «privacy by default»[813] means that privacy safeguards will have to be integrated into products as they are developed - an approach to systems engineering which takes privacy into account throughout the whole engineering process- as well as in social networking, the default settings must protect the privacy of individuals. The concept was originated in 1995, in a report on «Privacy Enhancing

---

811 JOHNSON, D. (2009): *Op. cit.,* p. 104.

812 European Commission (2012): *Op. cit., Proposal for a Regulation.*

813 We use the expression «privacy by design» when we refer to the industry and «privacy by default» relating to users.

Technologies» by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organization for Applied Scientific Research[814]. «Privacy by design», which framework was developed by Dr. Ann Cavoukian, the former Information and Privacy Commissioner of Ontario, starts from the point that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation[815]. In October 2010, this new framework was recognized as the global privacy standard in a landmark resolution by the International Conference of Data Protection and Privacy Commissioners in Jerusalem.

«Privacy by design», which is already mentioned as an innovative principle in the new EU Draft Data Protection Regulation, means that data protection safeguards should be built into products and services from the early stage of development and privacy-friendly default settings should be the norm, for instance, on SNS. This change would strengthen individual's right to privacy and control over personal data in a practical way, since all the applications would provide, by design, the higher level of protection. In this context, it is the user who decides whether to change or not predefined settings depending on their desires for privacy or their needs for social interaction.

4.3.2 **Active informed consent or «opt- in» model**

To embed privacy-friendly standards by design would avoid some of the most dramatic infringements taking place as, for instance, the automatic index of personal information by search engines without users' permission. Additionally, in the new scenery created by «privacy by design», the «informed consent» system would be improved as «opt-in» model, thus returning to users the active role in their privacy

---

814 HUSTINX, P. (2010): «Privacy by design: delivering the promises», in *Identity in the Information Society*, vol. 3, n. 2, pp. 253-265, p. 253.

815 CAVOUKIAN, A. (2009): *Privacy by Design*. Office of the Information and Privacy Commissioner. Available at: http://www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf [3/10/2014].

protection. It suggests that less effort is required of users who would not find themselves forced to deny permission whenever they post personal information. On the contrary, consent would be required only in those cases when they decide to confer more visibility to their data.

«Opt-out» regimens come to justify the use of personal data by SNS rather than providing users with control over their data. By implementing «opt-in» models, however, it is the user, from the very beginning, who controls whether to give visibility to their data or not — that is why it is also known as «active consent». As Deborah Johnson states, the use of «opt-in» rather than «opt-out» goes hand in hand with transparency, treating us as rational beings capable of making decisions, rather than passive objects to be manipulated:

> Given how little information consumers, clients and citizens have about information practices, the «opt-out» strategy seems unfair if not deceptive. Personal information is gathered and used and if we figure out what is happening we can opt-out. By contrast, if organizations cannot use personal information about us unless they get our permission, then they have to inform us of their practices and convince us that we want to opt-in[816].

Currently, no SNS has implemented «informed consent» as active or «opt-in» regime; not even it is mentioned in the existing legislation. However, in this research, we make a case for the implementation of this system which could become a useful tool to both protect users' privacy and to confer a control over their personal data. In the following pages, we will show in which ways it could be brought into play to fulfil users' informational determination requirements.

4.3.3 **Active «informed consent» by layers**

One of the main shortcomings we find when implementing informative tools such as «informed consent» is how to provide users with enough easy-to-understand information to illustrate them with the possible repercussions of giving more visibility to their data. In addition to this, we must reflect on how to proportion such information in a comfortable way. For these reasons, we recommend a system of informative

---

[816] JOHNSON, D. (2009): *Op. cit.*, p. 105.

layers which would emerge only in case of changing predefined settings for more visibility, warning users about the possible repercussions. This system with layers is already in use to agree or deny permission regarding the cookies, but has never been applied to consent.

4.3.4 **Design heuristics**

For user competence to be possible they need to know where and which of their data are being stored and what the consequences for their privacy maybe. To accomplish these requirements, the informed consent system we propose would work in two informative layers that would appear automatically. Each layer will show as many levels and cases as possible actions the user might carry out in each concrete context, thus supplying them with information and illustrating examples about the likely repercussions. In developing this approach, the information provided by layers would appear in the following way:

First layer: Basic Information (schematic)		**Second layer: Further Information (simulation of consequences)**
• The purpose of data collection:	–how data will be used –how long it will be stored –where will be stored	Depending on the level of visibility chosen by the user, it would emerge an informative layer showing the further consequences of giving more publicity to their data. Illustrating examples would be provided and there will be an explanation of how to deny any action.
• Property rights involved:	–how the property of information will change –how to exercise their right to access to their own information	
• Data collected by cookies	–how data will be used –how long it will be stored	
• Data collected by third companies:	–data shared when using applications –how data will be used	
• Privacy protection and others' actions:	–public indexations –how user's data will be showed to others	
•*How to turn down actions previously taken*		

Table 10.1 Informed consent by layers[817]

[817] Source: the author.

To fulfil users' mental models, the cases explained on first layer would be completed with more potential sceneries depending on the level of visibility users have decided to confer to their data. This information would be enunciated via propositions:

«When you activate this setting/control.... you consent that…»

«If you permit this action..... you consent that…»

To supply users with illustrating examples from layer two we could bring into play not only text, but preferably interfaces created by simulation programs to explain, in a more visual way, how our data would be shown to others or how it may be used by third parties. As an example we make mention of simulation programs like those developed by Hether Lipford in University of North Carolina at Charlotte[818]. However, there are many other examples of simulation software we could bring into play on layer two.

4.3.5 **Enhancing usability**

«Informed consent» application should be illustrated using specific colours and icons to facilitate users to identify the potential risks that a change for more visibility may involve, as well as to help them to internalize these processes. In addition, the application would save a file recording the actions formerly taken, such as previous settings or prior actions details. This file aims to remind them which data was made public thus avoiding users feeling forced to rely on their own memory for something the system already knows. Additionally, the interface may provide, automatically, visual cues, reminders, lists of choices and other aids. We can not forget that humans' brain works better with recognition than recall and by choosing to be consistent with references an interface can be made easier to learn. Consequently, the disclosure of images and concepts users already know and recognize would contribute to make them feel comfortable with any action taken. Nonetheless, if user's actions cause not expected outcomes, it would be possible to turn it down -users feel more comfortable with interfaces in which their actions do not cause irreversible consequences. Let see an example of how it works:

---

[818] LIPFORD, H. (2010): *Op. cit.*

As we mentioned before, this informed consent model would work together with «privacy by default». Within this framework, it is the user who consciously decides whether or not to change by design settings in order to confer more visibility to their data. For instance, a user who posts a photograph on a SNS might decide to change provided privacy settings from «only visible to me» —which in fact would be the default setting with privacy by design— to «visible to my friends», «visible to some friends» or even to «public to all the people».

At that moment, it would emerge a first layer of information indicating the likely repercussions this action may involve. Then, users would have three ways of action:

(1) To assume the possible outcomes of changing their privacy protection level and agree the consent;

(2) To deny consent;

(3) To continue to the second layer to obtain more information.

And the same sequence would be repeated on the second layer. Some users confer less protection to their data. This is because they do not think there is a good reason to hide it or they feel there will not be regrettable consequences. In those cases, whenever users decide to change for a higher level of visibility, they will receive much more information than at lower visibility levels - more visibility involves more risks; therefore, a larger amount of information is needed.

In a schematic diagram, the actions to be taken by users when modifying by default settings would be shown as a vector going from the inside to the outside of several concentric circles, from the maximum level of protection to the minimum at any time users decide to confer more visibility to their data.

4.4 LIMITATIONS

> [A]nyone who has studied the history of technology knows that technological change is always a Faustian bargain: Technology giveth and technology taketh away, and not always in equal measure. A new technology sometimes creates more than it destroys. Sometimes, it destroys more than it creates. But it is never one-sided[819].
>
> Neil Postman

As far as the preservation of personal data is regarded, we must admit that there are no catch-all solutions even using «informed consent». Taking this into account, we must outline the following drawbacks:

4.4.1 **Users' contradictory behaviour towards privacy protection**

Commonly, when we examine the relation between supplying users with information and its impact on their decisions, we observe contradictory behaviours towards protection. According to the authors reviewed on *Chapter IX,* it is not always the expectation of privacy what motivates users' actions when surfing the Web, let alone on SNS. To begin with we have mentioned how users are currently willing to share large amounts of personal information and giving up the control over it[820]. Additionally, it has been already observed the phenomena known as the «privacy paradox» which involves users' paradoxical behaviour relating to privacy concerns on SNS[821]. Moreover, the majority of concerns users showed were not about control over personal data: they showed regrets when there had been a possible breach in reputation[822]. From another perspective, we must point out that «privacy by default» seems to be a highly effective tool. However, relating to «informed consent» we find problems of under-

---

819 POSTMAN, N. (1990): *Informing Ourselves to Death, Address before the German Informatics Society.* Available at http://www.eff.org/Net-culture/Criticisms/informing__ourselves-to-death.paper.

820 WESTER, M. and Sandin P. (2011): *Op. cit.,* p. 90.

821 BARNES, S. B. (2006): *Op. cit.*

822 LAMPE, C., ELLISON, N. B., and STEINFIELD, C. (2008): *Op. cit.,* MADDEN, M. & SMITH, A. (2010): *Op. cit.,* YOUNG, A. L. and QUAN-HASSE, A. (2013): *Op. cit.*

standing as far as children and young people are regarded. This is because the complex sceneries which may appear turn into a difficult task to translate into a simple language the stunning array of potential risks and its further repercussions to those ranges of people. And the same would happen with those so called «digital outsiders».

4.4.2 **Legal limitations**

As far as responsibility and accountability for those processing personal data are concerning, new Draft European Data Protection Regulation introduces a notably innovation: European citizens will be able to refer cases where their data has been breached or rules on data protection violated to the Data Protection Authority in their country, even when it is processed by an organization based outside the EU. Additionally, this set of rules will apply even if personal data is processed abroad by companies that are active in the European Market. Nevertheless, there is no explicit mention relating to the use of «informed consent» or «privacy by default» if an enterprise is based outside the EU as it is the case of the majority of SNS. And taking into account that SNS platform businesses depend on collecting as much as possible information from users to target them -and even to track them down- it is unlikely they will be willing to support a measure which would most probably damage their business model.

In this context, despite the Data Commissioner claiming that new EU rules will apply even if personal data are processed abroad by companies which are based on the European Market[823] there might probably be disputes over competences and attributions of each jurisdiction. SNS and other Internet companies may allege that if their main headquarters are based on the United States they are force to act within the US normative framework which tends to be laxer when it comes to the protection of privacy. There should be, in this case, overlapping of competences, functions and powers between jurisdictions.

---

[823] European Commission (2012): *Data protection reform: Frequently asked question. Why do we need to reform the EU data protection rules?* Available at: http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=fr [12/02/2014].

In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. Instead, the US has a patchwork system of federal and state laws, and regulations that overlap, dovetail and may contradict one another. In addition, there are many guidelines, developed by Governmental Agencies and industry groups that are not legally enforceable but are part of self-regulatory efforts and are considered best practices. Among this myriad of regulations, there is no outlook of implementing «informed consent». Furthermore, the many legal gaps which exist and the fact that data protection is, by far, much laxer than in Europe could benefit the business model of SNS platforms.

In fact, in spite of the many petitions from the National Data Authorities, administrations and other institutions in order to clarify which data collect and for which purposes, there is, as yet, no uniformity in how many and what kind of data capture companies like Facebook —and not only Facebook—; after several requirements from the United States Authorities as well as some governments in Europe, powerful enterprises such as Google have never clarified the kind and amount of data they collect. Under such conditions, therefore, the implementation and correct functioning of «informed consent» would turn into an impossible task. Nevertheless, in the case of those companies such as Facebook which have opened headquarters in Europe, they are forced to collaborate with European Data Authorities.

4.4.3 **Conceptual limitations: consent and the information of others**

One of the main challenges for our privacy since the arrival of SNS is the possibility of being damaged by other's action. This is prone to happen as a result of the lack of control over personal data that the use of such tools involves. Consequently, when sharing information on SNS, «it is not only necessary to consider the privacy of, but the privacy of the information of others who may be tied to the information being shared» [824]. The digital landscape with its ever-increasing ability to capture, compute and communicate data facilitate

[824] PARRISH, J.L. (2010): *Op. cit.,* p. 190.

that the contents we put on the SNS may involve other's personal information. In this case, «informed consent» might not be a suitable tool to prevent the countless data breaches produced by other's sharing data since it refers, by essence, to one's actions, that is to say, to one's decisions and self-informative determination.

Following this line of reasoning and taking into account Parrish reflections on social contracts that may govern actions in the interconnected world, we must admit that even using «informed consent» the expectation of whole control over data is not always valid.

Parrish illustrates this problematic with the following example:

> Imagine that an individual takes pictures at a private social gathering and posts them on a SNS. What if a member […] who is pictures in those images deactivates their account? Do they disappear from the images? […] Furthermore, what are the chances the person posting in the pictures provides informed consent to every individual captures in the images? What about those individuals who indicate what others are doing in their status updates, do they provide informed consent?[825].

The practical implications of revealing personal data about oneself and others extend beyond immediate impact in virtual world and when information is released on the SNS it is difficult to regain control over. In addition, as it becomes opaque to what extend their personal data are on the Internet, this information could build a dossier of people even if they decide not to participate in the digital world.

4.4.4 **Technical limitations**

There are, of course, certain technical features that limit the efficiency of this application. The technical shortcomings refers, mainly, to the diversity and amount of potentially dangerous context that may appear in some moments as, for instance, when registering into a SNS, posting or sharing a photograph, especially if it involves tags relating to others. The amount of information the user might receive in that moment may be excessive and the quantity of layers which might appear could discourage users from using that service. This complexity might well go further especially as far as users with mo-

---

[825] Ibídem, p. 189

bile devices are concerned, for that reason we must face the challenge of how to provide large amounts of information in smaller interfaces, whilst being highly illustrative at the same time.

To sum up, the main drawback we have to face is the difficulty to explain exactly to what extend users personal data may be used, that is to say, which are the concrete implications of giving more visibility to their personal data or using some applications. In line with Nissenbaum and Barocas' argumentations, this tool might not be enough to confer informed permission in all cases since «it attempts to render participation a matter of choice, but generally fails to explain whether a user agrees to tracking, targeting or both» [826]. Finally, it may pose a real challenge to develop this system since the majority of SNS enterprises rarely contribute to clarify how they manage users' information.

5. FINAL CONCLUSION

Despite disclosing information on the Internet -including personal data- is an increasing part of modern life, it is necessary to ensure that personal data are protected in a way that does not prevent users from using ICT. In this context, this thesis has portrayed the main risks SNS may involve for users' privacy by exploring the flows of information behind most popular Web 2.0 services and evaluating this flows subsequently through the lenses of Nissenbaum's contextual integrity framework. As a result, we have verified that currently users are not capable of protecting their privacy since they do not understand the attributions of digital context shaped by informational flows on SNS. Moreover, as they cannot apply the norms of contextual integrity they have no control over their personal data.

In light of these findings, it seems clear that users' knowledge is a key concept to carry out informed decisions on SNS. That is to say, for user competence to be possible, they need to know which of their data are being collected and what the consequences for their privacy are. Once they understand the possible repercussions, they are capable of making conscious decisions relating to their expectations for

---

[826] NISSSEMBAUM, H. and BAROCAS, S. (2009): *Op. cit.*

privacy, defining and configuring their preferences. Thus, education to improve users' knowledge may contribute to strengthening their informational self-determination, giving them the capacity of deciding whether to post their personal data or not.

Concerning regulation, to guarantee the right to privacy in the future and focusing on the importance of giving more control to users, the European Commission's proposals update and modernize the principles enshrined in the 1995 Data Protection Directive underlining explicitly «privacy by default» and «informed consent» as essential tools to preserve users' privacy.

The development of «informed consent» is particularly important since it would offer users a reasonable degree of privacy and control over data, as well as confidence that their interaction with digital media may not involve unexpected repercussions. In line with it, our proposal contributes to conceptualize «informed concept» as «opt-in» model by layers with a view to informing a future prototype. Its implementation under the conditions explained above offers flexibility with respect to other tools and, furthermore, interoperability with respect to existing «privacy by design». To fulfil all the requirements, «informed consent» as a privacy-friendly design would clearly call for users' decisions and degrees of opting-in should support users' needs for informational autonomy, in getting out of the trap of submitting all their personal data as a trade-off for functionality.

We must underline, however, the complexities of digital environments have to be taken into account when designing protection strategies, especially pointing at such described shortcomings which may obscure the process of implementation. Still, supplying «informed consent» should not absolve digital platforms, third parties or other agents involved of their responsibilities.

The implementation of afore-mentioned measures in conjunction with regulation is needed not only to define responsibilities but to promote a safer navigation —as a collective good it is, safety becomes necessary for the development of a democratic society—. Consequently, supplying users with required flows of information to improve their understanding of digital environments as well as implementing «informed consent» may help to provide them the suitable

critical framework they may need to carry out their decisions and, therefore, their informational self-determination desires.

These premises are in tune with the majority of recommendations for regulation suggesting the main principles the preservation of privacy might involve: a complex approach that combines education and good practices with appropriate legislation and technology, in such a way that this choice becomes possible. Taking into account that it is the citizen the main actor of the digital revolution, all the agents involved, that is to say, authorities, enterprises and institutions are duty bound to improve this changes to protect our privacy. And this is not a minor issue: these technologies have become, nowadays, the most important instrument to obtain and spread information and, therefore, its correct use is a key concept to promote and preserve the values of a democratic society.

We expect the findings and proposals of this research had managed to supply viable solutions both for users to improve their privacy needs and to promote a safer use of Information and Communication Technologies.

BIBLIOGRAFÍA Y FUENTES DOCUMENTALES

ABSTRACT

ARENDT, H. (1958): *The human condition*. Chicago: The University of Chicago Press.

BARNES, S. B. (2006): «A privacy paradox: social networking in the United States», *First Monday*, vol. 11, n. 9. http://firstmonday. org/ojs/index. php/fm/article/view/1394/1312

BOYD, D. (2006): «Friends, friendsters, and myspace top 8: writing community into being on social network sites», *First Monday*, vol. 12, n. 11. Available at: http://www. danah. org/papers/FriendsFriendsterTop8. pdf.

— (2008): «Why youth (heart) social network sites: the role of networked publics in teenage social life», in *Youth, Identity, and Digital Medias*, D. Buckingham (ed.): Cambridge, MA: MIT Press, pp. 119-142.

BOYD, D. and ELLISON, N. B. (2007): «Social Network Sites: Definition, History, and Scholarship» in *Journal of Computer-Mediated Communication*, vol. 13, n. 1, pp. 210-230.

BUCHMANN, J. (ed.) (2013): *Internet Privacy: Taking opportunities, assesing risk, building trust* (Acatech – Deutsche Akademie der Technikwissenschaften, acatech STUDY) Heidelberg *et al.:* Springer Verlag.

CHEW, M., BALFANZ, D. and LAURIE, B. (2008): «(Under)mining Privacy in Social Networks». Available at: http://w2spconf.com/2008/papers/s3p2.pdf. Under mining privacy.

DEBATIN, B., LOVEJOY, J. P., HORN, A. K. and HUGHES, B. N. (2009): «Facebook and online privacy: attitudes, behaviors, and unintended consequences», in *Journal of Computer-Mediated Communication*, vol. 19, n. 2, pp. 83-108.

GOVANI, T. and PASHLEY, H. (2005): «Student awareness of the privacy implications when using Facebook», *Privacy Poster Fair at the School of Library and Information Science*, Pittsburgh: Carnegie Mellon University.

HABERMAS, J. (1989): *The structural transformation of the public sphere: An inquiry and category of bourgeois society.* Cambridge: Polity.

LENHART, A. and MADDEN, M. (2007): «Teens, privacy & online social networks: how teens manage their online identities and personal information in the age of myspace», in *Pew Internet & American Life Project, Washington,*

DC. Available at: http://www.atg.wa.gov/uploadedFiles/Another/Office_Initiatives/Teens, Privacy%20and%20Social%20Networks.pdf

LIPFORD, H. R., WISNIEWSKI, P., LAMPE, C., KISSELBURGH, L. and CAINE, K. (2012): «Reconciling Privacy with Social Media», in *Proceedings of the 2012 ACM Conference on Computer Supported Corporative Work Companion*, pp. 19-29.

MADDEN, M. and SMITH, A. (2010): «Reputation management and social media», in *Pew Internet & American Life Project*, Washington. Available at: http://www.pewinternet.org/2010/05/26/reputation-management-and-social-media/

NISSENBAUM, H. (2004): *Privacy as contextual integrity*. Washington Law Review, n. 79, vol. 1, pp. 119-158.

— (2010): *Privacy in context: Technology, policy and integrity of Social Life*. Standford, CA: Stanford University Press.

— (2011): «A Contextual Approach to Privacy Online», in *Daedalus*, vol. 140, n. 4, pp. 32-48.

NISSENBAUM, H. and BAROCAS, S., (2009): «On Notice: The Trouble with Notice and Consent», in *Media, Culture, and Communication*. New York: New York University.

NORBERG, P. A., HORNE, D. R. & HORNE, D. A. (2007): «The privacy paradox: personal information disclosure intentions versus behaviors», en *Journal of Consumer Affairs*, vol. 41, n. 1, pp. 100-126.

POLLER, A., KRAMM, A. and ILYES, P. (2013): «Designing privacy-aware online social networks –A reflective socio-technical approach», in *CSCW'13 Measuring Networked Social Privacy Workshop*, February 23-27, 2013, San Antonio, Texas, United States. Available at: http://testlab.sit.fraunhofer.de/downloads/Publications/poller_osn_design_cscw13_workshop_camera_ready_rot.pdf.

SOLOVE, D. J. (2007): «"I've Got Nothing to Hide" and other misunderstandings of privacy», in *San Diego Law Review*, n. 44, pp. 745-772.

STUTZMAN, F., CAPRA, R. & THOMPSON, J. (2011): «Factors mediating disclosure in social network sites», *Computers in Human Behavior*, vol. 27, n. 1, pp. 590-598.

SUNDÉN, J. (2003): *Material Virtualities: Approaching Online Textual Embodiment*, New York: Peter Lang.

THOMPSON, J. B. (1995): *The media and modernity: A social theory of the media*. Cambridge: Polity.

TUFECKI, Z. (2008): «Can you see me now? Audience and disclosure regulation in online social network sites», in *Bulletin of Science, Technology and Society*, vol. 28, n. 20, pp. 20-36.

WARREN, S. & BRANDEIS, L. D. (1890): «The right to privacy», *Harvard Law Review*, n. 4, pp. 193-219.

YOUNG, A. L. and QUAN-HASSE, A. (2013): «Privacy protection strategies on Facebook», in *Information, Communication and Society*, vol. 16, n. 4, pp. 479-500.

CAPÍTULO I

Bibliografía:

BAUMAN, Z. (2003): *Modernidad líquida*. México DF: Editorial Fondo de Cultura Económica.

CASTAÑARES, W. (2011): «Realidad virtual, mimesis y simulación», en *Cuadernos de Información y Comunicación*, vol. 16 59-81.

CASTELLS, M. (2001): *La galaxia Internet,* Barcelona: Areté.

CASTELLS, M. (1997): *La sociedad red*, Madrid: Alianza Editorial.

CASTELLS, M. (1998): *La era de la información. Economía, sociedad y cultura, Vol. III*, Madrid: Alianza.

HERREROS, C. (2010): *Desarrollos del periodismo en Internet,* Zamora: Comunicación Social Ediciones y Publicaciones.

MACHADO, A. (2009): *El sujeto en la pantalla. La aventura del espectador, del deseo a la acción*. Barcelona: Gedisa.

MORIN, E. (1990): *Introducción al pensamiento complejo*. Barcelona: Gedisa.

NISSENBAUM, H. (2004): «Privacy as contextual integrity», en *Washington Law Review*, vol. 79, n. 1.

ORWELL, G. (2009): *1984*. Barcelona: Ediciones Destino.

UNESCO (2005): *Hacia las sociedades del conocimiento*. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Disponible en: www.unesco.org/publications.

WOLTON, D. (2000): *Internet, ¿y después?: una teoría crítica de los nuevos medios de comunicación,* Barcelona: Gedisa.

Bibliografía sobre técnicas de investigación:

KRIPPENDORFF, K. (1990): *Metodología de análisis de contenido*. Barcelona: Paidós Ibérica.

LUNA CASTILLO, A. (1996): *Metodología de la tesis,* México: Trillas.

ROJAS SORIANO, R. (1977): *Guía para investigaciones sociales*. México: UNAM.

WOLF, M. (1987): *La investigación en comunicación de masas*. Barcelona: Paidós.

Webgrafía:

«NUMBER OF WORLD INTERNET USERS (2014)», en *Internet Live Stats*. Disponible en: www.internetlivestats.com/internet-users.

Páginas Web de Instituciones y autoridades referidas:

CAPURRO FIEK FUNDATION: www.capurro-fiek-stiftung.org

CENTRE FOR COMPUTING AND SOCIAL RESPONSIBILITY, De Montfort University. http://www.dmu.ac.uk/research/research-faculties-and-institutes/technology/centre-for-computing-and-social-responsibility/ccsr-home.aspx

DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN: www.acatech.de

EUROPEAN CENTER FOR SECURITY AND PRIVACY BY DESING (EC SPRIDE) en su Web: www.ec-spride.tu-darmstadt.de

ETHICS AND COMPUTER INTERNATIONAL CONGRESS (ETHICOMP): https://ec.europa.eu/digital-agenda/en/news/ethicomp-2015

JAMES FOWLER: www.fowler.ucsd.edu

INSTITUTO FRAUNHOFER PARA LA SEGURIDAD DE LA INFORMACIÓN (SIT). https://www.sit.fraunhofer.de/

INSTITUT FÜR KULTURANTHROPOLOGIE UND EUROPÄISCHE ETHNOLOGIE, Goethe-Universität Frankfurt am Main, se puede consultar su página Web: www.uni-frankfurt.de/39023844

UNIVERSIDAD DE LOS MEDIOS DE STUTTGART: www.hdm-stuttgart.de/

STEINBEIS TRANSFER INSTITUT INFORMATION ETHICS (STI-IE): http://sti-ie.de

CAPÍTULO II

Bibliografía:

ABBAGNANO, N. (1980): *Diccionario de Filosofía*, México: Fondo de Cultura Económica.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2009): *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Documento en línea: https://www.agpd.es/portalWebAGPD/canaldocumentacion/publicaciones/common/Estudios/est_inteco_redesso_022009.pdf.

ARENDT, H. (1958)*: The Human Condition*, Chicago: University of Chicago Press.

BADÍA, E. (2012): «Marco conceptual. Derecho ¿pendiente?», en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados*. Madrid: Ariel.

BÉJAR, H. (1988): «Privacidad», en *Terminología científico social. Aproximación científica*. Barcelona: Antrophos, pp. 785-787.

— *El ámbito íntimo: privacidad, individualismo y modernidad*, Madrid: Alianza.

BOBBIO, N. (1987) *The future of democracy: A defence of the rules of the game*, Cambridge: Polity Press.

— (1989): *Democracy and Dictatorship. The nature and Limits of state power.* Cambridge: Polity Press.

BOIX REIG, J. (1983): «Consideraciones sobre la protección penal de la intimidad y del honor e informática», en *Anales de la Universidad de Alicante. Facultad de derecho,* n. 2.

CHOZA ARMENTA, J. (1980): *La supresión del pudor y otros ensayos*. Pamplona: Eunsa.

COOLEY, T. M. (1895): *A treatise on the Law of Torts*. Chicago: Callaghan and Company.

CURRY, M. R. (2002): «Discursive displacement and the seminal ambiguity of space and place», en Lievrouw L. A. y Livingstone S. (eds.): *The handbook of New Media*, London: SAGE Publications, p. 502-517.

DE LA VÁLGOMA, M. (1983): «Comentario a la ley orgánica de protección civil al honor, a la intimidad y a la propia imagen», en *Anuario de Derechos humanos*.

DESANTES GUANTER, J. M. (1972): «Intimidad e información, derechos excluyentes», en *Nuestro tiempo*, n. º 213. Pamplona.

DESANTES GUANTER, J. M. y SORIA, C. (1991): *Los límites de la información. La información en la jurisprudencia del Tribunal Constitucional: las 100 primeras sentencias*. Madrid: Asociación de la Prensa de Madrid.

DUBY, G. (1987): «Preface» en Veyne, P. (ed.): *A history of Private Life*. Cambridge y Londres: Harvard University Press.

FAYOS GARDÓ, A. (2000): *Derecho a la intimidad y medios de comunicación*. Madrid. Centro de Estudios Políticos y Constitucionales.

GARCÍA FERNÁNDEZ, D. (2010): «El derecho a la intimidad y el fenómeno de la extimidad», en *Dereito*, vol. 19, n. º 2, 269-284.

GARCÍA MORENTE, M. (1972): *Ensayo sobre la vida privada*. Madrid: Universidad Complutense.

GARCÍA SAN MIGUEL, L. (1992) *Estudios sobre el derecho a la intimidad*. Madrid: Tecnos.

GIDDENS, A. (1990): *Modernity and self-identity.* Cambridge, United Kingdom: Polity Press.

GONZÁLEZ GAITANO, N. (1990): *El deber de respeto de la intimidad. Información pública y relación social,* Pamplona: Eunsa.

— «¿Deber de respeto a la intimidad o derecho a la intimidad?» en Innerarity, D. y Vaz, A. (ed.) (1987): *Información y derechos humanos. Actas de las I Jornadas de Ciencias de la Información.* Pamplona: Eunsa, pp. 129-140.

GOULDNER, A. (1967): *The dialectic of Ideology and technology.* New York: Seabury Press.

GRONAU, K. (2002): *Das Persönlichkeitsrecht von Personen der Zeitgeschichte und die Medienfreiheit.* Nomos: Baden-Baden.

HABERMAS, J. (1987): *The Theory of Communicative Action*, vol. 2, Boston: Beacon Press.

— (1989): *The structural transformation of the public Sphere: an inquiry into a category of Bourgeois society,* UK: Cambridge Polity Press.

HUBMANN, H. (1957): «Der zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion», en *Juristenzeitung*, pp. 521-528.

LAÍN ENTRALGO, P. (1985): *La intimidad del hombre. Homenaje a Antonio Maravall.* Madrid: Centro de Investigaciones Sociológicas.

LYON, D. (1995): *El ojo electrónico: el auge de la sociedad de la vigilancia.* Madrid: Alianza.

MARTÍNEZ, R. (2012): «El derecho a la vida privada en España», en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados.* Madrid: Ariel.

MEDINA GUERRERO, M. (2005): *La protección constitucional de la intimidad frente a los medios de comunicación.* Valencia. Tirant lo Blanch.

MÜNCH, H. (2002): *Freiwillige Selbstkonntrolle beu Indiskretionan der Presse.* Baden- Baden: Nomos.

MURILLO DE LA CUEVA, L. (2003): «La primera sentencia sobre el derecho a la autodeterminación informativa», en *Datos Personales*, *Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n. 1, marzo de 2003. Disponible en: www. datospersonales. org.

NEBEN, G. (2001): *Triviale Personenberichterstattung als Rechtsproblem.* Berlin: Duncker & Humblot.

ORELLANO, W. (2008): «La transmisión y protección de los datos personales y la privacidad en los blogs», en Flores Vivar Jesús (ed.): *Blogogalaxia y periodismo en red: estudios, análisis y reflexiones.* Madrid: Fragua, pp. 261-267.

PROSSER, W. L. (1960): «Privacy». *California Law Review*, n. 3.

QUÉRÉ, L. (1992): «L'espace public: de la théorie politique a la metathéorie sociologique», traducción de Castañares, W. y Orellana, R. (1992): «El espacio público: de la teoría política a la metateoría sociológica», en *Quaderni,* n. 18, pp. 1-25.

REDING, V. (2012): «Protección de la privacidad en un mundo conectado. Un marco europeo de protección de datos para el siglo XXI», en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados*. Madrid: Ariel, pp. XVII-XX.

SCHAWRTZ, P. (2012): «Privacidad *online*: planteamientos jurídicos en Estados Unidos y la Unión Europea», en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados*. Madrid: Ariel.

SCHLOTTFELDT, C. (2002): *Die Verwertung rechtswidrig beschaffter Informationen durch Presse und Rundfunk*. Nomos: Baden-Baden.

SENNET, R. (1977): *The fall of public man*. United Kingdom: Cambridge University Press

SHILS, E. (1956): *The Torment of Secrecy: The Background and Consequences of American Security Policies*. London: William Heinemann.

SIMMEL, G. (1986): *Sociología. Estudios sobre las formas de socialización*. Alianza: Madrid.

SOLOVE, D. J. (2006): «A Taxonomy of Privacy», en *University of Pennsilvania Law Review*, vol. 154, n. 3, pp. 477- 561.

— (2002): «Conceptualizing Privacy», en *California Law Review*, vol. 90, pp. 1087-1156. Disponible en: http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2.

THOMPSON, J. B. (1998): *Los media y la modernidad: una teoría de los medios de comunicación*. Barcelona: Paidós.

— (2011): «Los límites cambiantes de la vida pública y la privada», en *Comunicación y Sociedad,* n. 15, enero-junio, Méjico: Universidad de Guadalajara, pp. 11-42.

URABAYEN, M. (1977): *Vida privada e información: Un conflicto permanente*, Pamplona: Eunsa.

VERGARA PARDILLO, A. y MARTÍNEZ PÉREZ, J. (2012) «Modelos reguladores de protección de datos para una era global» en *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados*. Madrid: Ariel.

VIDAL MARTÍNEZ, J. (1980): «La protección de la intimidad de la persona en el ordenamiento positivo español», en *Revista de derecho privado,* julio y agosto, Madrid, pp. 755-774;

WARREN, S. y BRANDEIS, L. (1890): «The right to privacy», *Harvard Law Review*, vol. IV, n. 5, pp. 193-220. Traducción a cargo de Pendás, B. y Baselga, P. (1995): *El derecho a la intimidad*. Madrid: Civitas.

WESTIN, A. (1967): *Privacy and freedom*. New York: Athenaeum.

ZIMMERMAN, D. L. (1983): «Requiem for a heavy weight: a farewell to Warren and Brandeis privacy Tort», en *Cornell Law Review*, n. 68.

Webgrafía:

(2011): «US privacy groups welcome «Do Not Track'», en *Physorg. com*, 9 de mayo de 2011. Disponible en: billphysorg. com/news/2011-05-privacy-groups-track-bill. html. [14/08/2012].

European Commission (2011): *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in theEU. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_ en.pdf.*

Legislación, sentencias, convenios y declaraciones:

CONSTITUCIÓN ESPAÑOLA DE 27 DE DICIEMBRE DE 1978. (2013): Madrid: Editorial Civitas.

AEPD (2003): *Carácter de dato personal de la dirección IP. Informe 327/2003 de la Agencia Española de Protección de Datos 327/2003*. Documento en línea: https://www. agpd. es/portalWebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP. pdf.

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS (1948): *Declaración Universal de Derechos Humanos, (DUDH)*. París, artículo 12. http://www. un. org/es/documents/udhr/law. shtml

ASIA-PACIFIC ECONOMIC COOPERATION PRIVACY FRAMEWORK (2005) Singapur: APEC Secretariat. Disponible en: http://www. apec. org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework. aspx

Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre de 2000 (2000/C 364/01). *Diario Oficial de las Comunidades Europeas* el 18 de diciembre de 2000.

Carta Europea de Derechos del Niño. Resolución del Parlamento Europeo A3-0172/92 de 8 de julio de 1992.

CÓDIGO PENAL (2013): Madrid: Editorial Tecnos (19. ª ed.).

COMISIÓN EUROPEA (2007): *Dictamen 4/2007 sobre el concepto de datos personales*. Grupo de Trabajo del Artículo 29. Documento en línea: https://www. agpd. es/portalWebAGPD/canaldocumentacion/internacional/common/pdf/WP_148_Dictamen_Buscadores_es. pdf

Considerando 17. Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002.

Convenio de Roma para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 4 de noviembre de 1950, Instrumento de Ratificación de 26 de septiembre de 1979.

Convenio del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado el 27 de enero de 1984.

Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, de 23 de septiembre de 1980. http://www.oecd.org/document/18/0,3343, en_2649_34255_1815186_1_1_1_1,00.html.

Directrices para la regulación de los archivos de datos personales informatizados, Adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990.

EU Chapter of Fundamental Rights (2000/C 364/01) de 18 de diciembre de 2000. Disponible en: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Artículo1.

Ley Orgánica 15/1999, de 13 de diciembre, sobre Protección de Datos de Carácter Personal (LOPD).

Pivacy Act. Disponible en: www.epic.org/privacy71974act

Real Decreto 1720/2007, de 21 de diciembre.

STC 254/1988, de 21 de diciembre.

STC 254/1993.

STC 53/1985.

The USA Patriot Act (UPA) de 24 de octubre de 2001. Disponible en: http://www.justice.gov/archive/ll/highlights.htm

CAPÍTULO III

Bibliografía:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) e Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2009): *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes*. Disponible en: www. agpd. es. [29/03/2013].

ALADRO VICO, E. (1999): *Teoría de la información y la comunicación efectiva*. Madrid: Fragua.

ARISTÓTELES (1999): *Política*. Madrid: Espasa Calpe.

ARMAÑANZAS, E., DÍAZ NOCI, J. y MESO, K. (1996): *El periodismo electrónico, información y servicios multimedia en la era del ciberespacio*. Barcelona: Ariel.

BALLESTEROS MOFFA, L. A. (2005): *La privacidad electrónica. Internet en el centro de protección*. Agencia Española de Protección de Datos, Valencia: Tirant lo Blanch.

BARABÁSI, A. -L. (2002): *Linked: How everything is connected to everything else and what it means,* en New York: Plume.

BARNES, J. A. (1954): «Class and Committees in a Norwegian Island Parish», en *Human Relations,* n. 7, pp. 39-58.

BELL, D. (1974): *The coming of post-industrial society: a venture in social forecasting,* New York: Basic Books.

BENITO, Á. (dir.) (1991): *Diccionario de ciencia y técnicas de la comunicación*. Madrid: Ediciones Paulinas.

BERNERS-LEE, T. (2008): *Tejiendo la red*. Madrid: Siglo XXI.

BOYD, D. (2006): «Friendster lost steam. Is myspace just a fad?», en *Apophenia Blog*, 21 de marzo de 2006. Disponible en http://www.danah.org/papers/FriendsterMySpaceEssay.html.

BOYD, D. y ELLISON, N. B. (2007): «Social Network Sites: Definition, History, and Scholarship» in *Journal of Computer-Mediated Communication*, vol. 13, n. 1, pp. 210-230.

BOYD, D. y JENKINS, H. (2006): «MySpace and Deleting Online Predators Act (DOPA)», MIT Tech Talks. Disponible en: http://www.danah.org/ papers/MySpaceDOPA.html.

BRAJNOVIC, L. (1979): *El ámbito científico de la información,* Pamplona: Eunsa.

— (1979): *Tecnología de la información*, Pamplona: Eunsa.

CABERO, J. (comp.) (2000): *las nuevas Tecnologías Aplicadas a la Educación*. Madrid: Síntesis.

CABRERA, M. A. (2000): *La prensa online. Los periódicos en la «www»,* Barcelona: CIMS.

CAMPUZANO TOMÉ, H. (2000): *Vida privada y datos personales. Su protección jurídica frente a la sociedad de la información*. Madrid: Tecnos.

CAPRA, F (2002): *Las conexiones ocultas. Implicaciones sociales, medioambientales, económicas y biológicas de una nueva visión del mundo*. Nueva York: Doubleday.

CASTAÑARES, W. (2012): «Nuevos medios, nuevas sociedades. La investigación en comunicación hoy», en Mirna, M.; Sepúlveda, L. y Garzón, J. A. (ed.): *Convergencia digital y medios de comunicación*. Méjico: Universidad Autónoma de Nuevo León.

CASTELLS, M. (1997): *La sociedad red*, Madrid: Alianza Editorial.

— (2001): *La galaxia Internet,* Barcelona: Plaza & Janés Editores.

CEBRIÁN HERREROS, M. (2005): *Información multimedia*. Madrid: Pearson.

CEBRIÁN, J. L. (1998): *La Red*. Madrid. Santillana.

COBO, J. C. (2005): *Arquitectura de la información y su impacto en la usabilidad de las tecnologías interactivas*. Tesis para obtener el grado de Doctor en Comunicación Audiovisual y Publicidad en la Facultad de Ciencias de la Comunicación de la Universidad Autónoma de Barcelona.

DAVARA RODRÍGUEZ, M. Á. (2001): *Manual de Derecho Informático*. Madrid: Aranzadi.

DE SOLA POOL, I., y KOCHEN, M. (1978): «Contacs and influence», en *Social Networks* n. 1, pp: 5-51.

DREXLER, E. (1991): «Hipertext Publishing and the evolution of Knowledge», en *Social intelligence*, vol. 1, n. 2, pp. 87-120.

ECHEVERRÍA, J. (1994): *Telépolis,* Barcelona: Destino.

— (1995): *Cosmopolitas domésticos,* Barcelona: Anagrama.

— (1999): *Los señores del aire: Telépolis y el Tercer Entorno*. Barcelona: Destino.

EULER, L. (1736): «Solutio problematis ad geometriam situs pertinentis», en *Commentarii Academiae Scientiarum Imperialis Petropolitanae*, vol. 8, pp. 128-140.

FERNÁNDEZ, S. y FUENTES J. F. (dirs.) (2008): *Diccionario político y social del siglo XX español*, Madrid: Alianza Editorial.

FERNÁNDEZ-SHAW BALDASANO, F. (1997): *Cuaderno de bitácora de las telecomunicaciones*. Madrid: Ministerio de Fomento.

FIDLER, R. (1998): *Mediamorfosis. Comprender los nuevos medios*. Buenos Aires: Granica.

FLORES VIVAR, J. (2009): «Nuevos modelos de comunicación, perfiles y tendencias en las redes sociales» [New Models of Communication, Profiles and Trends in Social Networks], en *Comunicar,* vol. 17, n. 33, 2. º semestre, 1 octubre 2009, pp. 73-81.

FLÓRES-VIVAR, J. (2004): «Internet ya es una realidad y la brecha digital, también. Mitos y realidades de Internet en la sociedad», en *A distancia,* UNED, vol. 22, n. 1.

FOWLER, J. y CHRISTAKIS, N. (2010): *Conectados*. Madrid: Taurus.

GARCÍA ESTÉVEZ, N. (2012): *Redes sociales en Internet. Implicaciones y consecuencias de las plataformas 2. 0 en la sociedad*. Universitas: Madrid.

GARCÍA JIMÉNEZ, L. (2008): «Las ciencias de la comunicación a la luz de las nuevas tecnologías: retos para una disciplina de la incertidumbre», en *Global Media Journal Mexico*, vol. 5, n. 10.

GATES, B. (1995): *El camino al futuro*. Madrid: Mcgraw-Hill.

GIBSON, W. (1984): *Neuromancer,* Nueva York. Traducción al castellano (1998): *Neuromante*, Barcelona: Minotauro.

GIL LÓPEZ, E. (2014): *La importancia del derecho de las TIC y su influencia en los Derechos Fundamentales: La colisión entre el Derecho a la Intimidad y el Derecho a la Tutela Judicial Efectiva en la descarga de archivos*. Tesis doctoral inédita dirigida por Rodríguez Baena, L. Universidad Pontificia de Salamanca.

GILLMOR, D. (2004): *We the media: Grassroots Journalism By the People, For the People*. Sebastopol, CA: O'Reilly.

HAYTHORNTHWAITE, C. (2005): «Social networks and Internet connectivity effects», en *Information, Communication & Society*, vol. 8, n. 2, pp. 125-147.

HERREROS, C. (2000): «La información en Red», en *Sphera Pública, revista de ciencias sociales y de comunicación*, pp: 9-28.

HOLTZ-BONNEAU, F. (1986): *La imagen y el ordenador.* Madrid: Fundesco.

Informe Bangemann. Europa y la Sociedad de la Información global (1994). Disponible en: http://www. cyber-rights. org/documents/bangemann. htm.

JOHNSON, D. (2009): *Computer Ethics*. New Jersey: Pearson.

JOYANES AGUILAR, L. (1997): *Cibersoceidad*. Madrid: McGraw-Hill.

KELSEY, S. St., y AMANT, K. (ed.). (2008): *Handbook of Research on Computer-Mediated Communication*. IGI global, pp: 447-498.

KERCKHOVE, D. (1999): *Inteligencias en conexión. Hacia una sociedad de la Web*. Barcelona: Gedisa.

KOCHEN, M. (1989): *The Small World,* Norwood, NJ: Ablex. Disponible en: http://deepblue. lib. umich. edu/bitstream/handle/2027. 42/22688/0000241. pdf?sequence=1.

KROL, E. (1995): *Conéctate al mundo de Internet. Guía y Catálogo*. Méjico: Mc Graw Hill.

LASWELL, H. D. (1948): «The structure and function of communication in society», en L. Bryson (ed.): *The communication of ideas*. Nueva York: Harper, pp. 37-51.

LENHART, A. y MADDEN, M. (2007): «Teens, privacy & online social networks: how teens manage their online identities and personal information in the age of myspace», en *Pew Internet & American Life Project, Washington, DC*. Disponible en: http://www. atg. wa. gov/uploadedFiles/Another/Office_ Initiatives/Teens, Privacy%20and%20Social%20Networks. pdf

LESSIG, L. (2006): *Code and other laws of Cyberspace*, *Version 2. 0*. New York: Basic Books.

LÉVY, P. (2004): *Inteligencia colectiva por una antropología del ciberespacio*. Washington, DC: OPS /OMS.

— (2007): *Cibercultura. La cultura de la sociedad digital*. Barcelona: Anthropos.

LICKLIDER, J. C. R. y TAYLOR, Robert W. (1968): «The computer as Communication Device», en *Science and Technology,* abril. Disponible en: http:// Web.stanford.edu/dept/SUL/library/extra4/sloan/mousesite/Secondary/Licklider.pdf.

LYON, D. (1995): *El ojo electrónico: el auge de la sociedad de la vigilancia*. Madrid: Alianza.

MACBRIDE, S. (1980): *Un solo mundo, voces múltiples*, París: UNESCO, Fondo de cultura económica.

MARTÍNEZ CABIEDES, L. (2002): «Prólogo» en Estévez, J. (ed.) *Periodismo en la Red*, Madrid: Anaya Multimedia.

MARTÍNEZ RAVANAL, V. (2004): *El trabajo en y con las redes*. Chile: Universidad de Chile. Disponible en http://es.slideshare.net/SOCIOLOGA/el-trabajo-en-y-con-las-redes.

MATÍAS, G. (1995): «Telecomunicaciones en el umbral del infolítico, una introducción prospectiva», en *Situación,* número especial. Bilbao: BBV.

MAYANS I PLANELLS, J. (2003): «El ciberespacio un nuevo espacio público para el desarrollo de la identidad local» conferencia inaugural del III Encuentro de Telecentros y redes de Telecentros. Peñafiel. Valladolid, octubre. Disponible en Observatorio para la CiberSociedad: http://www. cibersociedad. net/mayans/.

MILGRAM, S. (1967): «The Small World Problem», *Psychology Today*, Americam Sociological Association, vol. 1, n. 1, mayo, pp. 61-67. Disponible en: http://snap.stanford.edu/class/cs224w-readings/milgram67smallworld.pdf.

MILGRAM, S. y TRAVERS, J. (1969): «An Experimental Study of the Small World Problem Stanley Milgram», en *Sociometry*, vol. 32, diciembre, n. 4. pp. 425-443. Disponible en: http://www.cis.upenn.edu/~mkearns/teaching/NetworkedLife/travers_milgram.pdf.

MITCHEL, J. C. (1969): *Social networks in urban situations*. Manchester: Manchester University Press.

MULTIGNER, G. (1994): «¿Sociedad interactiva o sociedad programada?» en *Apuntes de la sociedad interactiva. Autopistas inteligentes y negocios multimedia*. Cuenca: Fundesco.

NAFRÍA, I. (2007): *El usuario el nuevo rey de internet*. Barcelona: Gestión.

NEGROPONTE, N. (1995): *El mundo digital*. Barcelona: Ediciones B.

ORIHUELA, J. L. (2005): «Apuntes sobre redes sociales» en el *blog ecuaderno,* 19 de julio 2005, en línea http://www.ecuaderno.com/2005/07/19/apuntes-sobre-redes-sociales/.[13/02/2013].

OSUNA ACEBEDO, S. (2012): «Interantes e interactuados en la Web 2. 0», en Aparici, R. (ed.) *Conectados en el ciberespacio*. Madrid: UNED, pp: 135-150.

PARRA VALCARCE, D. y ÁLVAREZ MARCOS, J. (2004): *Ciberperiodismo*. Madrid: Síntesis.

PARRISH, J. L. (2010): «PAPA knows best: principles for the ethical sharing of information on social networking sites», en *Ethics and Information Technology*, vol. 12, n. 2, pp. 187-193.

PISANI, F. y PIOTET, D. (2009): *La alquimia de las multitudes. Cómo la Web está cambiando el mundo*. Barcelona: Paidos ibérica.

RADCLIFE-BROWN, A. R. (1940): «On social Structure» en *Journal of the Royal Anthropological Society of Britain and Ireland*, n. 70, pp. 1-12. Reproducido en Leinhardt's (ed.) (1977): *Social Networks: a developing paradigm*, Nueva York: Academic Press., pp. 221-232. Disponible en http://www.jstor.org/stable/2844197?origin=JSTOR-pdf&seq=1#page_scan_tab_contents.

REQUENA SANTOS, F. (2003): «Orígenes sociales del análisis de redes», en Requena Santos F. (ed.) *Análisis de redes sociales. Orígenes, teorías y aplicaciones*, Madrid: Centro de investigaciones sociológicas, pp. 3-12.

RHEINGOLD, H. (2000): *The Virtual Community.* Cambridge/Londres: MIT Press.

— (2004): *Multitudes inteligentes. La próxima revolución social. La integración tecnológica en la Era Digital*. Barcelona: Icaria Editorial.

— (2008): «Virtual communities-exchanging ideas through Computer Bulletin boards», en *Journal of Virtual Worlds Research,* vol. 1., n. 1, pp. 1-5.

RIZO GARCÍA, M. (2003): «Redes. Una aproximación al concepto», en *Conaculta*, Universidad Autónoma de la Ciudad de México. Disponible en: http://sic.conaculta.gob.mx/centrodoc_documentos/62.pdf.

SAPERAS, E. (1998): *Manual básico de teoría de la comunicación*. Barcelona: Editorial CIMS.

SCHEER, L. (1994): *La Démocratie virtuelle*, París: Flammarion.

SHAYNE, B. y CHRIS, W. (2003): «We Media. How audiences are shaping the future of news and information», en *The media Center.* Disponible en http:// www. hypergene. net/wemedia/Weblog. php.

SUROWIECKI, J. (2004): *Cien mejor que uno: la sabiduría de la multitud o por qué la mayoría es siempre más inteligente que la minoría.* Barcelona: Urano Tendencias.

TAPSCOTT, D. (1998): *Growing up digital: the rise of the Net Generation,* New York: McGraw-Hill.

TERCEIRO, J. B. (1996): *La Sociedad Digital*, Madrid: Alianza Editorial.

TERCEIRO, J. B. y MATÍAS, G. (2001): *Digitalismo*. Madrid: Taurus.

TOFFLER, A. (1980): *La tercera ola plaza*. Madrid: Plaza & Janés.

TOURAINE, A. (1969): *La societé post-industrielle,* París: Denoël-Gonthier.

TREJO DELARBRE, R. (2010): «Internet como expresión y extensión del espacio público», en Aparici, R. (cord.): *Conectados en el ciberespacio,* Madrid: UNED, pp: 93-106.

TREJO DELARBRE, R. (1996): *La nueva alfombra mágica: Usos y mitos de Internet, la red de redes*, Madrid: Fundesco.

UNESCO (1982): *Repercusiones Sociales de la Revolución Científica y Tecnológica*. París.

UNESCO (2005): *Hacia las sociedades del conocimiento*. Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. Disponible en: www.unesco.org/publications.

VELÁZQUEZ ÁLVAREZ, O. A. y AGUILAR GALLEGOS, N. (2005): *Manual introductoria al análisis de las redes sociales Medidas de Centralidad*. México DF: Universidad Autónoma del Estado de México y universidad Autónoma de Chapingo. Disponible en: http://revista-redes.rediris.es/Webredes/talleres/Manual_ARS.pdf

WASSERMAN, T. (2012): «Pinterest is now the no. 3 social network in the U. S», en *Mashable. com*, 6 de abril, disponible en: http://mashable.com/2012/04/06/pinterest-number-3-social-network/ [26/09/2012].

WATTS, D. J. (2004): *Six Degrees*: *The Science of a Connected Age* (Primera edición de 1971). New York: W. W. Norton & Company.

WHITAKER, R. (1999): *El fin de la privacidad: cómo la vigilancia total se está convirtiendo en realidad*. Barcelona: Paidós.

WOLF, M. (1995): «Nuevos medios y vínculos sociales», Revista de Occidente, n. 107-171, pp. 98-105.

WOLTON, D. (2000): *Internet, ¿y después?: una teoría crítica de los nuevos medios de comunicación,* Barcelona: Gedisa.

ZIMMER, M. (2007): «Privacy and surveillance in Web 2. 0: A study in contextual integrity and the emergence of Netaveillance», en *Society for Social studies of Science*. Disponible en: http://www.academia.edu/3943172/Privacy_and_Surveillance_in_Web_2.0_A_study_in_Contextual_Integrity_and_the Emergence_of_Netaveillance.

Legislación, sentencias, convenios y declaraciones:

Directiva 2000/31/CE del Parlamento de Europa y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información.

Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000 relativa a Servicios de la Sociedad de la Información.

Ley 34/2000 de 11 de junio de Servicios de la Sociedad de la Información y Ley 56/2007, de 28 de diciembre de Medidas de Impulso de la Sociedad de la Información.

UNITED NATIONS (UN) (2000): *United Nations Millennium Declaration*. Resolution adopted by the General Assembly 55/2. Chapter III: Development and poverty eradication. Disponible en: http://www.un.org/millennium/declaration/ ares552e.htm.

Webgrafía:

Alexa Internet: http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none.

ANDREWS, M. (2006): «Decoding Myspace», en *U. S. News and World Report*, 18 de septiembre de 2006.

CLINTON, W. J. y GORE, A. (1993): *Technology for America's economic growth. A new direction to build economic strength*, 22 de febrero de 1993. Disponible en: http://ntl.bts.gov/lib/jpodocs/briefing/7423.pdf.[15/02/2011].

EU FP7 ETICA project: Ethical Issues of Emerging ICT Applications, Comisión Europea, dentro del 7. º Progama Marco, de abril de 2009 a mayo de 2011. Más información en: www.etica-project.eu

GERLOFF, K. (2013): «Microsoft desaparecerá en cinco o diez años y Facebook en tres», en *ABC,* Tecnología, 30 de julio de 2013. Disponible en: http://www.abc.es/tecnologia/videojuegos/20130729/abci-microsoft-facebook-euskal-encounter-201307290950.html.[20/12/2013].

LENHART, A., PURCELL, K., SMITH, A. y ZICKUHR, K. (2010): «Social media and young adults», en *Pew Internet and American Life Project*, Washington, DC. Available at: http://www. pewinternet.org/Reports/2010/Social-Media-and-Young- Adults.aspx [14/03/2011].

LEWIS, P. H. (1995): «William Gibson: creador del término Ciberespacio», entrevista a William Gibson en *El País*, 4 de junio de 1995, p. 29. [19/12/2010].

MARTYNIUK, C. (2008): «Antes lo íntimo era secreto, ahora se lo hace público en Internet», en *Diario Clarín, 21 de septiembre*. Disponible en: http://edant.clarin.com/suplementos/zona/2008/09/21/z-01764657.htm.[22/03/2012].

MUÑOZ, R. y RIVIERO, A. (2009): «Twitter no es una red social sino una herramienta de comunicación», en *El País,* 30 mayo de 2009. Disponible en: tecnologia.elpais.com/tecnologia/2009/03/.../12379 73279_850215.html.[22/02/2010].

GARTON, T. (2010): *Facebook: restablecer la privacidad*, en *El País*, 11 de octubre de 2010. Disponible en: http//elpais.com/diario/2010/10/11/ opinion/12867 48 -011_ 850215.html.[04/03/2012]

O'REILLY, T. (2005): «What is the Web 2. 0. Design Patterns and Busines Models for the Next Generation software», en www.oreilly.com, 30 de septiembre de 2005. Disponible en: http://www.oreilly.com/pub/a/Web2/archive/what-is-Web-20.html.[07/02/2011].

Social bakers Facebook statistics. http://www.socialbakers.com/statistics/facebook/

Citas para ilustrar el capítulo:

BORGES, J. L (1975): «El libro de arena», en *Ficciones,* Buenos Aires: Emecé.

GREEN, G. (1951): *The End of the Affair,* Reino Unido: Heinemann.

CAPÍTULO IV

Bibliografía:

BARTH, A. (2006): «Privacy and contextual integrity: framework and applications» en *IEEE Symposium in security and privacy»*, pp. 184-186.

BAUMAN, Z. (2007): *Amor líquido. Acerca de la fragilidad de los vínculos humanos*. México: Fondo de Cultura Económica.

BÉJAR, H. (1988): «Privacidad» en *terminología científico social. Aproximación científica*. Barcelona: Antrophos, pp. 785-787.

— *El ámbito de lo íntimo*. Madrid: Alianza.

BENKLER, Y. (2006): *The Wealth of Networks: how social production transforms markets and freedom*, New Haven: Yale University Press.

BOYD, D. (2006): «Friends, friendsters and myspace top 8: writing community into being on social networks sites», en *First Monday*, vol. 1, No. 12. Disponible en: http://www. firstmonday. org/issues/issue11_12/boyd/index. html.

BOYD, D. y ELLISON, N. B. (2013): «Sociality through social network sites», in Dutton, W. H. (ed.): The Oxford Handbook of Internet Studies, Oxford: Oxford University Press, pp. 151-172.

BUCHMANN, J. (ed.) (2013): *Internet Privacy: Taking opportunities, assesing risk, building trust* (Acatech – Deutsche Akademie der Technikwissenschaften, acatech STUDY) Heidelberg *et al.:* Springer Verlag.

— Internet Privacy: Taking opportunities, assessing risk, building trust (Acatech – Deutsche Akademie der Technikwissenschaften, acatech STUDY) Heidelberg *et al.:* Springer Verlag.

CHAMBAT, P. y EHRENBERG, A. (1993): «Les reality shows, nouvel âge télévisuel?», *Espirit*, n. 1, enero, pp. 45-50.

COTTEREAU, A. (1992): «Esprit public et capacité de juger. La stabilisation d'un espace public en France aux lendemains de la Révolution», en *Raisons Pratiques*, n. 3.

DONALSON, T., y DUNFEE, T. (1994): «Towards a unified conception of bussiness ethics: integrative social contracts theory», en *The Academy of management Review*, vol. 19, n. 2, pp. 252-284.

DUNFEE, T. (1991): «Business ethics and extant social contracts», en *Business Ethics Quaterly*, n. 1, vol. 1, pp. 23-51.

ECHEVERRÍA, J. (1994): *Telépolis*. Barcelona: Destino.

FOULCAULT, M. (1975): *Surveiller et punir*, edición en castellan (2012): *Vigilar y castigar*, Madrid: Siglo XXI.

FRIED, C. (1968): «Privacy», en *The Yale Journal,* vol. 77, pp. 475-493.

FRIEDEWALD, M. y POHORYLES, R. J., (2013):«Technology and privacy», en *Innovation: The European Journal of Social Science Research*, n. 26, vol. 1-2, pp. 5-20.

GARCÍA JIMÉNEZ, L. (2008): «Las ciencias de la comunicación a la luz de las nuevas tecnologías: retos para una disciplina de la incertidumbre», en *Global Media Journal Mexico*, vol. 5, n. 10.

GERETY, T. (1977): «Redefining privacy», en *Harvard Civil Rights-Civil Liberties Law Review,* vol. 12, n. 2, pp. 233-296.

GOFFMAN, E. (1997): *La presentación de la persona en la vida cotidiana*. Buenos Aires: Amorrortu.

GOULDNER, A. (1976): *The dialectic of Ideology and Technology: the origin, grammar and future of ideology*, Londres: Mcmillan.

GOVANI, T. y PASHLEY, H. (2005): «Student awareness of the privacy implications when using Facebook», en *Privacy Poster Fair at the School of Library and Information Science*, Pittsburgh, PA: Carnegie Mellon University.

ILYES, P. y OCHS, C. (2013): «Sociotechnical Privacy. Mapping the Research landscape», en *Tecnoscienza, Italian Journal of Science & Technology Studies,* n. 4, vol. 2.

KERR, I.; STEEVES, V. y LUCOCK, C. (eds) (2009): *Lessons from the identity tail: anonymity, privacy and identity in a networked society.* Oxford: Oxford University Press.

LACAN, J. (2008): *Seminario 16. De un Otro al otro*, Barcelona: Paidós.

LYON, D. (1995): *El ojo electrónico,* Alianza, Madrid.

MASON, R. O. (1986): «Four ethical issues of the information age», en *MIS Quarterly*, n. 10, vol. 1, pp. 5-12.

MEDINA GUERRERO, M. (2005): *La protección constitucional de la intimidad frente a los medios de comunicación.* Valencia: Tirant lo Blanch.

MEHL, D. (1994): «La «vie publique privée», en *Hermès, la revue,* vol. 1, n. 13-14, pp. 95-113.

MILLAR, J-A. (1994): *Extimité in lacanian theory of discurse*. París: Paidós.

NISSENBAUM, H. (1998): «Protecting privacy in an Information Age: The problem of privacy in public» en *Law and Philosophy*, vol. 17, n. 5-6, pp. 559-596.

— (2010): *Privacy in context: technology, policy, and the integrity of social life*. Stanford: Stanford Law Books.

— (2004): *Privacy as contextual integrity.* Washington Law Review, n. 79, vol. 1, pp. 119-158

PARENT, W. (1983): «Privacy morality and the law», en *Philosophy & Public Affairs*, vol. 12, n. 4, pp. 269-288.

POSTER, M. (1990): *The Mode of Information: Poststructuralism and Social Context*. Chicago: University of Chicago Press.

RACHELS, J. (1975): «Why privacy is important», en *Philosophy & Public Affairs,* vol. 4, n. 4, pp. 323-333.

RULE, J. B. (1974): *Private Lives, public surveillance*, Michigan: Schocken Books.

SCHOEMAN F. D. (1994): «Gossip and privacy», en R. F. Goodman y A. Ben-Zeev, (ed.): *Good Gossip*, pp. 403-408.

— (1984): «Privacy and intimate information», en Schoeman, F. D. (ed.): *Philosophical Dimensions of Privacy*, Cambridge: Cambridge University Press, pp. 403-418.

— «Privacy: philosophical dimensions of the literature», en Schoeman, F. D. (ed.): *Philosophical Dimensions of Privacy*, Cambridge: Cambridge University Press, pp. 1-33.

SENNET, R. (1977): *The fall of public man,* United Kingdom: Cambridge University Press.

— (1979): *Les tyrannies de l'intimité*, París: Seuil.

SIBILA, P. (2008): *La intimidad como espectáculo*. Fondo de Cultura Económica: Argentina.

SIMMEL, G. (1986): *Sociología. Estudios sobre las formas de socialización*. Alianza: Madrid.

SOLOVE, D. J. (2008): *Understanding Privacy*, Cambridge, United States: Harvard University Press.

THOMPSON, J. B. (1998): *Los media y la modernidad: una teoría de los medios de comunicación*. Barcelona: Paidós.

— (2011): «Los límites cambiantes de la vida pública y la privada», en *Comunicación y Sociedad,* n. 15, enero-junio, Méjico: Universidad de Guadalajara, pp. 11-42.

TISSERON, S. (2001): *L'intimité surexposée*, Paris: Hachette.

VAN DER HOVEN, J. (1998): «*Privacy and the varieties of informational wrongdoing*», en *Austr. Journal of Professional and Applied Ethics*, vol. 1, no. 1, pp. 30-43.

— (2001): «*Privacy and the varieties of moral wrongdoing*», en Spinello y Tavani (eds.): *Readings in Cyberethics*. Sudbury: Bartlett & Jones, pp. 430-443.

VERDÚ, V. (2003): *El estilo del mundo. La vida en el capitalismo de ficción,* Barcelona: Anagrama.

WACKS, R. (1989) *Personal information: Privacy and the law.* New York: Oxford University Press.

WESTER, M. y SANDIS, P. (2010): «Privacy and the public», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds): *The «backwards, forwards and sideways» changes of ICT, 11th International conference on the Social and Ethical Impacts of Information and Communication Technology,* (ETHICOMP 2010) 14 al 16 de abril, 2010, Tarragona, España: Universitat Rovira i Virgily, pp. 580-586.

WOLTON, D. (1991): «Les contradictions de l'espace public médiatisé» en *Hermès* n. 10.

ZIMMER, M. (2005): «Surveillance, privacy and the ethics of vehicle safety communication technologies», in *Ethics and Information Technology*, vol. 7, n. 4, pp. 201-221.

Webgrafía:

MOZOROV, E. (2010): «e-outed. Review of Privacy in context», en The times Literary Supplement, 12 de marzo de 2010: Disponible en: https://www.evgenymorozov.com/essays/review_tls_privacy.PDF.[14/04/2012].

Citas para ilustrar el capítulo:

BAUDRILLARD, J. (1983): *Las estrategias fatales,* Barcelona: Anagrama.

CAPÍTULO V

Bibliografía:

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) e Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2009): *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes*, febrero de 2009. Disponible en: www.agpd.es/portalWebAGPD/canaldocumentacion/publicaciones/common/Estudios/estudio_inteco_aped_120209_redes_sociales.pdf.

ALBORNOZ, M. B. (2007): «Cibercultura y las nuevas nociones de privacidad». Primera versión disponible en: www.flacsoandes.org/comunicacion/aaa/imagenes/publicaciones/pub_209.pdf. Posteriormente publicado en la revista *Nómadas*, n. 28, ene. /jun. 2008, Bogotá: Universidad Central, pp. 2-17

ALCÁNTARA, J. F. (2008): *La sociedad del Control*, Barcelona: El Cobre.

ANDRÉS DURÀ, R. (2010)*: Los ángeles no tienen Facebook*. Barcelona: Ediciones Carena.

BACKSTROM, L.; DWORK, C. y KLEINBERG, J. (2007): «Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography», en *Proceedings of the 16th international conference on World Wide Web*. Disponible en: https://utd.edu/~mxk055100/courses/privacy08f_files/social-network-privacy-backstrom.pdf.

BAUMAN, Z. (2004): *Modernidad liquida,* México DF: Editorial Fondo de Cultura Económica.

BÉJAR, H. (1988): *El ámbito íntimo: privacidad, individualismo y modernidad,* Madrid: Alianza.

BENKLER, Y. (2006): *The wealth of networks: How social production transforms markets and freedom*. New Haven: Yale UP.

BOYD, D. (2006): «Friends, friendsters, and myspace top 8: writing community into being on social network sites», en *First Monday*, vol. 12, n. 11. Disponible en: http://www.danah.org/papers/FriendsFriendsterTop8.pdf

BOYD, D. y ELLISON, N. B. (2007): «Social Network Sites: Definition, History, and Scholarship», en *Journal of Computer-Mediated Communication*, vol. 13, n. 1, pp. 210-230.

CACIOPPO, J. T.; FOWLER, J. H. y CHRISTAKIS, N. A. (2009): «Solo en la multitud: Estructura y Difusión de la soledad en una gran red social», en

Diario de la Personalidad y Psicología Social, vol. 97, n. 6, diciembre, pp. 977-991, [doi: 10.1037/a0016076].

CELAYA, J. (2008) *La empresa en la Web 2. 0*. Madrid: Planeta, p. 95.

DEBATIN, B.*;* LOVEJOY, J. P.*;* HORN, A. K. y HUGHES, B. N. (2009): «Facebook and online privacy: attitudes, behaviors, and unintended consequences', en *Journal of Computer-Mediated Communication*, vol. 19, n. 2, pp. 83-108.

DUMBAR, R. I. M. (1992): «Neocortex size as a constraint on group size in primates», en *Journal of Human Evolution,* vol. 22, n. 6, pp. 469-493. [doi:10. 1016/0047-2484(92)90081-J. edit].

ELLISON, N. B.*,* STEINFIELD, C. y LAMPE, C. (2007): «The "Benefits" of Facebook-Friends: Social Capital and College Students' Use of Online Social Network Sites», en *Journal of Computer-Mediated Communication*, n. 12, pp. 1143-1168, p. 1161. http://jcmc.indiana.edu/vol12/ issue4/ellison.html.

EUROPEAN COMMISSION (2011): *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union.* http:// ec.europa.eu/public_opinion/archives/ebs/ebs_359_ en.pdf.

FERNÁNDEZ, S. (2008): «Redes sociales, fenómeno pasajero o reflejo del nuevo interactor», en *Telos,* n. 76, pp. 118-120.

FOWLER, J. y CHRISTAKIS, N. (2010): *Conectados*. Madrid: Taurus.

GELMAN, L. (2009): «Privacy, free speech, and «blurry-edged' social networks», en *Boston College Law Review*, n. 50, pp. 1315-1344.

GOFFMAN, E. (1997): *La presentación de la persona en la vida cotidiana*. Buenos Aires: Amorrortu.

GOVANI, T. y PASHLEY, H. (2005): «Student awareness of the privacy implications when using Facebook», *Privacy Poster Fair at the School of Library and Information Science*, Pittsburgh, PA: Carnegie Mellon University.

GRANOVETTER, M. (1983): «The Strenght of weak ties: a network theory revisited», en *Sociological theory*, vol. 1, pp. 201-233.

HAN, B-C. (2013): *La sociedad de la transparencia.* Barcelona: Herder.

HAYTHORNTHWAITE, C. (2005): «Social networks and Internet connectivity effects», en *Information, Communication & Society*, vol. 8, n. 2, pp. 125-147.

HORVÁT E. A.*,* HANSELMANN M.*,* y HAMPRECHT. A. L. (2012): «One Plus One Makes Three (for Social Networks)», en *PLoS ONE,* vol. 7, n. 4. Disponible en: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0034740.[13/03/2013].

HULL, G.*,* LIPFORD, H. y LATULIPE, C. (2010): «Contextual gaps. Privacy issues on Facebook», en *Ethics and Informaction Technology*, n. 4, pp. 289-302. Disponible en: pages. uoregon. edu/. . . /hull_ context_ privacy_fb. pdf. [12/11/2013].

JAVALOY, F.*,* ESPELT, E. y RODRÍGUEZ, A. (2007): «Comportamiento colectivo y movimientos sociales en la era global», en Morales, J. F. Moya, M. Ga-

viria, E. y Cuadrado, I. (eds.): *Psicología Social,* Madrid: McGrawHill, pp. 641-692.

JONES, J. J., SETTLE, J. E. y BOND R. M. (2013): «Inferring Tie Strength from Online Directed Behaviour», en *PLoS ONE*, vol. 8, n. 1. Disponible en: http:// journals. plos. org/plosone/article?id=10. 1371/journal. pone. 0052168.

LACALLE, C. (2011): «La ficción interactiva. Televisión y Web 2. 0. », en *Ámbitos*, n. 20, pp. 87-107.

LIVINGSTONE, S. (2008): «Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy, and self-expression», en *New Media Society*, n. 10, pp. 393-411.

LIVINGSTONE, S. (2008): «Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy, and self-expression», en *New Media Society*, vol. 10, pp: 393-411

NOËLLE-NEUMANN, E. (1977): *Espiral del silencio. Opinión pública: nuestra piel social,* Barcelona: Paidós.

PABLO, F., SORIANO, S., GOMERO, R., SÁNCHEZ PERNIA, P. y DANS, E. (2009): «identidad digital», en *Foro de la gobernanza en internet en España*, 9 de julio de 2009. Disponible en: www. igfspain. com/doc/archivos/22_ Mayo_Documentaci%C3%B3n_Jornadas_Madrid_2015_05_28_29_v3. pdf

PAPACHARISSI, Z. (2009): «The virtual geographies of social networks: A comparative analysis of Facebook, LinkedIn and ASmallWorld», en *New Media Society*, n. 11, pp. 199-220.

SÁNCHEZ ÁLVAREZ, J. (2006): *Manual para cínicos de cómo triunfar en la sociedad de la mentira*, Madrid: Pensamiento alternativo.

SIBILA, P. (2008): *La intimidad como espectáculo*. Fondo de Cultura Económica: Argentina.

SOLOVE, D. J. (2007): «I've Got Nothing to Hide' and other misunderstandings of privacy», en *San Diego Law Review*, n. 44, pp. 745-772.

STRATER, K. y LIPFORD, H. R. (2008): «Strategies and struggles with privacy in an online social networking community», en *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*, John Moores University, Liverpool, United Kingdom: ACM Press, pp. 111-119.

SUNDÉN, J. (2003): *Material Virtualities: Approaching Online Textual Embodiment*, New York: Peter Lang.

THOMPSON, J. B. (1998): *Los media y la modernidad. Una teoría de los medios de comunicación*. Barcelona: Paidos.

VAN MANEN, M. (2010): «The Pedagogy of Momus Technologies: Facebook, Privacy and Online Intimacy», en *Qualitative Health Research*, vol. XX, n. X, pp. 1-10. [doi:10. 1177/10497323103 64990].

WESTER, M. y SANDIN, P. (2010): «Privacy and the public: perception and acceptance of various applications of ICT», en Arias-Olivia, M., Ward By-

num, T., Rogerson, S., Torres-Coronas, T. (eds): *The «backwards, forwards and sideways» changes of ICT*, 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (Ethicomp2010) 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp 580-586.

YOUNG, A. L. y QUAN-HASSE, A. (2013): «Privacy protection strategies on Facebook» in *Information, Communication and Society*, vol. 16, n. 4, pp. 479-500.

ZUCKERMAN, A. (ed.): *Lógica de la política social*. Filadelfia: Universidad Temple, pp. 269-287.

Webgrafía:

CHEW, M.; BALFANZ, D. y LAURIE, B. (2008): «(Under) mining Privacy in Social Networks», Google Inc. p. 1. Disponible en: http://w2spconf.com/2008/papers/s3p2.pdf.Under mining privacy.[28/01/2012].

Display advertising technology landcaper, http://www.lumapartners.com/resource-center/ [01/02/2012].

FITZPATRICK, B. y RECORDON, D. (2007): «Thoughts on the social graph», en *BradFitz.com*. Disponible en: http://bradfitz.com/socialgraph-problem/. [27/02/2013].

GRIMMELMANN, J. (2009): «Saving Facebook», en *Iowa Law Review*, n. 94, p. 1137-1148. [07/05/2010].

LinkedIn: http://es. linkedin. com/legal/user-agreement [27/03/2013].

MUÑIZ, J. (2010): «Geolocalización en las redes sociales», en *Blog Genbeta*, 20 de abril de 2010. Disponible en: www.genbeta.com.[15/08/2013].

RICHMOND, S. (2010): «Gamestation collects customers' souls in April Fools gag», en *the Telegraph*, 17 de abril de 2010. Disponible en: http://blogs.telegraph.co.uk/technology/shanerichmond/ 100004946/gamestation-collects-customers-souls-in-april-fools-gag/ [17/11/2012].

SAMUELSON, R. (2006): «The Web of Exhibitionsits». Disponible en: http://msl1.mit.edu/furdlog/docs/washpost/2006-09-20_washpost_www_exhibitionists.pdf.[12/03/2010].

WEINBERGER, D. (2005): «Famous to fifteen people», en *The original,* 23 de julio de 2005. [30/01/2010].

Materiales audiovisuales:

DUMBAR, R. I. M. (2011): «Don't Believe Facebook; You Only Have 150 Friends» *National Public Radio*, 4 de junio de 2011. Disponible en: www.npr.

org/2011/06/04/136723316/dont-believe-facebook-you-only-have-150-friends.[30/01/2012].

HOBACK, C. (2013): *Terms and Conditions May Apply*, Documental emitido en *La noche temática: control tecnológico*, La 2, 26 de octubre de 2013. [12/11/2013].

PUNSET, E. (2011): «El poder de las redes sociales», entrevista realizada a James Fowler en el programa *Redes*, 22 de enero de 2011. Disponible en: www.rtve.es/television/20110403/poder-redes-sociales/421888.shtml.[22/01/2011].

Citas para ilustrar el capítulo:

BENAVENTE, J. (1907): *Los intereses creados*. Acto I: Prologo. Cátedra: Madrid.

NIETZSCHE, F. (1994): *Ecce Homo*. Madrid: Alianza Editorial, p. 15.

WINTHER, J. y Balslev, J. (2004): «Weblogs», en *PC Cuadernos Técnicos*, n. 19, mayo de 2004.

CAPÍTULO VI

Bibliografía:

AGUILAR, M. A. (2014): «La opacidad necesaria», en Albergamo, M. (ed.): *La transparencia engaña*, Madrid: Biblioteca Nueva, pp. 83-97.

ALLAN, R. (2012): «Contribuciones para el impacto de la regulación sobre los nuevos servicios. La posición de Facebook sobre la privacidad y la seguridad», en Pérez, J. y Badía, E., (coords.): *El debate sobre la privacidad y seguridad en la red: regulación y mercados*, Madrid: Fundación Telefónica, Ariel, pp. 163-167, p. 164.

ANDRÉS DURÀ, R. (2010)*: Los ángeles no tienen Facebook*. Barcelona: Ediciones Carena.

BENTHAM, J. (1791): *Panopticon; or the Inspection House*. Londres: T. Pyne. Traducción al castellano: (1979): *El panóptico*. Madrid: La Piqueta.

FOUCAULT, M. (1975): *Surveiller et punir: naissance de la prison*. París: Gallimard. Traducción al castellano: (1998): *Vigilar y castigar: nacimiento de la prisión*. Madrid: Siglo XXI.

GROSS, R. y ACQUISITI, A. (2005): «Information revelation and privacy in online social networks», en *Proceedings of ACM Workshop on Privacy in the Electronic Society'05*. Nueva York: ACM Press, pp. 71-80.

KIRKPATRICK, D. (2011): *El efecto Facebook: la verdadera historia de la empresa que está conectando el mundo*. Barcelona: Planeta.

QUAN-HASSE, A. (2013): «Privacy protection strategies on Facebook», en *Information, Communication and Society*, vol. 16, n. 4, pp. 479-500.

RAYCO, G. (2014): «La transparencia como efecto de sentido», en Albergamo, M. (ed.): *La transparencia engaña*, Madrid: Biblioteca Nueva, pp. 99-115.

THOMPSON, J. B. (1998): *Los media y la modernidad. Una teoría de los medios de comunicación*. Barcelona: Paidos.

Webgrafía:

ALEXA (2014): «Top sites on the Web». Disponible en: http://www.alexa.com/topsites.[19/05/2014].

— (2010): «Alexa Traffic Ranks. How popular is facebook. com?» Disponible en: http://www.alexa.com/siteinfo/facebook.com.[19/11/2011].

— «The top 500 sites on the Web». Disponible en: http://www.alexa.com/topsites.[13/02/2012].

— (2013): «Alexa Traffic Ranks». Disponible en: www. alexa.com/siteinfo/facebook.com.[08/02/2013].

Archive. org (ed.) (2007): Política de privacidad de Facebook, 2005, en *Archive. org*. Disponible en: http://Web.archive.org/Web/20050809235134/www.facebook.com/policy.php.[14/02/2010].

— Política de privacidad de Facebook, 2006, en *Archive. org*. Disponible en: Web.archive.org/Web/20060406105119/http:/www.facebook.com/policy.php.[14/02/2010].

— Política de privacidad de Facebook, 2007. *Archive. org*. Disponible en: Web.archive.org/Web/20070118161422/http:/www.facebook.com/policy.php.[14/02/2010].

ARRINGTON, M. (2007): «Is Facebook Really Censoring Search When It Suits Them?», en *TechCrunch*, 22 de noviembre de 2007. Disponible en: http://www.techcrunch.com/2007/11/22/is-facebook-really-censoring-search-when-it-suits-them/.[03/02/2010].

ASPAN, M. (2008): «How Sticky Is Membership on Facebook? Just Try Breaking Free», en *New York Times*, 11 de febrero de 2008. Disponible en: http:/www.nytimes.com/2008/02/11/technology/11facebook.html?pagewanted=all.[10/01/2010].

BBC (ed.) (2007): «Facebook Opens Profiles to Public» en *BBC Online*, 6 de septiembre de 2007. Disponible en: http://news. bbc. co. uk/2/hi/technology/6980454. stm. [01/04/2010].

— «Facebook security», en *BBC Online*, 24 de octubre de 2007. Disponible en: http://www.bbc.co.uk/consumer/tv_and_radio/watchdog/reports/internet/internet_20071024.shtml.[10/11/2010].

Centro de Protección Online de Menores Británico se puede encontar en: http://ceop.police.uk/

CHAN, K. (2009): «People own and control their information», *Facebook blog*, 16 de febrero de 2009. Disponible en: http://www.facebook.com/notes/facebook/on-facebook-people-own-and-control-their information/54434097130. [15/02/2011].

Electronic Frontier Foundation. (ed.) (2010): Facebook. Política de privacidad de Facebook, abril de 2010. *www. eff. org/*. Disponible en: https://www.eff.org/deeplinks/2010/04/handy-facebook-english-translator» \l «connections [10/01/2011].

EL ECONOMISTA (ed.) (2010): «Facebook has become the third-largest nation», en *The Economist*, 22 de julio de 2010. Disponible en: http://www.economist.com/node/16660401.[18/11/2011].

— «El efecto Facebook la historia oculta: la gente confía en mí, son tontos del culo», en *eleconomista.com*, 30 de mayo de 2010. Disponible en: http://www.eleconomista.es/telecomunicaciones-tecnologia/noticias/2188124/05/10/2/La-historia-oculta-de-Facebook-La-gente-confia-en-mi-son-tontos-del-culo.html#Kku 8a6Eavx9tyDh3.[02/08/2011].

— (2014): «Google cerrará Orkut en septiembre», en *eleconomista. com*, 30 de junio de 2014. Disponible en: Disponible en: http://eleconomista. com. mx/tecnociencia/2014/06/30/google-cerrara-orkut-septiembre. [18/08/2014].

EL PAÍS (ed.) (2009): «Facebook alcanza los 250 millones de usuarios», en *El País*, 16 de julio de 2009. Disponible en: http://sociedad.elpais.com/sociedad/2009/07/16/actualidad/1247695209_850215.html.[16/07/2009].

ELECTRONIC FRONTIER FOUNDATION (ed.) (2009): Política de privacidad de Facebook, 9 de diciembre de 2009, en *www.eff.org/*. Disponible en: https://www.eff.org/deeplinks/2010/04/handy-facebook-english-translator»\l«pages».[19/04/2010].

EPIC (ed.) (2009): «Facebook Privacy» *Electronic Privacy Information Center* (EPIC). Disponible en: https://epic.org/privacy/facebook/ [02/01/2012].

Facebook (2014): Política de uso de datos. Los menores y la seguridad. *Facebook.com*.https://es-es.facebook.com / about/ privacy/minors.[12/05/2014]

— Facebook. Servicio de atención al usuario de Facebook. *Facebook.com*. https://www.facebook.com/help/? page=746.[08/02/2014].

— Servicios que ofrece Facebook. *Facebook.com*. Disponible en: http://www.facebookla.com/2009/11/ servicios-que-ofrece-facebook.html [8/10/2012].

— Política de privacidad de Facebook, 2014. *Facebook.com*.Disponible en: https://es-es.facebook.com/about/privacy/update.[12/05/2014].

— (2013): Solicitud de cuenta conmemorativa. *Facebook.com*. Disponible en: https://es-es.facebook.com/help/ contact/651319028315841.[01/03/2013].

— (2010): Facebook: «Controlling How You Share». *Facebook.com*.Disponible en: http://www.facebook.com/privacy/explanation.php [08/02/2010].

Facebook España (2012): «Facebook supera los 900 millones de usuarios», en *Facebook Newsroom,* 2 de mayo de 2012. Disponible en: https://www.facebook.com/FacebookEspana.[08/02/2013].

FORBES (2012): «Is Facebook Lying About 900 Million Users?», en *forbes.com,* 13 de junio de 2012. Disponible en: http://www.forbes.com/sites/thestreet/2012/06/13/is-facebook-lying-about-900-million-users/.[29/01/013].

Global Web Index (2014): *GWI Social Summary*, publicado en enero de 2014. Disponible en: https://app.globalWebindex.net/products/report/gwi-social-q3-2014.[30/01/2014].

GROSSMAN, L.(2010): «Person of the Year», en *Time,* 15 de diciembre de 2010. Disponible en: http://content.time.com/time/specials/packages/article/0,28804,2036683_2037183,00.html.[19/02/2011].

JOHNSON, B.(2010): «Privacy no longer a social norm, says Facebook founder», en *The Guardian,* 11 de enero de 2010. Disponible en: www.theguardian.com/technology/2010/jan/11/facebook-privacy.[20/01/2011].

KAPLAN, K.A.(2003): «Facemash Creator Survives Ad Board», en *The Harvard Crimson,* 19 de noviembre de 2003. Disponible en: www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/ [15/01/2010].

KIRKPATRICK, M.(2010): «Facebook's Zuckerberg Says The Age of Privacy is Over», en *Readwrite*, 9 de enero de 2010. Disponible en: readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_ of_privacy_is_ov.[14/03/2011].

LOGAN, B.(2009): «Blog post commemorating Facebook's 200 millionth user», en *Facebook blog*. Disponible en://www.facebook.com/notes/facebook/200-million-strong/72353897130.

MCKEON, M. (2010): «The Evolution of Privacy on Facebook. Changes in default profile settings over time», en *mattmckeon. com*. Disponible en: http://mattmckeon. com/facebook-privacy/ [10/01/2011]

MELBER, A.(2008): «Does Facebook Own You Forever?» en *The Huffington Post*, 2 del 11 de 2008. Disponible en: www.huffingtonpost.com/ari-melber/does-facebook-own-youfor_b_86115.html

NIELSEN, W.(2009): «Time spent on Facebook up 700%, but MySpace Still Tops for Video». Disponible en: http://blog.nielsen.com/nielsenwire/online_mobile/time-spent-on-facebook-up-700-but-myspace-stilltops-for-video/. [20/01/2012].

OPSAHL, K.(2010): «Facebook's Eroding Privacy Policy: A Timeline», en *www.eff.org,* 30 de abril de 2010. Disponible en: https://www.eff.org/es/deeplinks/2010/04/facebook-timeline.[12/03/2011].

SPRENGER, P.(1999): «Sun on Privacy: «Get Over It'», en *Wired,* 26 de enero de 1999.

The Zuckerberg Files: zuckerbergfiles.org.[19/02/2013].

THOMPSON, C.(2008): «Brave new world of ambient intimacy», en *The New York Times,* 7 de septiembre 2008. Disponible en: www.nytimes.

com/2008/09/07/magazine/07awareness-t.html?pagewanted=all&_r=0.[19/02/2011].

TOSBACK (2009): Política de privacidad de Facebook, 29 de octubre de 2009. *Tosback.org*. Disponible en: www.tosback.org/version.php?vid=961/ http://www.facebook.com/privacy/.[14/02/2010].

ZIMMER, M.(2014): «Mark Zuckerberg's theory of privacy», en *The Washington Post,* 3 de febrero de 2014. Disponible en: www.washingtonpost.com/lifestyle/style/mark-zuckerbergs-theory-of-privacy/2014/02/03/2c1d780a-8cea-11e3-95dd-36ff657a4dae_story.html.[12/08/2012].

ZUCKERBERG, M.(2010): «From Facebook, answering privacy concerns with new settings» in *The Washington post,* 24 de Mayo de 2010. Disponible en: www.washingtonpost.com/wp-dyn/content/article/2010/05/23/AR2010052303828.html.[23/03/2011].

Materiales audiovisuales:

FINCHER, D. (2010): *La red Social* (*The social network*)

KING, B. (2007): «Facebook Data Protection Row», en *Channel 4*, 17 de noviembre de 2007. Disponible en: www channel4.com[01/12/2010].

Otras fuentes:

ALONSO, J. (2015): «Mesa redonda: Vigilancia, secretos, transparencia, cultura, documentos, periodismo». *XV Congreso de la Asociación Española de Semiótica*. Celebrado el 5 de mayo de 2015, en la Facultad de Ciencias de la Información, Universidad Complutense de Madrid. Para más información: http://semioticagesc. com/quienes-somos/historial-del-grupo/

Citas para ilustrar el capítulo:

GOETHE, W. (1810): *Zur Farbenlehre*. Traducción al castellano (1999): *Teoría de los colores*. Madrid: Celeste.

MACHADO, A. (1923): *Proverbios y cantares* I, en *Revista de Occidente*, n. III, septiembre de 1923.

CAPÍTULO VII

Bibliografía:

ALLAN, R. (2012): «Contribuciones para el impacto de la regulación sobre los nuevos servicios. La posición de Facebook sobre la privacidad y la seguri-

dad», en Pérez, J. y Enrique, B. (coord.): *El debate sobre la privacidad y seguridad en la red: regulación y mercados*. Madrid: Fundación Telefónica, Ariel.

ANDRÉS DURÀ, R. (2010)*: Los ángeles no tienen Facebook*. Barcelona: Ediciones Carena.

BESMER, A y LIPFORD, H. R. (2010): «User's (Mis)conceptions of social implications», en *Proceedings of Graphics Interface*, pp. 63-70.

BOYD, D. (2008): «Facebook's Privacy Trainwreck: Exposure, Invasion and Social Convergence», en *Convergence: The International Journal of Research into New Media Technologies*, vol. 14, pp. 13-20.

BONNEAU, J. (2009): «Democracy Theatre on Facebook», en *Light Blue TouchpaperSecurity Research*, Computer Laboratory, University of Cambridge, 29 de marzo de 2009. Disponible en: http://www.lightbluetouchpaper.org/2009/03/29/commentary-on-facebooks-terms-of-service/ [05/04/2012]

CHEW, M., BALFANZ, D. y LAURIE, B. (2008): «(Under) mining Privacy in Social Networks». Disponible en: http://w2spconf.com/2008/papers/s3p2.pdf.[12/01/2012].

CONLEY, C. (2009): «Take Our Quiz: See What Do Facebook Quizzes Know About You!» en www.aclu.org, 26 de agosto de 2009.Disponible en: http apps.facebok.com/aclunc-privacy-quiz.[20/06/2011].

FELT, A y EVANS, D. (2009): «Privacy protection for social networking APIs», en *Proceedeings of Web 2. 0 Security and Privacy* (*W2SP 2009*) Oakland, California.

GROSS, R. y ACQUISITI, A. (2005): «Information revelation and privacy in online social networks», en *Proceedings of ACM Workshop on Privacy in the Electronic Society'05*. Nueva York: ACM Press, pp. 71-80.

HULL, G., LIPFORD, H. y LATULIPE, C. (2010): «Contextual gaps. Privacy issues on Facebook», en *Ethics and Informaction Technology*, n. 4, pp. 289-302. Disponible en: pages.uoregon.edu/. . . /hull_context_ privacy_fb. pdf.

INTRONA, L. D., y NISSENBAUM, H. (2000): «Shaping the Web: Why the politics of search engines matters», en *The Information Society*, vol. 16, n. 3, pp. 169-185.

JERNIGAN, C. y MISTREE, B. F. (2009): «Gaydar: Facebook friendships expose sexual orientation», en *First Monday*, vol. 14, n. 10, 5 de octubre de 2009. Disponible en: http://firstmonday.org/article/view/2611/2302.

JOINSON, A. N. (2008): «"Looking at", "Looking up", or "Keeping up with" People? Motives and uses of Facebook», en *CHI 2008 Proceedings: Online Social Networks*, pp. 1027-1036.

KIRKPATRICK, D. (2011): *Op. cit.,* p. 365.

KOSINSKIA M., STILLWELLA, D. y GRAEPELB, T. (2013): «Private Traits and Attributes are Predictable from Digital Records of Human Behaviour», en

Proceedings of the National Academy of Sciences (PNAS) University of California, Berkeley. [doi: 10. 1073/ pnas. -1218772110]

LESSIG, L. (2006): *Code and other laws of cyberspace, Version 2. 0*. New York: Basic Books.

MACKENZIE, A. (2006): *Cutting code: Software and sociality*. New York: Peter Lang.

MAURIENI, C. (2012): *Facebook is Deception (Volume One)*. Estados Unidos: WSIC Ebooks

NISSENBAUM, H. (2004): Privacy as contextual integrity. Washington Law Review, n. 79, vol. 1, pp. 119-158

PAPACHARISSI, Z. (2009): «The virtual geographies of social networks: A comparative analysis of Facebook, LinkedIn and ASmallWorld», en *New Media Society*, vol. 11, pp. 199-220.

SCHWARTZ, P. M. (2012): «Privacidad online: planteamientos jurídicos en Estados Unidos y la Unión Europea», en Pérez, J. y Enrique, B. (coords.): *El debate sobre la privacidad y seguridad en la red: regulación y mercados*. Madrid: Fundación Telefónica, Ariel, pp. 59-71.

SIMONITE, T. (2014): «Facebook creates software that matches faces almost as well as you do», en *Mit Technbology Review*, 17 de marzo de 2014. Disponible en: http://www. technologyreview. com/news/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/.

SOLOVE, D. J. (2007): *The future of reputation: Gossip, rumour and privacy on the internet*. New Haven, CT: Yale UP.

TAIGMAN, Y., YANG, M., RANZATO, M. y WOLF, L. (2014): «DeepFace: Closing the gap to human-level performance in face verification», en *Proceedings of IEEE conference on Computer Vision and Pattern Recognition* (CVPR) Columbus, Ohio, 24 de junio de 2014. Disponible en: https://research. facebook. com/publications/480567225376225/deepface-closing-the-gap-to-human-level performance-in-face-verification.

TERRANOVA, T. (2004): *Newtork culture: Politics for the information age*. London: Pluto Press, pp: 73-97.

YOUYOU, W., KOSINSKI, M. y STILLWELL, D. (2015): «Computer-based personality judgments are more accurate than those made by humans», en *Proceedings of the National Academy of Sciences (PNAS)* University of California, Berkeley, 12 de enero de 2015, [doi:10. 1073/pnas. 1418680112].

ZIMMER, M. (2007): «Privacy and surveillance in Web 2. 0: A study in contextual integrity and the emergence of Netaveillance», en *Society for Social studies of Science*. Disponible en: http://www.academia.edu/3943172/Privacy_and_Surveillance_in_Web_2.0_A_study_in_Contextual_Integrity_and_the Emergence_of_Netaveillance.[22/01/2010].

Webgrafía:

Archive.org (ed.) (2007): Política de privacidad de Facebook, 2007. *Archive.org*. Disponible en: http://Web.archive.org/Web/20070118161422/http:/www.facebook.com/policy.php.[14/02/2010].

BILTON, N. (2010): «Price of Facebook Privacy? Start Clicking», en *The New York Times*, 12 de mayo de 2010. Disponible en: www.nytimes.com/2010/05/13/technology/personaltech/13basics.html?_r=0.[07/01 /2011].

CASPAR, J. (2011): «Facebook's biometric database continues to be unlawful«, *Der Hamburgische Beauftragte fürDatenschutz und Informationsfreiheit* 10 de noviembre de 2011. Disponible en: https://www.datenschutz-hamburg.de/uploads/media/PressRelease-2011-11-10-Facebook_BiometricDa tebase.pdf. [02/04/2012].

CBS (ed.) (2012): «Zuckerberg family pic stirs Facebook privacy debate», en *CBS News*, 27 de diciembre de 2012. Disponible en: http://www.cbsnews.com/news/zuckerberg-family-pic-stirs-facebook-privacy-debate/ [12/05/2013].

CNET (ed.) (2011): «How to disable facial recognition in facebook», en www.cnet.com, 8 de junio de 2011. Disponible en: http://www.cnet.com/how-to/how-to-disable-facial-recognition-in-facebook/ [02/11/2012].

CNN (ed.) (2009): «Las redes sociales crecen en publicidad», en *CNN Expansión,* 2 de septiembre de 2009. Disponible en: www.cnnexpansion.com/tecnologia/2009/09/02/facebook-se-aduena-de-publicidad-online.[02/07/2010].

CRIADO, M.A. (2013): «Cien "me gusta" bastan para saber el sexo, raza o ideología de un usuario de Facebook», en *El País*, 11 de marzo de 2013. Disponible en: http://esmateria.com/2013/03/11/cien-me-gusta-bastan-para-saber-el-sexo-raza-o-ideologia-de-un-usuario-de-facebook/ [22/12/2013].

— (2015): «Eres lo que "te gusta"», en *El País,* 12 de enero de 2015. Disponible en: http://elpais.com/elpais/2015/01/12/ciencia/1421084469_835718.html. [25/01/2015].

CUBRILOVIC, N. (2012): «Facebook and many other sites also bypass Internet Explorer privacy controls», en *New Web Order*, 21 de febrero de 2012. Disponible en: https://www.nikcub.com/posts/facebook-also-doesnt-honor-p3p/ [12/03/2012].

EL ECONOMISTA (2009): «Facebook corrige su cláusula sobre derechos de contenidos tras la polémica», en *eleconomista.com*, 18 de febrero de 2009. Disponible en: http://ecodiario.eleconomista.es/internet/noticias/1042909/02/09/Facebook-corrige-su-clausula-de-contenidos-tras-la-polemica-de-derecho-perpetuo-sobre-ellos.html.[29/07/2010].

EL MUNDO (Ed.) (2012): «Facebook y Linkedin se comprometen a reforzar su privacidad», en *El Mundo*, 29 de junio de 2012. Disponible en: www.elmundo.es/elmundo/2012/06/29/navegante/134095 5573.html.[12/03/2013]

EL PAÍS (ed.) (2009): «El misterio de las fotos de Zuckerberg en Facebook», en *El País,* 16 de diciembre de 2009. Disponible en: http://tecnologia.elpais.com/tecnologia/2009/12/16/actualidad/1260957661_850215.html.[12/01/2010].

HANSELL, S. (2007): «Zuckerberg Apologizes, Allows Facebook Users to Evade Beacon», en *The New York Times*, 5 de diciembre de 2007. Disponible en: http://bits.blogs.nytimes.com/2007/12/05/zuckerberg-apologizes-allows-facebook-users-to-evade-beacon/?_r=0.[02/08/2010].

HODGKINSON, T. (2008): «Por qué detesto Facebook y las redes sociales», en *Diario Clarín,* 23 de enero de 2008. Disponible en: http://edant.clarin.com/suplementos/informatica/2008/01/23/f-01591338.htm.[12/06/2009].

MANETTO, F. (2008): «La cara oculta de Facebook», en *El País*, 27 de enero de 2008. Disponible en: http://elpais.com/diario/2008/01/27/sociedad/1201388405_850215.html.[09/02/2010].

MCCARTHY, C. (2007): «MoveOn.org takes on Facebook's 'Beacon' ads», en *News.cnet.com*, noviembre de 2007. Disponible en: http://www.news.com/8301-13577 3-9821170-36.html.[04/05/2012].

— (2009): «Facebook backtracks on public friend lists», en *News.cnet.com*, 12 de diciembre de 2009. Disponible en: http://www.cnet.com/news/facebook-backtracks-on-public-friend-lists/ [07/01/2010].

NAKASHIMA, E. (2007): «Feeling betrayed, Facebook users force site to honor their privacy», en *The Washington / Post,* 30 de noviembre de 2007. Disponible en: www.washingtonpost.com/wp-dyn content/article/2007/11/29/AR2007112902503.html.[22/06/2012].

LA VANGUARDIA (ed.) (2014):«Facebook aumenta usuarios, ingresos y presencia en el móvil», en *La Vanguardia,* 23 de abril de 2014. Disponible en: www.lavanguardia.com/tecnologia/redes-sociales/facebook/20150423/54430141868/facebook-aumenta-usuarios-ingresos-presencia-movil.html.[12/05/2014]

REISINGER, D. (2012): «Facebook sued for $15 billion over alleged privacy infractions», en *News.cnet.com*, 18 de mayo de 2012. Disponible en: http://news.cnet.com/8301-1023_3-57437060-93/Facebook-sued-for-$15-billion-over-alleged-privacy-infractions/ [12/01/2012].

ROSMARIN, R. (2006): «Facebook's Makeover», en *Forbes*, 5 de octubre de 2006. Disponible en: http://www.forbes.com/technology/2006/09/01/facebook-myspace-internet_cx_rr_0905facebook.html.[29/03/2009].

ORTUTAY, B. (2010): «Facebook Privacy Change Sparks Federal Complaint», en *The Huffington Post,* 13 de marzo de 2010. Disponible en: www.huffingtonpost.com/2009/12/17/facebook-privacy-watchdog_n_396103.html.[09/02/2014].

O'BRIEN, K.J. (2012): «Germans Reopen Investigation on Facebook Privacy», en *The New York Times*, 15 de agosto de 2012. Disponible en: www.nytimes.com/2012/08/16/technology/germans-reopen-facebook privacy-inquiry-html).[08/06/2014].

PRIVACY TIMES (ed.) (2006): «Facebook's "news feed" feature sparks privacy revolt among users», en *Privacy Times*, 18 de septiembre de 2006. Disponible en: http://privacytimes.com/facebookers.html.[30/01/2010]

BANKSTON, K. (2010): «Facebook's New Privacy Improvements Are a Positive Step, But There's Still More Work to Be Done», en *www.eff.org,* 26 de mayo de 2010. Disponible en: https://www.eff.org/es/deeplinks/2010/05/facebooks-new-privacy-improvements-are-positive.[12/06/2011].

BERTEAU, S. (2007): «Facebook's Misrepresentation of Beacon's Threat to Privacy: Tracking users who opt out or are not logged in», en *CA Security Advisor Research Blog*, 29 de noviembre de 2007. Disponible en: http://community.ca.com/blogs/securityadvisor/archive/2007/11/29/facebook-s misrepresentation-of-beacon-s-threat-to-privacy-tracking-users-who-opt-out-or-are-not-logged-in.aspx.[09/04/2011].

CHAN, K.H. (2009): «An update on Facebook governance», en *Facebook blog*, 18 de marzo de 2009. Disponible en: https://www.facebook.com/notes/facebook/an-update-on-facebook-governance/60812327 130.[20/05/2009].

— «Improving Your Ability to Share and Connect», en *Facebook blog*, 4 de marzo de 2009. Disponible en: https://www.facebook.com/notes/facebook/improving-your-ability-to-share-and-connect /57822962130.[20/06/2009].

CHAN, K.H. (2009): «Governing the Facebook Service in an Open and Transparent Way», en *Facebook newsroom*, 26 de febrero de 2009. Disponible en: www.facebook.com/notes/facebook/governing-the-facebook-service-in-an-open-and-transparent-way/56566967130.[18/11/2014].

CIPPIC (2008): «CIPPIC files privacy complaint against Facebook», en *www.cippic.ca*, 30 de mayo de 2008. Disponible en: https://cippic.ca/sites/default/files/NewsRelease _30May08.pdf.

DORIGHTS (2009):«What Does Facebook's Privacy Transition Mean for You?», en *Dotrights.org*, 4 de diciembre de 2009. Disponible en: http://dotrights.org/what-does-facebooks-privacy-transition-mean-you.[12/01/2010].

ELECTRONIC FRONTIER FOUNDATION (ed.) (2010): Facebook.Política de privacidad de Facebook, abril de 2010.*www.eff.org/*. Disponible en: https://www.eff.org/deeplinks/2010/04/handy-facebook-english-translator» \l «connections [10/01/2011].

EPIC (2015): «With new policy changes, Facebook tracks users across the Web», en *epic.org*, Electronic Privacy Information Center (EPIC) 4 de febrero de 2015. Disponible en: https://epic.org/2015/02/with-new-policy-changes-facebo.html.[15/05/2015].

— (2012): «In re Facebook and the Facial Identification of Users», en *epic.org*. Disponible en: https://epic.org/privacy/facebook/facebook_and_facial_ recognitio.html.[02/01/2012].

Europe *vs*.Facebook (2012): «Facebooks Data Pool», en *Europe vs Facebook Web page*. Disponible en: http//europe-v-facebook.org/ EN/Data_ Pool/ -data pool.html.[10/11/2012].

Facebook (2014): Política de privacidad de Facebook, 2014.*Facebook.com*. Disponible en: https://es-es.facebook.com/about/privacy/update.[12/05/2014].

— «Publicidad y contenido de Facebook.Publicidad.Información sobre el usuario» y «Publicidad y contenido de Facebook.Publicidad en Facebook». Disponible en: https://es-es.Facebook.com/about/ads»

— (2009): *Licencia y términos de uso*. https://es-es.facebook.com/legal/terms?locale=es_ES

«Facebook Principles» y «Statement of Rights and Responsibilities», *Facebook blog*, el 18 de marzo de 2009.[20/05/2009].

— (2009): «Las políticas de privacidad de Facebook cambian», en *Facebook newsroom*, 27 de abril de 2009. Disponible en: https://newsroom.fb.com/

— (2010): «Controlling How You Share».Política de privacidad de Facebook, 2010. Disponible en: https://www.facebook.com/privacy/explanation. [12/12/2010].

— (2009): «FaceBook vs.YOUR Privacy - AKA Note: Your Friend List is always visible to you and your friends», en *Facebook blog,* 27 de diciembre de 2009. Disponible en: https://m.facebook.com/notes/colnect-collectors-club-community-stamps-coins-banknotes-collectibles/facebook-vs-your-privacy-aka-note-your-friend-list-is-always-visible-to-you-and-/380530885206/ [27/03/2010].

— (2014): «Información sobre la publicidad en Facebook». Política de privacidad 2014. Disponible en: https://www.facebook.com/about/ads.

— (2007): «Thoughts on Beacon», en *Facebook Newsroom,* 6 de diciembre de 2007. Disponible en: https://newsroom.fb.com/news/2007/12/announcement-facebook-users-can-now-opt-out-of-beacon-feature/ [13/04/2010].

GAWKER (ed.) (2009): «Facebook CEO's Private Photos Exposed by the New «Open' Facebook», en *Gawker.com*, 11 de diciembre de 2009. Disponible en: gawker.com/5423914/facebook-ceos-private-photos-exposed-by-the-new-openface book /gallery.[12/01/2010].

GILLMOR, D. (2009): «facebook-starting-over», en *Mediactive.com*, 12 de diciembre de 2009. Disponible en: http://mediactive.com/2009/12/12/facebook-starting-over/ [25/09/2010].

HICKS, M. (2010):«Making Control Simple», en *Facebook blog*, 26 de mayo de 2010. Disponible en: http://blog.Facebook.com/blog.php?post=391922327130. [19/06/2010].

KILLOCK, J. (2009): «Facebook's theatrical rights and wrongs», en *openrightsgroup.org*, página Web de la Open Rights Group. Disponible en: www.openrightsgroup.org/blog/2009/facebooks-theatrical-rights-and-wrongs. [12/11/2012].

KIRKPATRICK, M. (2010): «Facebook's Zuckerberg Says The Age of Privacy is Over», en *Readwrite*, 9 de enero de 2010. Disponible en: readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.[23/09/2010].

OPSAHL, K. (2010): «Facebook Should Follow Its Own Principles», en *www.eff.org,* página Web de la Electronic Frontier Foundation, 13 de mayo de 2010. Disponible en: http://www.eff.org/deeplinks/2010/05/Facebook-should-follow.[12/11/2012].

— «Facebook's eroding privacy policy: a timeline», en *www.eff.org,* página Web de la Electronic Frontier Foundation, 27 de mayo de 2010. Disponible en: https://www.eff.org/deeplinks/2010/ 04/facebook-timeline.[07/01/2011].

— «Updated: Facebook Further Reduces Your Control Over Personal Information.en *www.eff.org,* página Web de la Electronic Frontier Foundation, 19 de abril de 2010. Disponible en: https://www.eff.org/deeplinks/2010/04/Facebook-further-reduces-control-over-personal-information.[10/05/2011].

— «Six Things You Need to Know About Facebook Connections», en *www.eff.org,* 4 de mayo de 2010. Disponible en: www.eff.org/es/deeplinks/2010/05/things-you-need-know-about-facebook.[12/02/2012].

— «How to Opt Out of Facebook's Instant Personalization», en *www.eff.org*, 22 de abril de 2010. Disponible en: www.eff.org/deeplinks/2010/04/how-opt-out-Facebook-s-instant-personalization.[15/05/2012].

ORTUTAY, B. (2009): «Facebook to end Beacon tracking tool in settlement», en *USA Today*, 21 de septiembre de 2007. Disponible en: http://usatoday30.usatoday.com/tech/hotsites/2009-09-21-facebook-beacon_N.htm.[12/05/2011].

OZER, N. (2009): «Facebook Privacy in Transition - But Where is it Heading?», en *www.aclu.org,* página Web de American Civil Liberties Union (ACLU) 9 de diciembre de 2009. Disponible en: https://www.aclu.org/blog/speakeasy/facebook-privacy-transition-where-it-heading.[05/01/2012].

RICHARD, E. (2010): «A Handy Facebook-to-English Translator», en *www.eff.org,* 10 de abril de 2010. Disponible en: https://www.eff.org/es/deeplinks/2010/04/handy-facebook-english-translator.[12/06/2012].

RYAN, T. (2009): «Valleywag «Facebook's New 'Privacy' Scheme Smells Like an Anti-Privacy Plot» en *gawker.com,* 12 de febrero de 2009. Disponible en: gawker.com/5417145/facebooks-new-privacy-scheme-smells-like-an-anti-privacy-plot.[01/07/2012].

TOSBACK (2009): Política de privacidad de Facebook, 29 de octubre de 2009. *Tosback.org.* Disponible en: http://www.tosback.org/version.php?vid=961/ «http://www.facebook.com/privacy/».[14/02/2010].

WALTERS, C. (2009): «Facebook's New Terms Of Service: 'We Can Do Anything We Want With Your Content.Forever'», en *The Consumerist*, 20 de febrero de 2009. Disponible en: http://consumerist.com /2009/02/15/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever/ [12/ 03/2010].

Materiales audiovisuales:

HOBACK, C. (2013): *Terms and Conditions May Apply*, documental emitido en *La noche temática - Términos y condiciones de uso*, La 2 TVE, 26 octubre de 2013.

VALLÉS, V. (2012): Entrevista a Paloma Llaneza, en *24 horas*, TVE, 19 de junio de 2012.

Instituciones y fuentes oficiales:

American Civil Liberties Union: www. aclu. org

Canadian Personal Information Protection and Electronic Documents Act (PIPEDA): http://laws-lois. justice. gc. ca/eng/acts/P-8. 6/index. html.

European Commission (2012): Proposal for a Regulation Of The European Parliament And Of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Bruselas, 25 de enero de 2012. Disponible en: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.[02/02/2012].

Facebook Settlement. Agreement Containing Consent Order, In re Facebook, Inc., File No. 092-3184 (F. T. C. Nov. 29, 2011).

FAIR, L. (2011): «The FTC's settlement with Facebook. Where Facebook went wrong». Federal Trade Commission Protecting America´s Consumers, 29 de noviembre de 2011. Disponible en: business. ftc. gov/blog/ 2011/ 11/ ftc%E2%80%99s-settlement-facebook-where-facebook-wentwrong. [12/05/2012].

Federal Trade Commission (2011): «Facebook settles FTC Charges that it Deceived Consumers by Failing to Keep Privacy Promises», Federal Trade Commission Protecting American Consumers, 29 de noviembre de 2011. http//ftc. gov/opa/2011/11/privacysettlement.-shtm.[10/01/2012].

Office of the Privacy Commissioner of Canada, https://www.priv.gc.ca/index_e. asp.

Specially Designated Nationals List (SDN): http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

Citas para ilustrar el capítulo:

Henckel, F. (2006): *Das Leben der Anderen.*

CAPÍTULO VIII

Bibliografía:

ACQUISTI, A. y GROSS, R. (2006): «Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook», in G. Danezis and P. Golle (eds.): *Privacy Enhancing Technologies*, 6th International Workshop PET 2006, Berlin and Heidelberg: Springer, pp. 36-58.

ACQUISTI, A. y GROSSKLAGS, J. (2003): «Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior», en *2nd annual Workshop on Economics and Information Security*, p. 10. Disponible en: http://www.cpppe.umd.edu/rhsmith3/papers/Final_session6_acquisti.grossklags.pdf.[05/11/2013]

ACQUISTI, A. y GROSSKLAGS, J. (2005): «Privacy and rationality in individual decision making», en *IEEE Security & Privacy*, vol. 3, n. 1, pp. 26-33.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) e Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2009): *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes*, febrero de 2009. Disponible en: www.agpd.es/portalWebAGPD/canaldocumentacion/publicaciones/common/Estudios/estudio_inteco_aped_120209_redes_sociales.pdf.[29/03/2013].

ANDRÉS DURÀ, R. (2010)*: Los ángeles no tienen Facebook*. Barcelona: Ediciones Carena.

BADÍA, E. (2012): «Marco conceptual. Derecho ¿pendiente?», en Pérez, J. y Badía, E., (coord.): *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados*. Madrid: Ariel.

BARNES, S. B. (2006): «A privacy paradox: social networking in the United States», in *First Monday*, vol. 11, n. 9, http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312 [29/05/2014].

BESMER, A y LIPFORD, H. R. (2010): «Moving beyond untagging: photo privacy in a tagged world», en Mynatt, D. Schoner, G. Fitzpatrick, S. E. Hudson, W. K. Edwards y T. Rodden (eds.): *CHI 2010*, pp. 1563-1572.

BIRN, D. (1998): *The Transparent Society,* Reading MA: Perseus Books

BLUMER, H. (1986): *Symbolic Interactionism: Perspectives and Method*, Berkeley: University of California Press.

BOYD, D. (2007): «Social Network Sites: Public, Private, or What?» en *Knowledge Tree*, 13 May, 2007. http://kt. flexiblelearning. net. au/tkt2007/?page_id=28.

— «Why Youth (Heart): Social Network Sites: The Role of Networked Publics in Teenage Social Life», en D. Buckingham (ed.): *Youth, Identity, and Digital Media*, Cambridge, MA: MIT Press, pp. 119-142.

— «Why Youth (Heart): Social Network Sites: The Role of Networked Publics in Teenage Social Life», en D. Buckingham (ed.): *Youth, Identity and Digital Media*, Cambridge, MA: MIT Press, pp. 119-142.

— (2008): «Facebook's Privacy Trainwreck: Exposure, Invasion and Social Convergence», en *Convergence: The International Journal of Research into New Media Technologies*, vol. 14, pp. 13-20.

— *Taken Out of Context: American Teen Sociality in Networked Publics,* PhD Dissertation, University of California-Berkeley, School of Information.

BOYD, D. y ELLISON, N. B. (2007): *Op. cit.*

BOYD, D. y HARGITTAI, E. (2010): «Facebook's Privacy Settings: Who Cares?» en *First Monday*, vol. 15, n. 8.

BOYD, D. y MARWICK, A. (2011): «Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies», en *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, septiembre, 2011. Disponible en: http://ssrn. com/abstract=1925128, [4/11/2013].

BOYD, D. y MARWICK, A. E. (2010): «I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience», en *New Media and Society*, vol. 13, n. 1, pp. 114-133

BRANDTZAEG, P. B., LÜDERS, M. y SKJETNE, J. H. (2010): «Too Many Facebook 'Friends'? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites», en *International Journal of Human-Computer Interaction*, *Special Issue: HCI and Social Computing*, vol. 26, n. 11-12, pp. 1006-1030.

BUCHMANN, J. (ed.) (2013): *Internet Privacy: Taking opportunities, assesing risk, building trust* (Acatech -Deutsche Akademie der Technikwissenschaften, acatech STUDY) Heidelberg *et al.:* Springer Verlag.

CHAI S., y RAO, H. R. (2008): «'WiRed' senior citizens and online information privacy», en M., Ward Bynum, T., Rogerson, S., (eds): *Living, working and learning beyond technology* (ETHICOMP 2008), International conference on the Social and Ethical Impacts of Information and Communication Technology, 24-26 September 2008, en Mantua Italia: University of Pavia, pp. 101-110.

CUNNINGHAM, S. J. y MASOODIAN, M. (2010): «Analysing user's behaviours to identify their privacy concerns», en *Workshop Proceedings of Privacy and Usability Methods Pow-wow (PUMP): 2010*, 24th BCS International Conference on Human-Computer Interaction (Dundee, UK, 6-10 September) British Computer Society.

DEBATIN, B., LOVEJOY, J. P., HORN, A. K. y HUGHES, B. N. (2009): «Facebook and online privacy: attitudes, behaviors and unintended consequences», en *Journal of Computer-Mediated Communication*, vol. 19, n. 2, pp. 83-108;

DEY, R., JELVEH, Z. and ROSS, K. (2012): «Facebook users have become much more private: a large-scale study», en *2012 IEEE International Conference*

on Pervasive Computing and Communications Workshops, Lugano, Switzerland, pp. 346-352.

DWYER, C., HILTZ, S. y PASSERINI, K. (2007): «Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace, en *AMCIS 2007 Proceedings*. Paper 339.

ELLISON, N. B., VITAK, J., STEINFIELD, C., GRAY, R. y LAMPE, C. (2011): «Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment», en S. TREPTE, S. and L. REINECKE (eds.): *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web*, New York: Springer, pp. 19-32.

ELLISON, N. B. y STEINFIELD, C. (2008): «Changes in use and perception of Facebook», en *Proceedings of the 2008 ACM conference on Computer supported cooperative work (CSCW «08)* San Diego, California: ACM Press, pp. 721-730.

FOWLER, J. y CHRISTAKIS, N. (2010): *Conectados*. Madrid: Taurus.

FREDERIC S. y WOODROW H. (2012): «Boundary regulation in social media», en *CSCW'12*, Nueva York: ACM Press: ACM Press, pp. 769-778.

GONZÁLEZ GAITANO, N. (1990): *El deber de respeto de la intimidad. Información pública y relación social,* Pamplona: Eunsa.

GOVANI, T. y PASHLEY, H. (2005): «Student awareness of the privacy implications when using Facebook», en *Privacy Poster Fair at the School of Library and Information Science*, Pittsburgh, PA: Carnegie Mellon University.

GROSS, R. y ACQUISITI, A. (2005): «Information revelation and privacy in online social networks», en *Proceedings of ACM Workshop on Privacy in the Electronic Society'05*, Nueva York: ACM Press, pp. 71-80.

GRUBBS, M. y MILNE, G. (2010): «Gender differences in privacy-related measures for young adult Facebook users», en *Journal of Interactive Advertising*, vol. 10, n. 2, pp. 28-45.

GÜRSES, S. y DIAZ, C. (2013): «Two Tales of Privacy in Online Social Networks», en *IEEE Security and Privacy*, vol. 11, n. 3, pp. 29-37.

ILYES, P. y OCHS, C. (2013): «Sociotechnical Privacy. Mapping the Research landscape», En *Tecnoscienza, Italian Journal of Science & Technology Studies*, n. 4, vol. 2.

JAGATIC, T. N., JOHNSON, N. A., JAKOBSSON, M. y MENCZER, F. (2007): «Social phishing», en *Communications of the ACM,* vol. 50, n. 10, pp. 94-100. Disponible en: http://Webpages. uncc. edu/richter/classes/2007/6010/readings/phishing-preprint. pdf. [19/02/ 12].

KELLEY, P., BREWER, R., MAYER, Y., CRANOR, L., y SADEH, N. (2011): «An investigation into Facebook friend grouping», en *Interact 2011*, Berlin / Heidelberg: Springer, pp. 216-233.

KRAMER, A. D., GUILLORY, J. E., y HANCOCK, J. T. (2014): «Experimental evidence of massive-scale emotional contagion through social networks» en

Proceedings of the National Academy of Sciences (PNAS) vol. 111, n. 24, pp. 8788 - 8790. Disponible en: http://www. pnas. org/content/111/24/8788. full. [12/11/2014].

KRAMM, A. (2011): «The field site as a tool: mixed methods in social network studies», en *Graduate Journal of Social Science,* vol. 8, n. 3, pp. 127-141.

— (2012): «The Field Site as a Tool: Insights in Privacy Protection Mechanisms of OSN Users», working paper at 4S/EASST, Copenague, octubre de 2012. Disponible en: http://www-wordpress. sit. fraunhofer. de/dipo/wp-content/uploads/sites/6/2013/03/4s_ EASST. pdf. [14/11/2012].

LAMPE, C., ELLISON, N. B. y STEINFIELD, C. (2008): «Changes in use and perception of Facebook», en *Proceedings of the 2008 ACM conference on Computer supported cooperative work (CSCW'08)* San Diego, California: ACM Press, pp. 721-730.

LAMPINEN, A., LEHTINEN, V., LEHMUSKALLIO, A., y TAMMINEN, S. (2011): «We're in it Together: Interpersonal Management of Disclosure in Social Network Services», en *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems, CHI 2011*, Session: Privacy Mayo, 7-12 de 2011, Vancouver, BC, Canada, Nueva York, NY: ACM Press, pp. 3217-3226.

LAMPINEN, A., TAMMINEN, S. y OULASVIRTA, A. (2009): «All my people right here, right now»: management of group co-presence on a social networking site», en *GROUP'09*, New York, NY: ACM Press, pp. 281- 290.

LANGE, P. G. (2007): «Publicly Private and Privately Public: Social Networking on Youtube», en *Journal for Computer Mediated Communication*, vol. 13, n. 1, pp. 361-380; Nippert-Eng, C. (2007): «Privacy in the United States: Some Implications for Design Privacy in the United States», en *International Journal of Design*, vol. 1, n. 2, pp. 1-10.

LENHART, A. y MADDEN, M. (2007): «Teens, privacy and online social networks: how teens manage their online identities and personal information in the age of myspace», en *Pew Internet and American Life Project*, Washington, DC. Disponible en: http://www. atg. wa. gov/uploadedFiles/Another/Office_Initiatives/ Teens, Privacy%20and%20Social%20Networks. pdf. [27/11/2012].

LEWIS, K., KAUFMAN, J. y CHRISTAKIS, N. (2008): «The taste for privacy: an analysis of college student privacy settings in an online social network», en *Journal of Computer- Mediated Communication*, vol. 14, n. 1, pp. 79-100

LILLEY, S., GUMBUS A. y GRODZINSKY, F. (2010): «Ethical Implications of Internet Monitoring: A Comparative Study», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds): The «backwards, forwards and sideways» changes of ICT, 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010) 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgili, pp. 597.

LIPFORD, H. R., DOU, W., JEONG, D., STUKES, F., RIBARSKY, W., and CHANG, R. (2009): «Recovering Reasoning Process From User Interactions», en *Computer Graphics and Applications*, vol. 29, n. 3, pp. 52-51. Disponible en: http://viscenter.uncc.edu/sites/viscenter.uncc.edu/files/CVC-UNCC-09-03.pdf. [09/11/2012].

LIPFORD, H. R., DOU, W., JEONG, D., STUKES, F., RIBARSKY, W., y CHANG, R. (2009): «Recovering Reasoning Process from User Interactions», en *Computer Graphics and Applications*, vol. 29, n. 3, pp. 52-51. Disponible en: http://viscenter.uncc.edu/sites/viscenter.uncc.edu/files/CVC-UNCC-09-03.pdf.[09/11/2012].

LIPFORD, H. R., KARR-WISNIEWSKI, y P. WILSON, D. (2011): «A new social order: mechanisms for social network site boundary regulation», en *Proceedings of the International Information Systems Conference AMCIS 2011*, del 4 al 8 de agosto de 2011, Detroit, Michigan. Disponible en: http://www. proceedings. com/12585. html. [14/11/2012].

MACKEY, R. (2009): *Thursday: Updates on Iran's disputed election*, en *The New York Times,* 18 de junio de 2009. Disponible en: http://thelede. blogs. nytimes. com/2009/06/18/latest-updates-on-irans-disputed-election-2/?hpw. [23/09/2011]

MADDEN, M. y SMITH, A. (2010): «Reputation management and social media», en *Pew Internet & American Life Project*, Washington, DC. Disponible en: http://pewinternet. org/Reports/2010/Reputation-Management. aspx. [14/03/2011].

MCCARTHY, C. (2007): «Facebook users pretty willing to add strangers as "friends"», en *CNET,* 13 de agosto de 2007. Disponible en: http://www.cnet. com/news/facebook-users-pretty-willing-to-add-strangers-as-friends/ [12/07/2009]

MILLER, A. S. (2013): *Speculative Grace. Bruno Latour and Object-Oriented Theology.* Nueva York: Fordham University Press.

NISSENBAUM, H. (2004): *Privacy as contextual integrity.* Washington Law Review, n. 79, vol. 1, pp. 119-158.

NOË, A. (2010): *Fuera de la cabeza,* Barcelona: Kairós, p. 145. Citado en Aladro Vico, E. (2012): «Cultura y distribuciones humanas», en *Estudios sobre el mensaje periodístico,* vol. 18, número especial, octubre de 2012, pp. 35- 43, p. 35.

NORBERG, P. A., HORNE, D. R. y HORNE, D. A. (2007): «The privacy paradox: personal information disclosure intentions versus behaviors», en *Journal of Consumer Affairs*, vol. 41, n. 1, pp. 100-126.

PARISER, E. (2011): *The Filter Bubble: What the Internet Is Hiding from You*, London: Viking. WESTER, M. y SANDIN, P. (2010): «Privacy and the public: perception and acceptance of various applications of ICT», en ARIAS-OLIVIA, M., WARD BYNUM, T., ROGERSON, S., TORRES-CORONAS, T. (eds): The «backwards, forwards and sideways» changes of ICT, 11th In-

ternational conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010) 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp. 597, pp. 581-586.

PARRISH, J. L. (2010): «PAPA knows best: principles for the ethical sharing of information on social networking sites», en *Ethics and Information Technology*, vol. 12, n. 2, pp. 187-193.

POLLER, A.; ILYES, P. y KRAMM, A. (2013): «Designing privacy-aware online social networks - A reflective socio-technical approach» en *CSCW'13 Measuring Networked Social Privacy Workshop*, 23 y 27 de febrero de 2013, San Antonio, Texas, United Estates. Disponible en: http://testlab. sit. fraunhofer. de/downloads/Publications/poller_osn_design_cscw13_workshop_camera_ready_rot. pdf. [20/01/2014].

POLLER, A.; ILYES, P.; KOCKSCH, L. y KRAMM, A. (2014): «Investigating OSN Users' Privacy Strategies with ROSE- A Research Tool for Online Social Environments». *CSCW'14,* Poster, Companion, Baltimore, 2014. Disponible en: https://dipo. sit. fraunhofer. de/wp-content/uploads/sites/6/2014/02/cscw14-poster-final-rot. pdf. [15/01/2014].

RAYNES-GOLDIE, K. (2010): «Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook», en *First Monday*, vol. 15, n. 1. Disponible en: firstmonday. org/htbin/cgiwrap/bin/ojs/index. php/fm/article/view/2775/2432. [27/11/2012].

REYNOLDS, B., VENKATANATHAN, J., GONCALVES J. y KOSTAKOS V. (2011): «Sharing ephemeral information in online social networks: privacy perceptions and behaviours», en Proceedings *of the 13th IFIP TC13 Conference on Human-Computer Interaction-Interact 2011*, June 16, 2011, Lisbon, Portugal: Springer, pp. 204-215.

ROBARDS, B. (2010): «Randoms in my bedroom: negotiating privacy and unsolicited contact on social network sites», en *PRism Online PR Journal*, vol. 7, n. 3, pp. 1-12. Disponible en: http://www. doaj. org/doaj?func=abstractandid=614104. [09/02/2013].

SLEEPER, M., BALEBAKO, R., DAS, S., MCCONAHY, A. L., WIESE, J. y CRANOR, L. F. (2013): «The Post that Wasn't: Exploring Self-Censorship on Facebook», en *CSCW13*, 23-27 de febrero, 2013, San Antonio, Texas, Estados Unidos.

SOPHOS (2007): «Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieve», 14 de agosto de 2007. Disponible en: https://www. sophos. com/en-us/press-office/press-releases/2007/08/facebook. aspx. [12/11/2009]

STRATER, K., y LIPFORD, H. R. (2008): «Strategies and struggles with privacy in an online social networking community», en *Proceedings of the 22nd British HCI Group 2008*, Liverpool, United Kingdom: ACM.

STUTZMAN, F. (2011): «Networked information behavior in life transition». Disponible en: http://media. proquest. com/media/pq/classic/doc/2374161701/

fmt/ai/rep/NPDF?_s=yGsXK32hWfSQVGkfoQHfyyp0keE%3D. [27/07/2012]; DEY, R., JELVEH, Z. y ROSS, K. (2012): *Op. cit.;* YOUNG, A. L. y QUAN-HASSE, A. (2013): *Op. cit.*

STUTZMAN, F. y KRAMER-DUFFIELD, J. (2010): «Friends Only: Examining a Privacy- Enhancing Behavior in Facebook», en *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, *CHI 2010*: *Privacy*, Austin, Texas: ACM Press, pp. 1553-1562.

STUTZMAN, F., GROSS, R. and ACQUISTI, A. (2012): «Silent Listeners: The Evolution of Privacy and Disclosure on Facebook», en *Journal of Privacy and Confidentiality*, vol. 4, n. 2, pp. 7-41.

STUTZMAN, F., VITAK, J., ELLISON, N. B., GRAY, R. y LAMPE, C. (2012a): «Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook», en *Proceedings of the 6th annual International Conference on Weblogs and Social Media (ICWSM)* Washington, DC: Association for the Advancement of Artificial Intelligence.

SUNDÉN, J. (2003): *Material Virtualities: Approaching Online Textual Embodiment*, New York: Peter Lang.

TEMPLETON, H. (2009): «Social media benefity trump security fears», en Medill Reports Chicago. Disponible en http://news. medill. northwestern. edu/chicago/. [12/02/2010]

THE INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (2008): *Report and Guidance on Privacy in Social Network Services. «Rome Memorandum»*, aprobado el 4 de marzo de 2008, Roma, Italia. Disponible en: www. datenschutzberlin. de/attachments/461/WP_social_network_ services. pdf. [17/05/2010].

TUFECKI, Z. (2008): «Can you see me now? Audience and disclosure regulation in online social network sites», in *Bulletin of Science, Technology and Society,* vol. 28, n. 20, pp. 20-36.

VISEU, A., CLEMENT, A., y ASPINALL, J. (2004): «Situating Privacy Online», en *Information, Communication and Society*, vol. 7, n. 1, pp. 92-114.

WANG, Y., NORCIE, G., KOMANDURI, S., ACQUISTI, A., LEON, P. G. y CRANOR, L. F. (2011) «I regretted the minute I pressed share: A qualitative study of regrets on Facebook», en *Proceedings of the Seventh Symposium on Usable Privacy and Security, SOUPS «11*, 10:1-10:16, Nueva York.

WISNIEWSKI, P., LIPFORD, H. y WILSON, D. (2012): «Fighting for my space: coping mechanisms for SNS boundary regulation», en *CHI '12,* Nueva York: ACM Press, pp. 609-618.

YOUNG, A. L. y QUAN-HASSE, A. (2013): «Privacy protection strategies on Facebook», en *Information, Communication and Society*, vol. 16, n. 4, pp. 479-500.

YOUNG, A. L., GURZICK, D. y QUAN-HAASE, A. (2011): «Online multi-contextual analysis: (re)connecting the social network site user with their profi-

le», in B. K. Daniel (ed.): *Handbook of Research on Methods and Techniques for Studying Virtual Communities: Paradigms and Phenomena*, Hershey, PA: IGI Global, pp. 542-554.

YOUNG, A. L. y QUAN-HAASE, A. (2009): «Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook», en *Proceedings of the 4th International Conference on Communities and Technologies*, pp. 265-274.

ZIMMER, M. (2007): «Privacy and surveillance in Web 2. 0: A study in contextual integrity and the emergence of Netaveillance», en *Society for Social studies of Science*. Disponible en: http://www. academia. edu/3943172/Privacy_ and_Surveillance_in_Web_2. 0_A_study_in_Contextual_Integrity_and_the Emergence_of_Netaveillance.

— (2010):«Social networking and the perception of privacy within the millennial generation Web 2. 0», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds): *The «backwards, forwards and sideways» changes of ICT, 11th International conference on the Social and Ethical Impacts of Information and Communication Technology* (E*THICOMP*2010) 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp. 597, pp. 273-279.

Instituciones y fuentes oficiales:

EUROPEAN COMMISSION (2011): *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union*. Disponible en: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359 _en.pdf.[12/02/12]

INSTITUTO FRAUNHOFER PARA LA SEGURIDAD DE LA INFORMACIÓN (SIT) se puede consultar su página Web: https://www.sit.fraunhofer.de/

INSTITUT FÜR KULTURANTHROPOLOGIE UND EUROPÄISCHE ETHNOLOGIE, Goethe-Universität Frankfurt am Main. www.uni-frankfurt. de/39023844

CAPÍTULO IX

Bibliografía:

BADÍA, E. (2012) «Marco conceptual. Derecho ¿pendiente?», en PÉREZ, J. y BADÍA, E., (coord.): *El debate sobre la privacidad y seguridad en la red: regulación y mercados*, Madrid: Fundación Telefónica, Ariel, pp. 1-22.

BESMER, A. y RICHTER LIPFORD, H. (2010): «Moving Beyond Untagging: Photo Privacy in a Tagged World,» en MYNATT, D. SCHONER, G. FITZPATRICK, S. E. HUDSON, W. K. EDWARDS y T. RODDEN (eds.): *Proc. CHI 2010*, pp. 1563-1572.

BINDER, J., HOWES, A., y SUTCLIFFE, A. (2009): «The problem of conflicting social spheres: Effects of network structure on experienced tension in social network sites», en *Proceedings of CHI 2009*, Boston: ACM Press, pp. 965-974.

BOLTER, D. J. y GRUSIN, P. (1999): «Immediacy, Hypermediacy, and Remediation», en *Remediation: Understanding New Media*. Massachusetts: MIT Press. Traducción al castellano a cargo de Aladro Vico, E. (2011): «Inmediatez, hipermediación, Remediación», en Cuadernos de Información y Comunicación, vol. 16, pp. 19-57.

BOYD, D. (2008): «Facebook's Privacy Trainwreck: Exposure, Invasion and Social Convergence», en *Convergence*: The International Journal of Research into New Media Technologies, vol. 14, pp. 13-20.

BOYD, D. y HARGITTAI, E. (2010): «Facebook's Privacy Settings: Who Cares?», en *First Monday*, vol. 15, n. 8.

CASTAÑARES, W. (2012): «Nuevos medios, nuevas sociedades. La investigación en comunicación hoy», en Mirna, M.; Sepúlveda, L. y Garzón, J. A. (ed.): *Convergencia digital y medios de comunicación*. Méjico: Universidad Autónoma de Nuevo León.

CASTELLS, M. (2001): *La galaxia Internet,* Barcelona: Areté.

CEBRIÁN, J. L. (1998): *La Red*. Madrid. Santillana.

CITRON, D. (2011): «Aligning Privacy Expectations with Technical Tools», en *Concurring Opinions - The Law, the Universe and Everything,* 10 de abril, 2001. Disponible en: http://www.concurringopinions.com/archives/2011/04/aligning-privacy-expectations-with-technical-tools.html.[23/05/2013].

Diccionario de la lengua española (22. ª ed.) Real Academia Española, 2001.

DOURISH, P. y PALEN, L. (2003): «Unpacking «privacy» for a networked world», en *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI «03)* New York, NY: ACM Press, pp. 129-136, p. 133.

GRAUX, H.; AUSLOOS, J. y VALCKE, P. (2012): «El derecho al olvido en la era de Internet» en Pérez, J. y Badía, E., (coord.): *El debate sobre la privacidad y la seguridad en la Red: regulación y mercados,* Madrid: Ariel, pp. 107-124.

GROSS, R. y ACQUISITI, A. (2005): «Information revelation and privacy in online social networks», en *Proceedings of ACM Workshop on Privacy in the Electronic Society'05*, Nueva York: ACM Press, pp. 71-80.

HULL, G., LIPFORD H. R. y LATULIPE, C. (2010): «Contextual gaps: privacy issues on Facebook», en *Ethics and Information Technology,* vol. 13, n. 4, pp. 289-302. Disponible en: pages.uoregon.edu/. . . /hull_context_privacy_fb.pdf.[12/11/2013].

ILYES, P. (2012): *V Encuentro internacional de investigadores en información y comunicación*, 24 y 25 de septiembre de 2012, Facultad de Ciencias de la Información, Universidad Complutense, Madrid. Más información en: http://www. ucm. es/per3.

LAMPE, C., ELLISON, N. B. y STEINFIELD, C. (2008): «Changes in use and perception of Facebook», en *Proceedings of the 2008 ACM conference on Computer supported cooperative work (CSCW «08)* San Diego, California: ACM Press, pp. 721-730.

LILLEY, S., GUMBUS A. y GRODZINSKY, F. (2010): «What matters to non-experts about property and privacy rights?», en ARIAS-OLIVIA, M., WARD BYNUM, T., ROGERSON, S., TORRES-CORONAS, T. (eds): *The «backwards, forwards and sideways» changes of ICT*, 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010) del 14 al 16 abril, 2010, Tarragona, España: Universitat Rovira i Virgily, pp. 375-382.

LIPFORD, H. R., DOU, W., JEONG, D., STUKES, F., RIBARSKY, W., y CHANG, R. (2009): «Recovering Reasoning Process From User Interactions», en Computer Graphics and Applications, vol. 29, n. 3, pp. 52-51. Disponible en: http://viscenter.uncc.edu/sites/viscenter.uncc.edu/files/CVC-UNCC-09-03.pdf.[09/11/2012].

LIPFORD, H. R., HULL, G., LATULIPE, C., BESMER, A., y WATSON, J. (2009): «Visual flows: Contextual integrity and the design of privacy mechanisms on social network sites», en *Proceedings of the Workshop on Security and Privacy in Online Social Networking, IEEE International Conference on Social Computing* (SocialCom) agosto de 2009. Disponible en: http://cse. stfx. ca/~socialcom09/ [14/05/2012]

LIPFORD, H. R., KARR-WISNIEWSKI, y P. WILSON, D. (2011): «A new social order: mechanisms for social network site boundary regulation», en *Proceedings of the International Information Systems Conference AMCIS 2011*, del 4 al 8 de agosto de 2011, Detroit, Michigan. Disponible en: http://www.proceedings.com/12585.html.[14/11/2012]

LIPFORD, H. R., WISNIEWSKI, P., LAMPE, C., KISSELBURGH, L. y CAINE, K. (2012): «Reconciling Privacy with Social Media», en *Proceedings of the 2012 ACM Conference on Computer Supported Corporative Work Companion*, pp. 19-29.

MASON, R. O. (1986): «Four ethical issues of the information age», en *MIS Quarterly*, n. 10, vol. 1, pp. 5-12, p. 12

NISSENBAUM, H. (2004): *Privacy as contextual integrity.* Washington Law Review, n. 79, vol. 1, pp. 119-158

— (1998): «Protecting privacy in an Information Age: The problem of privacy in public», en *Law and Philosophy*, vol. 17, n. 5-6, pp. 559-596.

PARRISH, J. L. (2010): «PAPA knows best: principles for the ethical sharing of information on social networking sites», en *Ethics and Information Technology*, vol. 12, n. 2, pp. 187-193.

PRENSKY, M. (2001): «Digital Natives, Digital Immigrants, Part II: Do They Really Think Differently», en *On the Horizon,* vol. 9, n. 6, pp. 1-6. Disponi-

ble en: www.marcprensky.com/writing/Prensky%20%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part2.pdf.[12/10/2012]

— «Digital Natives, Digital Immigrants», en *On the Horizon,* vol. 9, n. 5, pp. 1-6.

— (2009): «Homo sapiens digital: de los inmigrantes y nativos digitales a la sabiduría digital», en Aparici, R. (cord.): *Conectados en el ciberespacio*, Madrid: UNED, pp: 93-106.

SIMMEL, G. (1986): *Sociología. Estudios sobre las formas de socialización*. Madrid: Alianza Editorial.

ZIMMER, M. (2007): «Privacy and surveillance in Web 2. 0: A study in contextual integrity and the emergence of Netaveillance», en *Society for Social studies of Science*. . Disponible en: http://www.academia.edu/3943172/Privacy_and_Surveillance_in_Web_2.0_A_study_in_Contextual_Integrity_and_the Emergence_of_Netaveillance.

Webgrafía:

EUROPEAN COMMISSION (2011): *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union*. Disponible en: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.[12/02/12]

CAPÍTULO X

Bibliografía:

ALTMAN, I.(1975): *The environment and social behavior.* Monterey, CA: Brooks/Cole.

BARNES, S. B. (2006): «A privacy paradox: social networking in the United States», in *First Monday*, vol. 11, n. 9, http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312 [29/05/2014].

BOYD, D. (2006): «Friends, friendsters, and myspace top 8: writing community into being on social network sites», in First Monday, n. 11, vol. 12. Available at: http://www.danah.org/papers/FriendsFriendsterTop8.pdf.[02/10/2013].

— (2008): «Taken out of context: Americam Teen Sociability in Networked Publics». Available at: http://www.danah.org/papers/TakenOutOfContext.pdf, p. 3. [3/10/2014].

BOYD, D. M. and ELLISON, N. B. (2007): «Social Network Sites: Definition, History, and Scholarship», in *Journal of Computer-Mediated Communication*, n. 13, vol. 1, 210-230.

BUCHMANN, J. (ed.) (2013): *Internet Privacy: Taking opportunities, assesing risk, building trust* (Acatech – Deutsche Akademie der Technikwissenschaften, acatech STUDY) Heidelberg *et al.:* Springer Verlag.

BUCHMANN, J. (ed.) (2013): *Op. cit.;* BUCHMANN, J. (ed.) (2013): Internet Privacy – Options for adequate realisation (acatech – Deutsche Akademie der Technikwissenschaften STUDY) Heidelberg *et al.:* Springer Verlag;

CAPURRO, R. (2005): «Privacy. An intercultural perspective», *Ethics and Information Technology*, vol. 7 n. 1, pp. 37-47.

CAVOUKIAN, A. (2009): Privacy by Design. Office of the Information and Privacy Commissioner. Available at: www.privacybydesign.ca/content/uploads/2009/01/privacybydesign.pdf.[3/10/2014].

COURT OF JUSTICE OF THE EUROPEAN UNION (2014): *Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*. Available at: http://europa. eu/rapid/press-release_CJE-14-70_en. htm [12/12/2014].

DIVSI (2012): *DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet*, Hamburg: Deutsches Institut für Vertrauen und Sicherheit im Internet(DIVSI).

EUROPEAN COMMISSION (2011): *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union*. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.[01/08/ 2014]

— (2012): *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*. Available at: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htmeuropeancommission [27/12/2013].

— (2012): *Data protection reform: Frequently asked question. Why do we need to reform the EU data protection rules?* Available at: http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=fr [12/02/2014].

— *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data (General Data Protection Regulation)*. 2012/0011 (COD).

EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION (1995) «Directive 95/46/EC», *Official Journal of the European Union*, L 281, 0031-0050.

FAIRWEATHER, B.; ASHMAN, H. and WAHLSTROM, K. (2011): «Brain computer interfaces: a technical approach to supporting privacy» in ROGERSON, Simon; ARIAS-OLIVA, Mario; WARD BYNUM, Terrel and TORRES-CORONAS, Teresa (eds.): *The «backwards, forwards and sideways» changes of ICT*. Proceedings of the eleventh international conference, Ethicomp 2010. Universidad Rovira i Virgili, Spain, pp. 580-586.

GOVANI, T. and PASHLEY, H. (2005): «Student awareness of the privacy implications when using Facebook», Privacy Poster Fair at the School of Library and Information Science, Pittsburgh PA: Carnegie Mellon University Press.

HULL, G., LIPFORD, H. R., and LLATULIPE, C. (2010): «Contextual gaps: privacy issues on Facebook», in *Ethics and Information Technology*, n. 13, vol. 4, pp. 289-302.

HUSTINX, P. (2010): «Privacy by design: delivering the promises», in *Identity in the Information Society*, vol. 3, n. 2, pp. 253-265.

JOHNSON, D. (2009): *Computer Ethics*, Pearson, New Jersey.

LAMPE, C., ELLISON, N. B., and STEINFIELD, C. (2008): «Changes in use and perception of Facebook. » In CSCW'08. ACM Press, San Diego, pp. 721-730.

LIPFORD, H. (2010): *Improving Privacy on Social Network Sites*. University of North Carolina at Charlotte. Disponible en: http://www.cs.vt.edu/files/files/Seminar/2010/Lipford-VTseminar.pdf [01/10/2014].

LIPFORD, H. and BESMER, A. (2010): «Moving beyond untagging: photo privacy in a tagged world», in MYNATT, E. D. et alt. (eds.) *CHI*, pp. 1563-1572.

MADDEN, M. & SMITH, A. (2010): «Reputation management and social media», in *Pew Internet & American Life Project,* Washington. Available at: http://www.pewinternet.org/2010/05/26/reputation-management-and-social-media/ [01/11/2014]

MASON, R.O. (1986): «Four ethical issues of the information age», en *MIS Quarterly Minnesota*. n. 10, vol. 1, pp. 5-12.

NISSENBAUM, H. (2010): *Privacy in Context*, Standford, CA: Stanford University Press,

— (2004):«Privacy as contextual integrity», *Washington Law Review,* n. 79, vol. 1.

NISSSEMBAUM, H. and BAROCAS, S. (2009): «On Notice: The Trouble with Notice and Consent», in *Media, Culture, and Communication*. New York: New York University.

PALEN, L. and DOURISH, P. (2003): «Unpacking «privacy» for a networked world», in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI «03)* New York, NY: ACM. pp. 129-136.

PARRISH, J. L. (2010): «PAPA knows best: principles for the ethical sharing of information on social networking sites», in *Ethics and Information Technology*, vol. 12, n. 2, pp. 187-193.

POSTMAN, N. (1990): *Informing Ourselves to Death, Address Before the German Informatics Society.* Available at: www.eff.org/Net-culture/Criticisms/informing_ourselves-to-death.paper.

REGAN, P. (2003): «Safe Harbours or free frontiers? Privacy and transborder data flows», in *Journal of Social Issues*, 59, pp. 263-282.

RÖSSLER, B. (2005): *The value of privacy*, Cambridge, MA: Polity Press.

YOUNG, A. L., GURZICK, D. and QUAN-HAASE, A. (2011): «Online multi-contextual analysis: (re)connecting the social network site user with their profile», in B. K. Daniel (ed.) *Handbook of Research on Methods and Tech-*

niques for Studying Virtual Communities: Paradigms and Phenomena, IGI Global, Hershey, PA, pp. 542-554.

WEBER, R. H. (2011): «The right to be forgotten. More than a Pandora's Box», in *Jipitec*, n. 2, vol. 2, pp. 120-130.

WESTER, M. and SANDIN P. (2011): «Privacy and the public – perception and acceptance of various applications of ICT», In ARIAS-OLIVIA, M., WARD BYNUM, T., ROGERSON, S., TORRES-CORONAS, T. (eds). *The «backwards, forwards and sideways» changes of ICT, 11th International conference on the Social and Ethical Impacts of Information and Communication Technology.* Proceedings of the twelfth international conference, Ethicomp 2011, Sheffield University, pp. 580-586.

YOUNG, A. L. and QUAN-HASSE, A. (2013) «Privacy protection strategies on Facebook», in Information, Communication and Society, n. 16, vol. 4, pp. 479-500.

ANEXOS

ANEXO 1

1. Artículos seleccionados y analizados en el estudio:

1. ACQUISITI, A. and GROSS, R. (2005): «Information revelation and privacy in online social networks», in *Proceedings of ACM Workshop on Privacy in the Electronic Society'05,* Nueva York: ACM Press, pp. 71-80.
2. ACQUISTI, A. (2009): «Nudging Privacy: The Behavioral Economics of Personal Information», in *IEEE Security and Priv*acy, vol. 7, n. 6, pp. 82-85.
3. ACQUISTI, A. and GROSS, R. (2006): «Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook», in G. Danezis and P. Golle (eds.): *Privacy Enhancing Technologies, 6th International Workshop PET 2006,* Berlin and Heidelberg: Springer, pp. 36-58.
4. ACQUISTI, A. and GROSSKLAGS, J. (2004): «Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior», in *2nd annual Workshop on Economics and Information Security.* Available at: http://www.cpppe.umd.edu/rhsmith3/papers/Final_session6_acquisti.grosskl ags.pdf [27/05/2012].
5. ACQUISTI, A. and GROSSKLAGS, J. (2005): «Privacy and Rationality in Individual Decision Making», in *IEEE Security and Priv*acy, vol. 3, n. 1, pp. 26-33.
6. Agencia Española de Protección de Datos (AEPD) e Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2009): *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las red*es, February, 2009. Available at: https://www.agpd.es/portalWebAGPD/canaldocumentacion/publicaciones/common/Estudios/estudio_inteco_aped_120209_redes_sociales.pdf [29/03/2013].
7. AIBAR, E. (2010): «A Critical Analysis of Information Society. Conceptualizations from an STS Point of View», in *TripleC,* vol. 8, n. 2: pp. 177-182.
8. ALBORNOZ, M. B. (2008): «Cibercultura y las nuevas nociones de privacidad», en *Nómadas,* n. 28, Colombia: Universidad Central Colombia.
9. American Management Association and the ePolicy Institute (2008): *Electronic monitoring and surveillance 2007 survey,* available at: www.amanet.org [22/11/2010].
10. AWAD, N. F. and M. S. KRISHNAN (2006): «The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the

Willingness to be Profiled Online for Personalization», in *MIS Quarterly,* vol. 30, n. 1, pp. 13-28.

11. BAILEY, J. (2009): «Life in the fishbowl: Feminist interrogations of Webcamming», in *Lessons from the identity trail: Anonymity, privacy and identity in a networked society,* Oxford: OUP, pp. 283-301.
12. BAILEY, J. and KERR, I. (2007): «The experience capture experiments of Ringley and Mann», in *Ethics and Information Technology,* Springer Netherlands, vol. 9, n. 2, pp. 129-139
13. BARNES, S. B. (2006): «A privacy paradox: social networking in the United States», in *First Monday,* vol. 11, n. 9. Available at: http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312 [29/05/2014].
14. BENEVENUTO, F., RODRIGUES, T., CHA, M. and ALMEIDA, V. (2009): «Characterizing user behavior in online social networks», in *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference,* New York: ACM Press, pp.49-62.
15. BERENDT, B., GÜNTHER, O. and SPIEKERMANN, S. (2005): «Privacy in E-Commerce: Stated Preferences vs. Actual Behavior», in *Communications of the ACM,* vol. 48, n. 4, pp. 101-106.
16. BESMER, A. and RICHTER LIPFORD, H. (2010): «Users (Mis)conceptions of Social Applications», in *Proceedings of Graphics Interface GI 2010.*
17. BESMER, A. and RICHTER LIPFORD, H. (2010): «Moving Beyond Untagging: Photo Privacy in a Tagged World,» in Mynatt, D. Schoner, G. Fitzpatrick, S. E. Hudson, W. K. Edwards and T. Rodden (eds.): *Proc. CHI* 2010, pp. 1563-1572.
18. BEYE, M., JECKMANS, A., ERKIN, Z., HARTEL, P., LAGENDIJK, R. and TANG, Q. (2010): «Literature Overview - Privacy in Online Social Networks», in *Technical Report TR-CTIT-10-36,* Enschede: Centre for Telematics and Information Technology University of Twente.
19. BGH (2013): Bundesgerichtshof (BGH): *Judgement of 24.1.2013* (Az. III ZR 98/12): Karlsruhe.
20. BIGGE, R. (2006): «The cost of (anti-)social networks: Identity, agency and neo-luddites», in *First Monday,* vol. 8.
21. BINDER, J., HOWES, A. and SUTCLIFFE, A. (2009): «The problem of conflicting social spheres: Effects of network structure on experienced tension in social network sites», in *Proceedings of CHI 2009,* Boston: ACM Press, pp. 965-974.
22. BISSETT, A. (2005): «Developing an Ethics Policy for Research that uses ICT», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Looking back to the future.* Linköping University, Linköping (Suecia).

23. BOBER, J. W. (2004): «Ethics of Information Societies», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

24. BOCZKOWSKI, P. and LIEVROUW, L. A. (2008): «Bridging STS and Communication Studies: Scholarship on Media and Information Technologies», in E. J. Hackett, O. Amsterdamska, M. Lynch and J. Wajcman (eds.): *Handbook of Science and Technology Studies,* Cambridge, MA: MIT Press, pp. 951-977.

25. BONNER, W. T. (2010): «An Exploration of the Loss of Context on Questions of Ethics Around Privacy and its Consequences», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010) 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily.

26. BOYD D. and DONATH, J. (2004): «Public Displays of Connection», in *BT Technology Journal,* vol. 22, n. 4, pp. 71-82.

27. BOYD, D. (2004): «Friendster and Publicly Articulated Social Networks», *working paper SIGCHI Conference on Human Factors in Computing Systems,* Vienna, Austria.

28. BOYD, D. (2006): «Friends, friendsters, and myspace top 8: writing community into being on social network sites», in *First Monday,* vol. 11, n. 12. Available at: http://www.danah.org/papers/FriendsFriendsterTop8.pdf [27/11/2012].

29. BOYD, D. (2007): «Social Network Sites: Public, Private, or What?», in *Knowledge Tree,* 13 May, 2007. http://kt.flexiblelearning.net.au/tkt2007/?page_id=28

30. BOYD, D. (2007): «Why Youth (Heart): Social Network Sites: The Role of Networked Publics in Teenage Social Life», in D. Buckingham (ed.): *Youth, Identity, and Digital Media,* Cambridge, MA: MIT Press, pp. 119-142.

31. BOYD, D. (2008): «Facebook's Privacy Trainwreck: Exposure, Invasion and Social Convergence», in *Convergence: The International Journal of Research into New Media Technologies,* vol. 14, pp. 13-20.

32. BOYD, D. (2008): «Taken Out of Context: American Teen Sociality in Networked Publics», PhD Dissertation, University of California-Berkeley, School of Information. Available at: http://www.danah.org/papers/TakenOutOfContext.pdf [27/11/2012].

33. BOYD, D. (2013): «Networked Privacy», in *Surveillance and Society,* vol. 10, n. 3/4, pp. 348-350.

34. BOYD, D. and Ellison, N. B. (2013): «Sociality through social network sites», in Dutton, W. H. (ed.): *The Oxford Handbook of Internet Studies,* Oxford: Oxford University Press, pp. 151-172.

35. BOYD, D. and ELLISON, N. B. (2007): «Social Network Sites: Definition, History, and Scholarship» in *Journal of Computer-Mediated Communication,* vol. 13, n. 1, pp. 210-230.

36. BOYD, D. and HARGITTAI, E. (2010): «Facebook's Privacy Settings: Who Cares?», in *First Monday,* vol. 15, n. 8.

37. BOYD, D. and J. HEER. (2006): «Profiles as Conversation: Networked Identity Performance on Friendster», in *Proceedings of the Hawaii International Conference on System Sciences 2006HICSS-39,* Kauai, Hawaii.

38. BOYD, D. and JENKINS, H. (2006): «MySpace and Deleting Online Predators Act (DOPA)», in *MIT Tech Talks,* Available at: http://www.danah.org/ papers/MySpaceDOPA.html [26/05/2009].

39. BOYD, D. and MARWICK, A. (2011): «Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies», in *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society,* September 2011. Available at: http://ssrn.com/abstract=1925128 [27/12/2012].

40. BOYD, D. and MARWICK, A. E. (2010): «I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience», in *New Media and Society,* vol. 13, n. 1, pp. 114-133.

41. BRANDTZAEG, P. B., LÜDERS, M. and SKJETNE, J. H. (2010): «Too Many Facebook «Friends»? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites», in *International Journal of Human-Computer Interaction, Special Issue: HCI and Social Computing,* vol. 26, n. 11-12, pp. 1006-1030.

42. BREITBART (2010): «Google software bug shared private online documents». Available at: http://www.breitbart.com/article.php?id=CNG.54c3200980573ae4c... [25/03/2011].

43. BUCHANAN, T., PAINE, C., JOINSON, A. N. and REIPS, U. (2007): «Development of measures of online privacy concern and protection for use on the Internet», in *Journal of the American Society for Information Sciences and Technology,* January 2007, vol. 58, n. 2, pp. 157-165.

44. BUCHMANN, J. (ed.) (2012): *Internet Privacy. Eine multidisziplinäre Bestandsaufnahme / Amultidisciplinary analysis (Acatech – Deutsche Akademie der Technikwissenschaften, acatech STUDY),* Berlin: Springer.

45. BUCHMANN, J. (ed.) (2013): *Internet Privacy: Taking opportunities, assessing risk, building trust (Acatech – Deutsche Akademie der Technikwissenschaften, acatech STUDY),* Heidelberg *et al.:* Springer Verlag.

46. BYNUM, T. W. (2008): «The Nature of the Universe, Human Nature and Contemporary Information Ethics», en Ward Bynum, T., Rogerson, S. (eds.): *Living, working and learning beyond technology* (ETHICOMP 2008), International conference on the Social and Ethical Impacts of Information and Communication Technology, 24-26 September 2008, en Mantua Italia: University of Pavia.

47. CACIOPPO, J. T., FOWLER, J. H., CHRISTAKIS, N. A. (2009):«Sólo en la multitud: Estructura y difusión de la soledad en una gran red social», en *Diario de la Personalidad y Psicología Social,* vol. 97, n. 6, diciembre, pp. 977-991 [doi: 10.1037/a0016076].

48. CALLON, M. (2004): «The role of hybrid communities and socio-technical arrangements in the participatory design», in *Journal of the Center for Information Studies,* vol.5, pp. 3-10.

49. CALLON, M. (2006): «What does it mean to say that economics is performative?», in *CSI Working Papers Series,* n. 005, París: Centre de Sociologie de l'Ecole des Mines / ed. La Découverte, Paris.

50. CAMP, L. J., CONNELLY, K. and SHANKAR, K. (2005): «Design for Privacy: Towards a Methodological Approach to Trustworthy Ubicomp Design», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Looking back to the future.* Linköping University, Linköping (Suecia).

51. CATANESE, S. DE MEO, P. FERRARA, E. and FIUMARA, G. (2010): «Analyzing the Facebook Friendship Graph», in *Proceedings of the 1st Workshop on Mining the Future Internet,* pp. 14-19.

52. CATHERINE, F.(2007): «Informed consent theory in information technology», en *Glocalisation: bridging the global nature of information and communication technology and the local nature of human beings* Ward Bynum, T., Rogerson, S. (eds.): *Living, working and learning beyond technology* (ETHICOMP 2007), International conference on the Social and Ethical Impacts of Information and Communication Technology, 2007, en Meiji University, Tokyo (Japón).

53. CAVOUKIAN, A. (2008): «Privacy in the Clouds: A White Paper on Privacy and Digital Identity: Implications for the Internet». Available at: http://www.ipc.on.ca/images/resources/privacyintheclouds.pdf [27/11/2012].

54. CHAI, S., y RAO, H. R. (2008): «'WiRed' senior citizens and online information privacy», en M., Ward Bynum, T., Rogerson, S. (eds.): *Living, working and learning beyond technology* (ETHICOMP 2008), International conference on the Social and Ethical Impacts of Information and Communication Technology, 24- 26 September 2008, en Mantua Italia: University of Pavia, pp. 101-110.

55. CHAU, D., PANDIT, S. WANG, S. and FALOUTSOS. C. (2007): «Parallel crawling for online social networks», in *Proceedings of the 16th international conference on World Wide Web,* New York, United States: ACM Press, pp. 1283-1284.

56. CHEW, M., BALFANZ, D. and LAURIE, B. (2008): «(Under) mining Privacy in Social Networks», Google Inc. Available at: http://w2spconf.com/2008/papers/s3p2.pdf. Under mining privacy [28/01/2012].

57. CHRISTOFIDES, E., MUISE, A. and DESMARAIS, S. (2009): «Information disclosure and control and facebook: Are they two sides of the same

coin or two different processes?», in *Cyberpsychology and Behavior,* vol. 12, n. 30, pp. 341-345.

58. CITRON, D. (2011): «Aligning Privacy Expectations with Technical Tools», *en Concurring Opinions - The Law, the Universe and Everything,* 10 de abril, 2001. Disponible en: http://www.concurringopinions.com/archives/2011/04/aligning-privacy-expectations-with-technical-tools.html [23/05/2013].

59. CLARKE, A. E. and STAR, S. L. (2008): «The Social Worlds Framework: A Theory/ Methods Package», in E. J. Hackett, O. Amsterdamska, M. Lynch and J. Wajcman (eds.): *The Handbook of Science and Technology Studies,* Cambridge MA: MIT Press, pp. 113-137.

60. COCKING, D. (2008): «Plural selves and relational identity», in van den Hoven, J. and Weckert, J. (eds.): *Information technology and moral philosophy,* Cambridge: CUP, pp. 123-141.

61. COPPOLA, N., HILTZ, S. R. and ROTTER, N. (2004): «Building Trust in Virtual Teams», in *IEEE Transactions on Professional Communication,* vol. 47, n. 2, pp. 95-104.

62. CRISTOFARO, E. D. SORIENTE, C. TSUDIK, G. and WILLIAMS. A. (2012): «Hummingbird: privacy at the time of Twitter», in IEEE Oakland 2012.

63. CUNNINGHAM, S. J. and MASOODIAN, B. (2007): «Management and usage of large personal music and photo collections», in *Proceedings of the 2007 IADIS International Conference on WWW/ Internet'07.,* Vila Real, Portugal, 5-8 October 2007, vol. 2, pp. 163-168.

64. CUNNINGHAM, S. J., MASOODIAN, M. and ADAMS, A. (2010): «Privacy issues for online personal photograph collections», in *Journal of Theoretical and Applied Electronic Commerce Research,* vol. 5, n. 2, August 2010, pp. 26-40.

65. CUNNINGHAM, S. J. and MASOODIAN, M. (2010): «Analysing user's behaviours to identify their privacy concerns», in *Workshop Proceedings of Privacy and Usability Methods Pow-wow (PUMP): 2010,* 24th BCS International Conference on Human-Computer Interaction. Dundee, UK, 6-10 September, British Computer Society.

66. DA COSTA, M., GONÇALO J. A., DA SILVA, N. S. and PAWLAK, P. (2010):«Network Tourism: A Fallacy Of Location Privacy!», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010) 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily.

67. DEBATIN, B., LOVEJOY, J. P., HORN, A. K. and HUGHES, B. N. (2009): «Facebook and online privacy: attitudes, behaviors and unintended conse-

quences», in *Journal of Computer-Mediated Communication,* vol. 19, n. 2, pp. 83-108.

68. DELOITTE (2012): *Measuring Facebook's Impact in Europe,* Executive Summary, London 2012. Available at: http://www.deloitte.com/assets/Dcom-UnitedKingdom/Local%20Assets/Documents/ Industries/TMT/uk-tmt-media-facebook-europe-economicimpact-exec-summary.pdf [04/02/2013].

69. DEY, R., JELVEH, Z. and ROSS, K. (2012): «Facebook users have become much more private: a large-scale study», in *2012 IEEE International Conference on Pervasive Computing and Communications Workshops,* Lugano, Switzerland, pp. 346-352. Available at http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?reload=true&punumber=6192378 [27/11/2012].

70. DIMICCO, J. M. and MILLEN, D. R. (2007): «Identity management: Multiple presentations of self in facebook identity», in *Proceedings of GROUP'07,* Florida: ACM Press, pp. 383-386.

71. DIMICCO, J., MILLEN, D. R., GEYER, W., DUGAN, C., BROWNHOLTZ, B. and MULLER, M. (2008): «Motivations for social networking at work», in *Proceedings of CSCW'08.* San Diego: ACM Press, pp 711-720.

72. DONATH, J. (2007): «Signals in social supernets», in *Journal of Computer-Mediated Communication,* vol. 12, n. 1, article 12. Available at: http://jcmc.indiana.edu/vol13/issue1/donath.html [27/11/2012].

73. DOURISH, P. (2004): «The Appropriation of Interactive Technologies: Some Lessons from Placeless Documents», in *Computer Supported Cooperative Work,* vol. 12, pp. 465-490.

74. DOURISH, P. (2004): «What We Talk About When We Talk About Context», in *Personaland Ubiquitous Computing,* vol. 8, n. 1, pp. 19-30.

75. DOURISH, P. and ANDERSON, K. (2006): «Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena», in *Human-Computer Interaction,* n. 21, pp. 319-342.

76. DOURISH, P. and PALEN, L. (2004): «Unpacking "privacy" for a networked world», in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'03),* New York, NY: ACM Press, pp. 129-136.

77. DOURISH, P., GRINTER, R. E., DELGADO DE LA FLOR, J. and JOSEPH, M. (2004): «Security in the Wild: User Strategies for Managing Security as an Everyday, Practical Problem», in *Personal and Ubiquitous Computing,* vol. 8 n. 6, pp. 391-401.

78. DOWD, M. (2011): «Contextualised concerns: The online privacy attitudes of young adults. Privacy and Identity Management for Life», in *IFIP Advances in Information and Communication Technology,* vol. 352, Springer, pp. 78-89.

79. DUQUENOY, P. (2004): «The missing element in an intelligent world, en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

80. DWYER C. (2007): «Digital Relationships in the 'MySpace' Generation: Results From a Qualitative Study», in *HICSS '07 Proceedings of the 40th Annual Hawaii International Conference on System Sciences,* Hawaii: IEEE Computer Society. Available at: www.computer.org/csdl/proceedings/hicss/index.html [25/01/2012].

81. DWYER, C. and HILTZ, S. R. (2008): «Designing privacy into online communities», in *Proceedings of Internet Research 9.0,* October 2008.

82. DWYER, C., HILTZ, S. and PASSERINI, K. (2007): «Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace», in *AMCIS 2007 Proceedings.* Paper 339.

83. ELLISON, N. B., STEINFIELD, C. and LAMPE, C. (2007): «The "Benefits" of Facebook- Friends: Social Capital and College Students' Use of Online Social Network Sites», in *Journal of Computer-Mediated Communication,* n. 12, pp. 1143-1168. Available at: http://jcmc.indiana.edu/vol12/ issue4/ellison.html. [27/11/2012].

84. ELLISON, N. B., VITAK, J., STEINFIELD, C., GRAY, R. and LAMPE, C. (2011): «Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment», in S. Trepte, S. and L. Reinecke (eds.): *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web,* New York: Springer, pp. 19-32.

85. *ETICA Project* (2011). http://www.etica-project.eu/

86. European Commission (2011): *Special Eurobarometer 359. Attitudes on Data Protection and Electronic Identity in the European Union.* Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf [12/02/12]

87. European Network and Information Security Agency (ENISA) (2007): *Recomendaciones y seguridad para las redes sociales online,* October, 2007. Available at: http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf [10/11/10]

88. EVANS, J. and MAHONEY, J. (2004): «Ethical Aspects of Using Digital Images of People», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

89. FANG L. and LEFEVRE. K. (2010): «Privacy wizards for social networking sites», in *WWW '10,* 351-360.

90. FARNHAM S. D. and CHURCHILL E. F. (2011): «Faceted identity, faceted lives: social and technical issues with being yourself online», in *CSCW '11,* New York, NY: ACM Press, pp. 359-368.

91. FELT, A. and EVANS, D. (2008): «Privacy protection for social networking APIs», in *Proceedings of Web 2.0 Security and Privacy 2008*. Available at: w2spconf.com/2008 [05/01/2011].

92. FERNÁNDEZ, S. (2008): «Redes sociales, fenómeno pasajero o reflejo del nuevo interactor», en Telos, n. 76, pp. 118-120.

93. FITZPATRICK, B. and RECORDON, D. (2007): «Thoughts on the social graph», in *BradFitz.com*. Available at: http://bradfitz.com/socialgraph-problem/. [27/02/2013].

94. FLECKENSTEIN, K. S. (2008): «Cybernetics, ethos, and ethics», in L. Worsham and G. A. Olson (Eds.): *Plugged in: Technology, rhetoric and culture in a posthuman age*. Cresskill, NJ: Hampton Press, pp. 3-23.

95. FLORIDI, L. (2008): «Information Ethics, its Nature and Scope», in Jeroen van den Hoven and John Weckert (eds.): *Information Technology and Moral Philosophy,* Cambridge: Cambridge University Press.

96. FOWLER, J. H. (2005): «La participación en un mundo pequeño», en Zuckerman, Alan (ed.): *Lógica de la política social*. Filadelfia: Universidad Temple, pp. 269-287.

97. FOWLEY, C. (2011): *Publishing the confidential. An ethnographic study of young Irish bloggers,* PhD Thesis, Dublin City University.

98. Fraunhofer-Institut für Sichere Informationstechnologie (2012): *Software Design for Interactional Privacy within Online Social Networks (DIPO)*. Available at: https://dipo.sit.fraunhofer.de/ [04/02/2013].

99. FREDERIC, S. and WOODROW, H. (2012): «Boundary regulation in social media», in *CSCW'12,* New York, NY: ACM Press, pp. 769-778

100. FREIDMAN, B., KAHN, P. and BORNING, A. (2008): «Value Sensitive Design and Information Systems», in Himma, K. E. and Tavani, H. T. (eds.): *The Handbook of Information and Computer Ethics*. Hoboken, NJ: John Wiley and Sons, pp. 69-101.

101. FRIEDEWALD, M. and POHORYLES, R. J. (2013): «Technology and privacy», in *Innovation: The European Journal of Social Science Research,* vol. 26, n. 1-2, pp. 1-6.

102. FUCHS, C. (2009): *Social Networking Sites and the Surveillance Society: A Critical Case Study of the Usage of studiVZ, Facebook, and Myspace by Students in Salzburg in the Context of Electronic Surveillance,* Salzburg/ Vienaa: Research Group Unified Theory of Information, UTI.

103. FUCHS, C. (2010): «StudiVZ: social networking in the surveillance society», in *Ethics and Information Technology,* vol. 12, n. 2, pp. 171-185.

104. GANANCIA, J.-G. (2010): «The Ethics Of The Generalized Suosveillance», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th International conference on the Social and Ethical Impacts of Information

and Communication Technology (ETHICOMP2010), 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp. 375-382.

105. GANASCIA, J. G. (2009): «The Great Catopticon», in *Proceedings of the 8th Computer Ethics and Philosophical Enquiry conference,* June 2009, Corfu, Greece.

106. GANDY, O. (2004): «Data mining and surveillance in the post-9/11 environment», in Ball, K. and Webster, F. (eds.): *The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Era,* London: Pluto Press, pp. 26-41.

107. GELMAN, L. (2009): «Privacy, free speech, and 'blurry-edged' social networks», in *Boston College Law Review,* n. 50, p. 1315-1344.

108. GIBSON, R. (2007): «Who's Really in Your Top 8: Network Security in the Age of Social Networking», in *SIGUCCS'07,* Orlando, Florida, p. 3.

109. GJOKA, M., KURANT, M., BUTTS, C. and MARKOPOULOU, A. (2010): «Walking in facebook: a case study of unbiased sampling of OSNs», in *Proceedings of the 29th conference on Information communications,* IEEE Press, pp. 2498-2506.

110. GJOKA, M., SIRIVIANOS, M., MARKOPOULOU, A. and YANG, X. (2008): «2Poking facebook: characterization of OSN applications», in *Proceedings of the first workshop on online social networks,* ACM PRESS, pp. 31-36.

111. GOGGINS, S. P., LAFFEY, J. and GALLAGHER, M. (2011): «Completely online group formation and development: small groups as socio-technical systems», in *Information Technology and People,* vol. 24, n. 2, pp. 104-133.

112. GOLBECK J. and HENDLER, J. (2006): «Inferring binary trust relationships in Web-based social networks», in *Transactions on Internet Technology,* New York, NY: ACM Press, vol. 6, n. 4, pp. 497-529.

113. GÓMEZ BARROSO, J. L. (2004): «A public threat to protection of privacy? Data retention requirements in the European Union», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

114. GOVANI, T. and PASHLEY, H. (2005): «Student awareness of the privacy implications when using Facebook», in *Privacy Poster Fair at the School of Library and Information Science,* Pittsburgh, PA: Carnegie Mellon University.

115. GREENGARD, S. (2008): «Privacy Matters», in *Communications of the ACM,* vol. 51, p. 2, September 2008.

116. GRIMMELMAN, J. (2009): «Saving Facebook», in *Iowa Law Review,* n. 94, pp. 1137-1206.

117. GRIMMELMAN, J. (2010): «Privacy as Product Safety», in *Widener Law Journal*. Available at: http://papers.ssrn.com/sol3/ papers.cfm?abstract_ id=1560243 [27/11/2013].

118. GRODZINSKY, F. S. and GUMBUS, A. (2005): «Internet and Productivity: Ethical Perspectives on Workplace Behaviour», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Looking back to the future*. Linköping University, Linköping (Suecia).

119. GRODZINSKY, F. S. and TAVANI, H. T. (2008): «Online File Sharing: Resolving the tensions between Privacy and Property Interests», en Ward Bynum, T., Rogerson, S. (eds.): *Living, working and learning beyond technology* (ETHICOMP 2008), International conference on the Social and Ethical Impacts of Information and Communication Technology, 24-26 September 2008, en Mantua Italia: University of Pavia.

120. GRODZINSKY, F. S. and TAVANI, H. T. (2009): «Can the 'Contextual Integrity' Model of Privacy Be Applied to Blogs and the Blogosphere?», in M. Bottis (ed.): *Eighth International Conference on Computer Ethics: Philosophy Enquiry.* Athens, Greece: Nomiki Bibliothiki, pp. 302-311. Reprinted in slightly revised form in *International Journal of Internet Research Ethics,* vol. 3, n. 1, 2010, pp. 38-47.

121. GRODZINSKY, F. S. LILLEY, S. and GUMBUS, A. (2008): «Ethical Implications of Internet Monitoring: A Comparative Study», en Ward Bynum, T., Rogerson, S. (eds.): *Living, working and learning beyond technology* (ETHICOMP 2008), International conference on the Social and Ethical Impacts of Information and Communication Technology, 24-26 September 2008, en Mantua Italia: University of Pavia.

122. GRUBBS, M. and MILNE, G. (2010): «Gender differences in privacy-related measures for young adult Facebook users», in *Journal of Interactive Advertising,* vol. 10, n. 2, pp. 28-45.

123. GÜRSES, S. and DÍAZ, C. (2013): «Two Tales of Privacy in Online Social Networks», in *IEEE Security and Privacy,* vol. 11, n. 3, pp. 29-37.

124. HAMPTON, K. N., GOULET, L. S., RAINIE, L. and PURCELL. K. (2011): «Social networking sites and our lives», *Pew Internet and American Life Project,* Washington, DC., June 2011.

125. HASHEMI, Y. (2009): «Facebook's privacy policy and its third-party partnerships: Lucrativity and liability», in *Boston University Journal of Science and Technology Law,* n. 15, pp. 140-161.

126. HEMPEL, J. (2005): «The MySpace Generation», in *Business Week,* n. 3963, pp. 86-100.

127. HERMAN T. TAVANI (2008): «Floridi's ontological theory of informational privacy: Some implications and challenges», in *Ethics and Information Technology,* vol. 10 n. 2-3, September 2008, pp. 155-166 [doi'10.1007/ s10676-008-9154-x].

128. HOWLEY, R., ROGERSON, S., FAIRWEATHER N. B. and PRATCHETT, L. (2005): «The role of information systems staff in the provision for data protection and privacy. A subjective approach», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

129. HULL, G. (2009): «Overblocking autonomy: The case of mandatory library filtering software», in *Continental Philosophy Review,* n. 42, pp. 81-100.

130. HULL, G., LIPFORD H. R. and LATULIPE, C. (2010): «Contextual gaps. Privacy issues on Facebook», in *Ethics and Informaction Technology,* n. 4, pp. 289-302. Available at: pages.uoregon.edu/.../hull_context_privacy_fb.pdf [12/11/2013].

131. ILYES, P. y OCHS, C. (2013): «Sociotechnical Privacy. Mapping the Research landscape», in *Tecnoscienza, Italian Journal of Science & Technology Studies,* n. 4, vol. 2.

132. ISMAIL, Z., MASROM, M., RAMLAH, H., NORSHIDAH, M. (2010): «Ethical Decision Making And Privacy: Related Theories And Models», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010), 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp. 375-382.

133. JAGATIC, T. N., JOHNSON, N. A., JAKOBSSON, M. y MENCZER, F. (2007): «Social phishing», in *Communications of the ACM,* vol. 50, n. 10, pp. 94-100. Available at: http://Webpages.uncc.edu/richter/classes/2007/6010/readings/phishing-preprint.pdf [19/02/12].

134. JENSEN, C., POTTS, C. and JENSEN, C. (2005): «Privacy practices of Internet users: self-reports versus observed behavior» in *International Journal of Human-Computer Studies,* vol. 63, n. 1-2, July 2005, pp. 203-227.

135. JOHNSON, M., EGELMAN, S. and BELLOVIN, S. M. (2012): «Facebook and Privacy: It's Complicated», in *Symposium on Usable Privacy and Security (SOUPS): 2012,* July 11-13, Washington. Available at: http://dl.acm.org/citation.cfm?id=2335356 [30/05/2012].

136. JOINSON, A. N. (2008): «'Looking at,' 'Looking up,' or 'Keeping up with' People? Motives and uses of Facebook», in *CHI 2008 Proceedings: Online Social Networks,* pp. 1027-1036.

137. JONES, H. and SOLTREN, J. H. (2005): «Facebook: Threats to privacy». Available at: http://groups.csail.mit.edu/mac/classes/6.805/studentpapers/fall05-papers/facebook.pdf [03/11/2012].

138. JONES, S. and O'NEILL, E. (2010): «Feasibility of structural network clustering for group-based privacy control in social networks», in *SOUPS'10,* New York, NY: ACM Press, pp. 1-13.

139. KAIRAM, S., BRZOZOWSKI, M., HUFFAKER, D. and CHI, E. (2012): «Talking in circles: selective sharing in Google+», in *CHI'12,* New York, NY: ACM Press, pp. 1065-1074.

140. KALLIAMVAKOU, E. PRASOPOULOU, E. POULOUDI, N. (2005): «Identity management architectures: Arguing for a socio-technical perspective», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Looking back to the future.* Linköping University, Linköping (Suecia).

141. KELLEY, P., BREWER, R., MAYER, Y., CRANOR L. and SADEH N. (2011): «An investigation into Facebook friend grouping», in *Interact 2011,* Berlin / Heidelberg: Springer, pp. 216-233.

142. KLIEN, J. (2006): «Schools use Facebook for admissions, disciplinary action», in *The Stanford Daily,* 14 February. http://daily.stanford.edu/article/2006/2/14/schoolsUseFacebookForAdmissions DisciplinaryAction [27/11/2012].

143. KNORR, E. and GRUMAN, G. (2010): «What Cloud Computing Really Means», in *InfoWorld.* Available at: http://www.infoworld.com/d/cloud-computing/what-cloud-computing-really-means-031?page=0,0 [27/11/2012]

144. KOSINSKIA M., STILLWELLA, D. y GRAEPELB, T. (2013): «Private Traits and Attributes are Predictable from Digital Records of Human Behaviour», en Proceedings of the National Academy of Sciences (PNAS) University of California, Berkeley. [doi: 10. 1073/ pnas. -1218772110] [29/03/2014].

145. KOSINSKIA M., STILLWELLA, D. y GRAEPELB, T. (2013): «Private Traits and Attributes are Predictable from Digital Records of Human Behaviour», in Proceedings of the National Academy of Sciences (PNAS) University of California, Berkeley. [doi: 10. 1073/ pnas. -1218772110] [29/03/2014].

146. KOUW, M., SCHREUDERS, E. and PATER, L. (2004): «No fear or hope, but new weapons. On privacy and technology», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

147. KRAMER, A. D., GUILLORY, J. E., y HANCOCK, J. T. (2014): «Experimental evidence of massive-scale emotional contagion through social networks», in *Proceedings of the National Academy of Sciences (PNAS),* vol. 111, n. 24, pp. 8788-8790. Available at: http://www.pnas. org/content/111/24/8788.full [12/11/2014]

148. KRAMM, A. (2011): «The field site as a tool: mixed methods in social network studies», in *Graduate Journal of Social Science,* vol. 8, n. 3, pp. 127-141.

149. KRAMM, A. (2012): « The Field Site as a Tool: Insights in Privacy Protection Mechanisms of OSN Users», working paper at *4S/EASST,* Copenha-

gen, October 2012. Available at: http://www-wordpress.sit.fraunhofer.de/dipo/wp-content/uploads/sites/6/2013/03/4s_EASST.pdf [14/11/2012].

150. KRISHNAMURTHY, B. and WILLS, C. E. (2009): «Privacy Diffusion on the Web: A Longitudinal Perspective», in *Security and Privacy / Session: Web Privacy,* April 20-24, 2009. Available at: http://ramb.ethz.ch/CDstore/www2009/proc/docs/p541.pdf [27/11/2012].

151. KUMAR, R., NOVAK, J. and TOMKINS. A. (2010): «Structure and evolution of online social networks», in *Link Mining: Models, Algorithms, and Applications,* pp. 337-357.

152. KUMAR. R. (2009): «Online Social Networks: Modeling and Mining», in *Conferene on Web Search and Data Mining,* p. 60558.

153. LAMPE, C., ELLISON, N. and STEINFIELD, C. (2007): «A familiar face (book): profile elements as signals in an online social network», in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* San Jose, California: ACM Press, pp. 435-444.

154. LAMPE, C., ELLISON, N. B. and STEINFIELD, C. (2007): «A face(book): in the crowd: Social searching versus socialbrowsing», in *Proceedings of the 20th Anniversary Conference on Computer Supported Cooperative Work, CSCW'06,* Alberta: pp. 167-170.

155. LAMPE, C., ELLISON, N. B. and STEINFIELD, C. (2008): «Changes in use and perception of Facebook», in *Proceedings of the 2008 ACM conference on Computer supported cooperative work (CSCW'08),* San Diego, California: ACM Press, pp. 721-730.

156. LAMPINEN, A., LEHTINEN, V., LEHMUSKALLIO, A. and TAMMINEN, S. (2011): «We're in it Together: Interpersonal Management of Disclosure in Social Network Services», in *Proceedings of the 2011 Annual Conference on Human Factors in Computing Systems,* CHI 2011, Session: Privacy May 7-12, 2011, Vancouver, BC, Canada, New York, NY: ACM Press, pp. 3217-3226.

157. LAMPINEN, A., TAMMINEN, S. and OULASVIRTA, A. (2009): «All my people right here, right now»: management of group co-presence on a social networking site», in *GROUP'09,* New York, NY: ACM Press, pp. 281-290.

158. LANGE, P. G. (2007): «Publicly Private and Privately Public: Social Networking on Youtube», in *Journal for Computer Mediated Communication,* vol. 13, n. 1, pp. 361-380.

159. LEGARD, R., KEEGAN, J. and WARD, K. (2004): «In-depth interviews», in (eds.): Ritchie, J. and Lewis, J. *Qualitative Research Practice: A Guide for Social Science Students and Researchers,* London: Sage Publications, pp. 138-169.

160. LESKOVEC. J. (2012): *Stanford Network Analysis Project* (SNAP). Available at: http://snap.stanford.edu/ [15/11/2012].

161. LESSIG, L. (1998): «The Architecture of Privacy». Available at: http://lessig.org/content/articles/works/architecture_priv.pdf. [27/11/2012].

162. LEWIS, K., KAUFMAN, J. and CHRISTAKIS, N. (2008): «The taste for privacy: an analysis of college student privacy settings in an online social network», *Journal of Computer- Mediated Communication,* vol. 14, n. 1, pp. 79-100.

163. LIBEN-NOWELL, D. and KLEINBERG, J. (2007): «The link-prediction problem for social networks», in *Journal of the American Society for Information Science and Technology,* vol. 58, n. 7, pp. 1019-1031.

164. LIGHT, B., MCGRATH, K. and GRIFFITHS, M. (2008): «More Than Just Friends? Facebook, Disclosive Ethics and the Morality of Technology», in *Twenty Ninth International Conference on Information Systems, Paris 2008. ICIS 2008 Proceedings,* Paper 193.

165. LILLEY, S., GUMBUS A. y GRODZINSKY, F. (2010): «Social Networking and the Perception of Privacy Within The Millennial Generation Web 2.0?», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010) 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp. 375-382.

166. LILLEY, S., GUMBUS A. y GRODZINSKY, F. (2010): «What matters to non-experts about property and privacy rights?», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010) 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp. 375-382.

167. LIPFORD, H. R., DOU, W., JEONG, D., STUKES, F., RIBARSKY, W. and CHANG, R. (2009): «Recovering Reasoning Process From User Interactions», in *Computer Graphics and Applications,* vol. 29, n. 3, pp. 52-51. Available at: http://viscenter.uncc.edu/sites/viscenter.uncc.edu/files/CVC-UNCC-09-03.pdf. [09/11/2012].

168. LIPFORD, H. R., HULL, G., LATULIPE, C., BESMER, A. and WATSON, J. (2009): «Visual flows: Contextual integrity and the design of privacy mechanisms on social network sites», in *Proceedings of the Workshop on Security and Privacy in Online Social Networking, IEEE International Conference on Social Computing (SocialCom),* August 2009. Available at: http://cse.stfx.ca/~socialcom09/ [14/05/2012].

169. LIPFORD, H. R., KARR-WISNIEWSKI, and P. WILSON, D. (2011): «A new social order: mechanisms for social network site boundary regulation», in *Proceedings of the International Information Systems Conference AMCIS 2011,* 4-8 August 2011, Detroit, Michigan. Available at: http://www.proceedings.com/12585.html [14/11/2012].

170. LIPFORD, H. R., WATSON and BESMER, A. (2008): «Understanding Privacy Settings in Facebook with an Audience View», *Proc. UPSEC,* 2008.

171. LIPFORD, H. R., WISNIEWSKI, P., LAMPE, C., KISSELBURGH, L. and CAINE, K. (2012): «Reconciling Privacy with Social Media», in *Proceedings of the 2012 ACM Conference on Computer Supported Corporative Work Companion,* pp. 19-29.

172. LIVINGSTONE, S. (2008): «Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy, and self-expression», in *New Media Society,* vol. 10, pp. 393-411.

173. LOCKTON, V. and ROSENBERG, R. S. (2005): «Technologies of surveillance: Evolution and Future Impact», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Looking back to the future.* Linköping University, Linköping (Suecia).

174. LYON, D. (2006): «Surveillance, power and everyday life», in *Oxford Handbook of Information and Communication Technologies,* Oxford: Oxford University Press.

175. MADDEN, M. (2012): «Privacy management on social media sites», in *Pew Internet and American Life Project,* Washington, DC. Available at: http://pewinternet.org/Reports/2012/Privacy-management-on-social-media.aspx [27/11/2012].

176. MADDEN, M. and JONES, S. (2004): «The Internet goes to college», in *Pew Internet and American Life Project,* Washington, DC. Available at: http://www.pewinternet.org/Reports/2002/The-Internet-Goes-to-College.aspx. [14/03/2010].

177. MADDEN, M. and SMITH, A. (2010): «Reputationmanagement and social media», in *Pew Internet and American Life Project,* Washington, DC. Available at: http://pewinternet.org/Reports/2010/Reputation-Management.aspx [14/03/2011].

178. MAIA, M., ALMEIDA, J. and. ALMEIDA, V. (2008): «Identifying user behavior in online social networks», in *Proceedings of the 1st workshop on Social network systems,* New York, NY: ACM Press, pp 1-6

179. MAKEDON, F., OWEN, C. B. and KING, C. G. (2004): «Changes in The Internet Privacy Practices of The Fortune Global 500 CompaniesSudborough, C. Kapidakis, S. Gloor, Peter A. Heckman, Carey Ford, J. Pearlman, J. The ethical dilemma of data sharing under risk, en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

180. MALHOTRA, N. K., KIM, S. S. and. AGARWAL, J. (2004): «Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale and a Causal Model», in *Information Systems Research,* vol. 15, December 2004, pp. 336-355.

181. MANDRE, B. R., AHER, C. G., PATIL, D. V. and KULKARNI, A. (2004): «Privacy and Freedom of Information in Information Society», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

182. MANN, S., NOLAN, J., WELLMAN, B. (2004): «Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments», in *Surveillance and Society,* vol. 1, n. 3, pp. 331-355. Available at: http://wearcam.org/sousveillance.pdf. [07/01/2012].

183. MARKELLOS, K., MARKELLOU, P., RIGOU, MARIA SIRMAKESSIS, S., TSAKALIDIS, A. (2004): «Web Personalization and the Privacy Concern», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

184. MARX, G. T. and MUSCHERT, G. (2007): «Personal Information, Borders, and the New Surveillance Studies», in *Annual Review on Law and Social Science,* n. 3, pp. 375-395.

185. MATTHEWS, S. (2008): «Identity and Information Technology», in van den Hoven, J. and Weckert, J. (eds.): *Information technology and moral philosophy,* Cambridge: CUP, pp. 142-160.

186. MCCOWN, F. and NELSON, M. (2009): «What happens when facebook is gone?», in *Proceedings of the 9th ACM/IEEE-CS joint conference on Digital libraries,* New York, NY: ACM Press, pp. 251-254.

187. MCKEON, M. (2010): «The Evolution of Privacy on Facebook», in *Matt-McKeon.com,* May 19, 2010. Available at: http://www.mattmckeon.com/facebook-privacy/ [4/10/11].

188. MCROBB, S. and ROGERSON, S. (2005): «Privacy Policies Online: further results from a continuing investigation», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Looking back to the future*. Linköping University, Linköping (Suecia).

189. MCROBB, S., ORITO, Y., MURATA, K. and ADAMS, A. (2007): «Towards an exploration of cross-cultural factors in privacy online», en *Glocalisation: bridging the global nature of information and communication technology and the local nature of human beings* Ward Bynum, T., Rogerson, S. (eds.): *Living, working and learning beyond technology* (ETHICOMP 2007) International conference on the Social and Ethical Impacts of Information and Communication Technology, 24-26 September 2008, en Meiji University, Tokyo (Japón).

190. MCROBB, STEVE ROGERSON, Simon: Privacy Policies Online: some reflections and conclusions from a continuing investigation, en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

191. MILLER, K. W. and VOAS J. (2010): «Ethics and the Cloud», in *IT Professional*, vol. 12 n. 5, September 2010, pp. 4-5 [doi'10.1109/MITP.2010.129]

192. MISLOVE, A., MARCON, M., GUMMADI, K., DRUSCHEL, P. and BHATTACHARJEE, B.: Measurement and analysis of online social networks. In Proceedings of the 7th ACM SIGCOMM conference on Internet measurement, pp 29-42. ACM, 2007.

193. MORAIS DA COSTA, G. J. (2005): «Internet: middle of communication ethically incompatible? Or not?», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Looking back to the future*. Linköping University, Linköping (Suecia).

194. MOSTASHARI, A. and SUSSMAN, J. M. (2009): «A Framework for Analysis, Design and Management of Complex Large-Scale Interconnected Open Sociotechnological Systems», in *International Journal of Decision Support System Technology (IJDSST),* vol. 1, n. 2, pp. 53-68.

195. MYSKJA, B. K. (2008): «The categorical imperative and the ethics of trust»*, in Ethics and Information Tech*nology, vol. 10, pp. 213-220.

196. NAAMAN, M., BOASE, J. and LAI, C. (2010): «Is it really about me?: message content in social awareness streams», in *CSCW'10,* New York, NY: ACM Press, pp. 189-192.

197. NELSON, III W. and. NELSON A. (2004): «The Drift of the United States Toward a Surveillance Society in Today's Networked Economy», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

198. NIPPERT-ENG, C. (2007): «Privacy in the United States: Some Implications for Design Privacy in the United States», in *International Journal of Design,* vol. 1, n. 2, pp. 1-10.

199. NISSENBAUM, H. (2004): «Privacy as contextual integrity», in *Washington Law Review,* vol. 79, n. 1, pp. 119-158.

200. NISSENBAUM, H. (2011): «A Contextual Approach to Privacy Online», in *Daedalus,* vol. 140, n. 4, pp. 32-48.

201. NISSSEMBAUM, H. and BAROCAS, S. (2009): «On Notice: The Trouble with Notice and Consent», in *Media, Culture, and Communication,* New York: New York University. Available at: http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf [12/12/2009]

202. NORBERG, P. A., HORNE, D. R. & HORNE, D. A. (2007): «The privacy paradox: personal information disclosure intentions versus behaviors», in *Journal of Consumer Affairs,* vol. 41, n. 1, pp. 100-126.

203. OCHS, C. (2013): «Wettrüsten der Skripte: Widersprüchlichkeiten soziotechnischer Privatheitspraktiken im Internet», in U. Ackermann (ed.): *Im Sog des Internets. Öffentlichkeit und Privatheit im digitalen Zeitalter,* Frankfurt/M.: Humanities Online, pp. 111-129.

204. OCHS, C. and LÖW, M. (2012): «Un/faire Informationspraktiken: Internet Privacy aus sozialwissenschaftlicher Perspektive», in J. Buchmann (ed.): *Internet Privacy. Eine multidisziplinäre Bestandsaufnahme / A multidisciplinary analysis (acatech STUDIE),* Berlin: Springer, pp. 15-61.

205. Office of the Privacy Commissioner of Canada (2009): *Facebook agrees to address Privacy Commissioner's concerns,* August 27, 2009. Available at http://www.priv.gc.ca/media/nr-c/2009/nr-c_090827_ e.cfm [14/12/2011].

206. OGURA, T. (2006): «Electronic government and surveillance-oriented society», in Lyon, D. (ed.): *Theorizing Surveillance. The Panopticon and Behind,* Portland: Willan, pp. 270-95.

207. OLSON, J. S., GRUDIN, J. and HORVITZ E. (2005): «A study of preferences for sharing and privacy», in *CHI EA'05,* New York, NY: ACM Press, pp. 1985-1988.

208. ORITO, Y. and MURATA, K. (2005): «Privacy Protection in Japan: Cultural Influence on the Universal Value», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Looking back to the future.* Linköping University, Linköping (Suecia).

209. ORITO, Y., MURATA, K., FUKUTA, Y., MCROBB, S. and ADAMS, A. (2008): «Online Privacy and Culture: Evidence from Japan», en Ward Bynum, T., Rogerson, S. (eds.): *Living, working and learning beyond technology* (ETHICOMP 2008), International conference on the Social and Ethical Impacts of Information and Communication Technology, 24-26 September 2008, en Mantua Italia: University of Pavia.

210. OUDSHOORN, N. and PINCH, T. (2008): «User-Technology Relationships: Some Recent Developments», in E. J. Hackett, O. Amsterdamska, M. Lynch and J. Wajcman (eds.): *The Handbook of Science and Technology Studies,* Cambridge, MA: MIT Press, pp. 541-565.

211. PAINE, C., REIPS, U., STIEGER, S., JOINSON, A. and BUCHANAN, T. (2007): «Internet users' perceptions of 'privacy concerns' and 'privacy actions'», in *International Journal of Human-Computer Studies,* vol. 65, n. 6, June 2007, pp. 526-536.

212. PALM, E. (2004): «An Ethical Questioning of Work Place Surveillance - strengthening employees' negotiating power», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

213. PALM, E. (2008): «Information Security-Security for whom and why?», en Ward Bynum, T., Rogerson, S. (eds.): *Living, working and learning beyond technology* (ETHICOMP 2008) International conference on the Social and Ethical Impacts of Information and Communication Technology, 24-26 September 2008, en Mantua Italia: University of Pavia.

214. PALM, E. (2010): «Privacy Online-The Case Of E-Government In Sweden», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th

International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010), 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgili, pp. 375-382.

215. PAPACHARISSI, Z. (2009): «The virtual geographies of social networks: A comparative analysis of Facebook, LinkedIn and ASmallWorld», in *New Media Society,* n. 11, pp. 199-220.

216. PARRISH, J. L. (2010): «PAPA Knows Best: Ethical Guidelines for Social Networking Sites», in *Journal of Ethics in Information Technology,* vol. 12, n. 2, pp. 187-193.

217. PATRIGNANI, N. (2008) «A Conceptual Framework for Computer Ethics», en Systems», en Ward Bynum, T., Rogerson, S. (eds.): *Living, working and learning beyond technology* (ETHICOMP 2008), International conference on the Social and Ethical Impacts of Information and Communication Technology, 24-26 September 2008, en Mantua Italia: University of Pavia.

218. PERER, A. and SHNEIDERMAN. B. (2006): «Balancing systematic and exible exploration of social networks, IEEE Transactions on Visualization and Computer Graphics performance», in *Journal of Information Management,* vol. 38, n. 2, pp 693-700.

219. PICCOLI, G. and IVES, B. (2003): «Trust And The Unintended Effects Of Behavior Control In Virtual Teams», in *MIS Quarterly,* vol. 27, n. 3, pp. 365-395.

220. PIETERS, W., VAN CLEEFF, A. (2009): «The Precautionary Principle in a World of Digital Dependencies», in *Computer,* vol. 42, n. 6, pp. 50-56. [doi'10.1109/MC.2009.203].

221. POLLER, A., KRAMM, A. and ILYES, P. (2011): «Data security and privacy in Social Networks. Cognitive conceps and problem awareness of young users.» Position paper, 2011.

222. POLLER, A., KRAMM, A. and ILYES, P. (2013): «Designing privacy-aware online social networks-A reflective socio-technical approach», in *CSCW'13 Measuring Networked Social Privacy Workshop,* February 23-27, 2013, San Antonio, Texas, United States. Available at: http://testlab.sit.fraunhofer.de/downloads/Publications/poller_osn_design_cscw13_workshop_camera_ready_rot.pdf [20/01/2014].

223. POLLER, A., KRAMM, A., ILYES, P. and KOCKSCH, L.(2014): «Investigating OSN Users' Privacy Strategies With In-Situ Observation», in *CSCW'14* Companion, Baltimore. Available at: http://testlab.sit.fraunhofer.de/downloads/Publications/poller_CSCW2014_Investigating_OSN_users_privacy_strategies.pdf. [15/01/2014].

224. POLLER, A., KRAMM, A., ILYES, P. and KOCKSCH, L. (2014): «Investigating OSN Users' Privacy Strategies with ROSE-A Research Tool for Online Social Environments», in *CSCW'14* Poster, Baltimore, 2014. Available at:

https://dipo.sit.fraunhofer.de/wp-content/uploads/sites/6/2014/02/cscw14-poster-final-rot.pdf [15/01/2014].

225. PRIOR, M. (2004): «Surveillance-capable technologies in the workplace: some evidence of the views of the next generation of computer professionals», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

226. Privacy Rights Clearing House (2008): *The Privacy Implications of Cloud Computing*. Available at http://www.privacy rights.org/ar/cloud-computing.htm. [15/03/2011].

227. RAYNES-GOLDIE, K. (2010): «Aliases, creeping, and wall cleaning: understanding privacy in the age of Facebook», in *First Monday,* vol. 15, n. 1, Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/ view/2775/2432. [27/11/2012].

228. RAYNES-GOLDIE, K. (2012): *Privacy in the Age of Facebook: Discourse, Architecture, Consequences,* PhD Thesis, Curtain University, Perth, Australia. Available at: http://www.k4t3.org/wpcontent/uploads/2012/09/privacy_in_the_age_of_facebook_raynes-goldie.pdf, retrieved [27/02/2012].

229. REYNOLDS, B., VENKATANATHAN, J., GONCALVES J. and KOSTAKOS V. (2011): «Sharing ephemeral information in online social networks: privacy perceptions and behaviours», in *Proceedings of the 13th IFIP TC13 Conference on Human-Computer Interaction-Interact 2011,* June 16, 2011, Lisbon, Portugal: Springer, pp 204-215.

230. RITCHIE, J., SPENCER, L. and O'CONNOR, W. (2004): «Carrying out qualitative analysis», in J. Ritchie and J. Lewis (eds.): *Qualitative Research Practice: A Guide for Social Science Students and Researchers,* Thousand Oaks, CA: Sage Publications, pp. 219-262.

231. ROBARDS, B. (2010): «Randoms in my bedroom: negotiating privacy and unsolicited contact on social network sites», in *PRism Online PR Journal,* vol. 7, n. 3, pp. 1-12. Available at: http://www.doaj.org/doaj?func=abstractandid=614104 [09/02/2013].

232. ROBISON, W. L. (2010): «Bioinformatics And Privacy», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010), 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp. 375-382.

233. ROGERSON, S., FAIRWEATHER, B. and PRIOR, M. (2008) «Exploring Motivations for Surprising views about Ethical Issues in Information Systems» (eds.): *Living, working and learning beyond technology* (ETHICOMP 2008) International conference on the Social and Ethical Impacts

of Information and Communication Technology, 24- 26 September 2008, en Mantua, Italia: University of Pavia.

234. ROTMAN, D., PREECE, J., HE, Y. and DRUIN, A. (2012): «Extreme Ethnography: Challenges for Research in Large Scale Online Environments», in *Proceedings of the 2012 iConference,* New York: ACM Press, pp. 207-214.

235. SANDOVAL, M. (2011): «A critical empirical case study of consumer surveillance on Web 2.0», in Fuchs, C., Boersma, K., Albrechtslund, A. and Sandoval, M. (eds.): *Internet and Surveillance: The Challenge of Web 2.0 and Social Media,* New York: Routledge.

236. SCHNEIDER, F., FELDMANN, A., KRISHNAMURTHY, B. and WILLINGER, W. (2009): «Understanding online social network usage from a network perspective», in *Proceedings of the 9th SIGCOMM Internet measurement conference,* New York: ACM Press, pp. 35-48.

237. SCHNEIER, B. (2006): «Facebook and Data Control», in *Schneier on Security.* Available at: http://www.schneier.com/blog/archives/2006/09/facebook_and_da.html [27/05/2012].

238. SCHNEIER, B. (2010): «A Taxonomy of Social Networking Data», in *IEEE Computer Society Security and Privacy,* July/August 2010, vol. 8, p. 88-100.

239. SIMPKINS, P. (2004): «I have the power!», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

240. SIMPKINS, P. and HASAN, I. (2008): «The Right to Know vs. The Right to Privacy», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes* of *ICT,* 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010) 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily.

241. SKINNER, G. HAN, S. and CHANG, E. (2006): «An Introduction to a Taxonomy of Information Privacy in Collaborative Environments», in *Proceedings of the 5th WSEAS International Conference on Applied Computer Science,* Hangzhou, China, pp. 981- 986.

242. SLEEPER, M., BALEBAKO, R., DAS, S., MCCONAHY, A. L., WIESE, J. and CRANOR, L. F. (2013): «The Post that Wasn't: Exploring Self-Censorship on Facebook», in CSCW13, February 23-27, San Antonio, Texas, United States.

243. SOLOVE, D. J. (2006): «A Taxonomy of Privacy», in *University of Pennsylvania Law Review,* n. 154, pp. 477-560.

244. SOLOVE, D. J. (2007): «I've Got Nothing to Hide' and other misunderstandings of privacy», in *San Diego Law Review,* n. 44, pp. 745-772.

245. SOLOVE, D. J. (2007): *The future of reputation: Gossip, rumor and privacy on the internet*. New Haven, United States: Yale UP.

246. SOPHOS (2007): «Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieve», August 14, 2007. Available at: https://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx [12/11/2009].

247. STAAB, S., DOMINGOS, P., MIKE, P., GOLBECK, J., DING, L., FININ, T., JOSHI, A., NOWAK, A. and VALLACHER R. (2005): «Social networks applied», in *IEEE Intelligent systems,* vol. 20, n. 1, pp. 80-93.

248. STAHL, B. C. (2007): «What Privacy? The Impact of the UK Human Rights Act 1998 on Privacy Protection in the Workplace», en *Glocalisation: bridging the global nature of information and communication technology and the local nature of human beings Ward Bynum,* T., Rogerson, S.(eds.): *Living, working and learning beyond technology* (ETHICOMP 2007), International conference on the Social and Ethical Impacts of Information and Communication Technology, 7 2007, en Meiji University, Tokyo (Japón).

249. STALDER, F. (2004): «Privacy is not the Antidote to Surveillance», in *Surveillance and Society,* vol. 1, n. 1, pp. 120-124.

250. STRATER, K. and LIPFORD, H. R. (2008): «Strategies and struggles with privacy in an online social networking community», in *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction,* John Moores University, Liverpool, United Kingdom: ACM Press, pp. 111-119.

251. STRATER, K. and LIPFORD, H. R. (2008): «Strategies and struggles with privacy in an online social networking community», in *Proceedings of the 22nd British HCI Group 2008,* Liverpool, United Kingdom: ACM Press, pp. 111-119.

252. STUTZMAN, F. (2006): «An evaluation of identity-sharing behavior in social network communities», in *Journal of the International Digital Media and Arts Association,* vol. 3, n. 1, pp. 10-18.

253. STUTZMAN, F. (2006): «Student Life on the Facebook», Available at http://ibiblio.org/fred/facebook/stutzman_fbook.pdf [02/03/2010].

254. STUTZMAN, F. (2011): «Networked information behavior in life transition», Available at: http://media.proquest.com/media/pq/classic/doc/2374161701/fmt/ai/rep/NPDF?_s=yGsXK32hWfSQVGkfoQHfyyp0keE%3D [27/07/2012].

255. STUTZMAN, F. and KRAMER-DUFFIELD, J. (2010): «Friends Only: Examining a Privacy-Enhancing Behavior in Facebook», in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI 2010: Privacy,* Austin, Texas: ACM Press, pp. 1553-1562. Available at: ACM Digital Library [27/11/2012].

256. STUTZMAN, F. and HARTZOG, W. (2013): «Obscurity by Design», in *Washington Law Review,* n. 88, pp. 385-50.

257. STUTZMAN, F. and HARTZOG, W. (2013): «The case for online obscurity», in *California Law Review,* vol. 101, n. 1, pp. 1-20.

258. STUTZMAN, F., CAPRA, R. and THOMPSON, J. (2011): «Factors mediating disclosure in social network sites», in *Computers in Human Behavior,* vol. 27, n. 1, pp. 590-598.

259. STUTZMAN, F., GROSS, R. and ACQUISTI, A. (2012): «Silent Listeners: The Evolution of Privacy and Disclosure on Facebook», in *Journal of Privacy and Confidentiality,* vol. 4, n. 2, pp. 7-41.

260. STUTZMAN, F., HARTZOG, W. (2012): «Boundary regulation in social media», in *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work,* ACM Press, pp. 769-778.

261. STUTZMAN, F., VITAK, J., ELLISON, N. B., GRAY, R. and LAMPE, C. (2012): «Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook», in *Proceedings of the 6th annual International Conference on Weblogs and Social Media (ICWSM),* Washington, DC: Association for the Advancement of Artificial Intelligence.

262. SUNSTEIN, C. R. and ULLMANN-MARGALIT, E. (1999): «Second-order decisions», in *Ethics,* n. 110, pp. 5-31.

263. TAVANI, H. (2011): *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing,* Hoboken, New Jersey: John Wiley and Sons, pp. 131-164.

264. TAVANI, H. T. (2007): «Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy», in *Metaphilosophy,* vol. 38, n. 1, pp. 1-2.

265. TAVANI, H. T. (2008): «Information Privacy: Concepts, Theories and Controversies», in Himma, K. E. and Tavani, H. T. (eds.): *The Handbook of Information and Computer Ethics,* Hoboken, New Jersey: John Wiley and Sons, pp. 131-164.

266. TAVANI, H. T. and GRODZINSKY, F. S. (2005): «P2P Networks and the Verizon v. RIAA Case: Implications for Personal Privacy and Intellectual Property», in *Ethics and Information Technology,* vol. 7, n. 4, pp. 243-250 [doi'10.1007/s10676-006-0012-4].

267. TAVANI, H. T. and Grodzinsky, F. S. (2008): «Online file sharing: resolving the tensions between privacy and property interests», in *ACM SIGCAS Computers and Society,* vol. 38, n. 4, pp. 28-39 [doi'10.1145/1497054.1497056]

268. The International Working Group on Data Protection in Telecommunications: (2008): *Report and Guidance on Privacy in Social Network Services. «Rome Memorandum»,* March 4, 2008, Rome, Italy. Available at:

http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf [17/05/2010].

269. TREPTE, S. and REINECKE, L. (2013): «The Reciprocal Effects of Social Network Site Use and the Disposition for Self-Disclosure: A Longitudinal Study», in *Computers in Human Behavior,* vol. 29, n. 3, pp. 1102-1112.

270. TSAI, J., EGELMANN, S., CRANOR, L. F. and ACQUISTI, A. (2011): «The Effect of Online Privacy Information on Purchasing Behaviour: An Experimental Study», in *Journal of Information Systems Research,* vol. 22, n. 2, pp. 254-268.

271. TUFECKI, Z. (2008): «Can you see me now? Audience and disclosure regulation in online social network sites», in *Bulletin of Science, Technology and Society,* vol. 28, n. 20, pp. 20-36.

272. TUROW, J. (2006): «Cracking the consumer code: advertising, anxiety and surveillance in the digital age», in Hagerty, K. and Ericson, R. (eds.): *The New Politics of Surveillance and Visibility,* Toronto: University of Toronto Press.

273. VAN DEN HOVEN, J. (2007): «ICT and Value Sensitive Design», in P. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa and V. Laurent (eds.): *The Information Society: Innovation, Legitimacy, Ethics and Democracy,* Boston: Springer, pp. 67-72.

274. VAN DEN HOVEN, J. (2008): «Information Technology, Privacy and the Protection of Personal Data», in. van den Hoven, J and Weckert, J (eds.): *Information Technology and Moral Philosophy,* Cambridge: Cambridge University Press, pp. 8-25

275. VAN DER VELDEN, M. and EL EMAM, K. (2012): «'Not All my Friends Need to Know': A Qualitative Study of Teenage Patients, Privacy, and Social Media», in *Journal of the American Medical Information Association,* n. 20, pp. 16-24.

276. VISEU, A., CLEMENT, A. and ASPINALL, J. (2004): «Situating Privacy Online», in *Information, Communication and Society,* vol. 7, n. 1, pp. 92-114.

277. WANG, Y., NORCIE, G. and CRANOR, L. F. (2011): «Who is Concerned about What? A Study of American, Chinese and Indian Users' Privacy Concerns on social Network Sites», in *Proceedings of the 4th International Conference on Trust and Trustworthy Computing,* June 22-24, Pittsburgh, PA, pp. 146-153. Available at: www.trust2011.org/ [24/10/2011].

278. WANG, Y., LEON, P. G., SCOTT, K., CHEN, X., ACQUISTI, A. and CRANOR, L. F. (2013): «Privacy Nudges for Social Media: An Exploratory Facebook Study», in *Proceedings of the 22nd international conference on World Wide Web companion,* Republic and Canton of Geneva, Switzerland, pp. 763-770. Available at: flosshub.org/.../biblio_field%3A103.6%3A%22Proc... [24/01/2012].

279. WANG, Y., NORCIE, G., KOMANDURI, S., ACQUISTI, A., LEON, P. G. and CRANOR, L. F. (2011): «'I regretted the minute I pressed share': A

qualitative study of regrets on facebook», in *Proceedings of the Seventh Symposium on Usable Privacy and Security, SOUPS'11,* New York, United States, vol. 10, n. 1, pp. 10-16.

280. WARD, C. (2004): «Privacy and human rights - 1984 revisited or simply the pursuit of a safer society?», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

281. WASSERMAN, T. (2012): «Pinterest is now the n. 3 social network in the U. S», *Mashable.com*, 6 April [Online] Available at: http://mashable.com/2012/04/06/ pinterest-number-3-social-network/ [5/03/12].

282. WESTER, M. and SANDIN, P. (2010): «Privacy and the public: perception and acceptance of various applications of ICT», in Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT, 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010),* 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp. 597, pp 580-586.

283. WESTIN, A. (2003): «Social and political dimensions of privacy», in *Journal of Social Issues,* vol. 59, n. 2, pp. 431-453.

284. WIESE, J., Kelley, P. G., Cranor, L. F., Dabbish, L., Hong J. I. and Zimmerman, J. (2011): «Are you close with me? Are you nearby?: investigating social groups, closeness, and willingness to share», in *UbiComp'11,* New York, United States: ACM Press, pp. 197-206.

285. WILFORD, S. (2004): «E-Government, Participation or Panopticon?», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *Challenges for the citizen of the information society,* University of the Aegean, Syros (Grecia).

286. WILSON, C., BOE, B., SALA, A., PUTTASWAMY, K. and ZHAO. B. (2009): «User interactions in social networks and their implications», in *Proceedings of the 4th ACM European conference on Computer systems,* New York, United States: ACM Press, pp. 205-218.

287. WISNIEWSKI, P. (2011): «Interpersonal Boundary Regulation within Online Social Networks», available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=059287 48 [27/11/2012].

288. WISNIEWSKI, P., LIPFORD, H. and WILSON. D. (2012): «Fighting for my space: coping mechanisms for SNS boundary regulation», in *CHI'12,* New York, United States: ACM Press, pp. 609-618.

289. YANG, S. and WANG, K. (2009): «The influence of information sensitivity compensation on privacy concern and behavioural intention», in *SIGMIS Database,* vol. 40, n. 1, pp. 38-51.

290. YOUYOU, W., KOSINSKI, M. y STILLWELL, D. (2015): «Computer-based personality judgments are more accurate than those made by humans», in Proceedings of the National Academy of Sciences (PNAS) University of

California, Berkeley, 12 January 2015 [doi:10.1073/pnas.1418680112]. [09/05/2015].

291. YOUNG, A. L. and QUAN-HAASE, A. (2009): «Information revelation and Internet privacy concerns on social network sites: a case study of Facebook», in *Proceedings of the 4th International Conference on Communities and Technologies,* June 25-27, Pennsylvania, PA: University Park, pp. 265-274. Available at: dl.acm.org/citation.cfm?id=1556460. [13/06/2009].

292. YOUNG, A. L. and QUAN-HAASE, A. (2010): «Uses and gratifications of social media: a comparison of Facebook and instant messaging», in *Bulletin of Science, Technology, and Society,* vol. 30, n. 5, pp. 350-361.

293. YOUNG, A. L., GURZICK, D. and QUAN-HAASE, A. (2011): «Online multi-contextual analysis: (re)connecting the social network site user with their profile», in B. K. Daniel (ed.): *Handbook of Research on Methods and Techniques for Studying Virtual Communities: Paradigms and Phenomena,* Hershey, PA: IGI Global, pp. 542-554.

294. YOUNG, A. L. and QUAN-HASSE, A. (2013): «Privacy protection strategies on Facebook» in *Information, Communication and Society,* vol. 16, n. 4, pp. 479-500. [doi: http://dx.doi.org/10.1080/1369118X.2013.777757].

295. ZENG, K. and CAVOUKIAN A. (2010): «Modeling Cloud Computing Architecture without Compromising Privacy: A Privacy by Design Approach». Available at: www.privacybydesign.ca [27/11/2012].

296. ZICKUHR, K. (2010): «Generation 2010», *Pew Internet and American Life Project,* Washington, DC. Available at: http://www.pewinternet.org/Reports/2010/Generations-2010.aspx [14/03/2012].

297. ZIMMER, M. (2005): «Surveillance, privacy and the ethics of vehicle safety communication technologies», in *Ethics and Information Technology,* vol. 7, n. 4, pp. 201-221.

298. ZIMMER, M. (2007): «Privacy and surveillance in Web 2.0: A study in contextual integrity and the emergence of Netaveillance», in *Society for Social studies of Science.* Available at: http://www.academia.edu/3943172/Privacy_and_Surveillance_in_Web_2.0_A_study_in_Contextual_Integrity_and_the Emergence_of_Netaveillance [27/12/2009].

299. ZIMMER, M. (2008): «Privacy on planet Google: using the theory of contextual integrity to clarify the privacy threats of Google's quest for the perfect search engine», in *Journal of Business and Technology,* vol. 3, pp. 109-132.

300. ZIMMER, M. (2010): «Social networking and the perception of privacy within the millennial generation Web 2.0», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th International conference on the Social and Ethical Impacts of Information and Communication Technology

(ETHICOMP2010), 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily, pp. 597, pp. 273-279.

301. ZURAINI, I., MASLIN, M., RAHIM, F. A. (2010): «Harnessing Computer Ethics In Establishing Information Security», en Arias-Olivia, M., Ward Bynum, T., Rogerson, S., Torres-Coronas, T. (eds.): *The «backwards, forwards and sideways» changes of ICT,* 11th International conference on the Social and Ethical Impacts of Information and Communication Technology (ETHICOMP2010), 14-16 April, 2010, Tarragona, Spain: Universitat Rovira i Virgily.

ANEXO 2

2. Artículos no encontrados:

1. Andrejevic, M. (2007): *Ispy: Surveillance and Power in the Interactive Era,* Lawrence, United States: University Press of Kansas.
2. Boyd, D. (2011): «Living in a Publicity World: Privatsphäre und Öffentlichkeit in sozialen Netzwerken», in Heinrich-Böll Stiftung (ed.): *#public life. Digitale Intimität, die Privatsphäre und das Netz,* Berlin: agit-druck, pp. 28-35.
3. Ferrara, E. Fiumara, G. and Baumgartner. R. (2010): «Web Data Extraction, Applications and Techniques: A Survey». Technical Report.
4. Fuster, G. (2009): «Inaccuracy as a privacy-enhancing tool», in *Ethics and Information Technology.*
5. Leskovec J. (2008): *Dynamics of large networks.* PhD thesis, Carnegie Mellon University,
6. Rachna Dhamija and Lisa Dusseault (2008): «The seven flaws of identity management: Usability and security challenges», in *IEEE Security and Privacy Special Issue on Identity Management.*
7. Stutzman, F. (2006): «Adopting the Facebook: A comparative analysis».
8. Watson, Whitney and Lipford (2009): «Configuring Audience Oriented Privacy Policies», in Proc. SafeConfig, University of North Carolina at Charlotte.

ANEXO 3

3. Artículos descartados por inapropiados:

En el siguiente apartado indicamos los estudios recopilados siguiendo los criterios de búsqueda (descriptores) especificados en el capítulo *Introducción a la Investigación,* pero que finalmente fueron descartados del análisis.

1. ADAMIC, L. A., BÜYÜKKÖKTEN, O. and ADAR, E. (2003): «A social network caught in the Web», in *First Monday,* vol. 8, n. 6.
2. ADAMS, A. (2000): «Multimedia information changes the whole privacy ballgame», in *Proceedings of the Tenth Conference on Computers, Freedom and Privacy: Challenging the Assumptions CFP '00,* April 04 - 07, 2000, Toronto, Ontario, Canada: ACM Press, pp. 25-32.
3. ADKINSON, W. F. Jr., EISENACH, J. A. and LENARD T. M. (2002): «Privacy online: A report on the information practices and policies of commercial Websites». Available at: http://pff.org/publications/privacyonlinefinalael.pdf accessed 01.09.2003.
4. AGRE, P. (1997): «Introduction», in Agre, P. and Rotenberg, M. (eds.): *Technology and Privacy: The New Landscape,* Cambridge, MA: MIT Press, pp. 1-28.
5. AIELLO, J. R. and KOLB, K. J. (1995): «Electronic performance monitoring and social context: impact on productivity and stress», in *Journal or Applied Psychology,* vol. 80, n. 3, pp. 339-353.
6. ANDERSON, B. (1996): «Work, Ethnography and System Design», in *Rank Xerox Research*. Centre Technical Report EPC 1996, Rank Xerox Research Centre, Cambridge.
7. BAILEY, J. (2000): «Some Meaning of 'the Private' in Sociological Thought», in *Sociology,* vol. 34, n. 3, pp. 381-401.
8. BARGH, J. A., MCKENNA, K. Y. and FITZSIMONS, G. M. (2002): «Can you see the real me? Activation and expression of the "true self" on the Internet», in *Journal of Social Issues,* vol. 58, n. 1, pp. 33-48.
9. BENKLER, Y. (2003): «Through the looking glass: Alice and the constitutional foundations of the public domain», in *Law and Contemporary Problems,* n. 66, pp. 173-224.
10. BERGER, T., CHAPIN, J., GERHARDT, G., MCFARLAND, D., PRINCIPE, J., SOUSSOU, W., TAYLOR, D. and TRESCO, P. (2007): International Assessment of Research and Development in Brain-Computer Interfaces.
11. BOYD, D. (2003): «Reflections on friendster, trust and intimacy», in *Intimate (Ubiquitous) Computing Workshop - Ubicomp 2003,* October 12-15, Seattle, Washington, USA.
12. BREY, P. (1999): «Worker autonomy and the drama of digital networks in organizations». *Journal of Business Ethics,* vol. 22, n. 1, pp. 15-25.

13. BREY, P. (1999): «Worker autonomy and the drama of digital networks in organizations», in *Journal of Business Ethics,* vol. 22 n. 1, pp. 15-25.

14. BREY, P. (2000): «Disclosive computer ethics» in *Computers and Society,* vol. 30 n. 4, December 2000, pp. 10-16 [doi'10.1145/572260.572264]

15. BURKERT, H. (1997): «Privacy-Enhancing Technologies: typology, critique, vision», in *Technology and privacy: the new landscape.*

16. CAIN, R. M. (2002); «Global Privacy Concerns and Regulation - Is the United States a World Apart?» *International Review of Law Computers & Technology,* vol. 26, n. 1 pp. 32-47.

17. CAMPBELL, A. J. (1997): «Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy». *Journal of Direct Marketing,* vol. 11, n. 3, pp. 44-56.

18. CARSTEN STAHL, B. and COLLINS D. (2002): «The Importance of Codes of Conduct for Irish IS/IT Professionals' Practice of Employee Surveillance», *ETHICOMP 2002,* Lisbon, Portugal, 13-15 November 2002.

19. CHAN, S. and CAMP, L. (2001): «Towards Coherent Regulation of Law Enforcement Surveillance in the Network Society», in *The Social Impacts of Information and Communication Technologies, ETHICOMP 2001,* Gdansk, 18-20 June 2001.

20. CLARKE, R. (1999): «Internet privacy concerns confirm the case for intervention», in *Communications of the ACM,* vol. 42, n. 2, pp. 60-7.

21. COLEMAN, R. and SIM, J. (2000): «You'll Never Walk Alone: CCTV Surveillance, Order and Neo-Liberal Rule in Liverpool City Centre», in *British Journal of Sociology,* vol. 51, n. 4, pp. 623-639.

22. COLIN, J. B., REGAN, P. and RAAB, C. D. (2002): «Onboard Telematics And The Surveillance Of Movement: The Case Of Car Rental Systems», in *ETHICOMP 2002,* Lisbon, Portugal, 13-15 November 2002.

23. COLLSTE, G. and HOLMQVIST, J. (2001): «ICT and Democratic Values», in *The Social Impacts of Information and Communication Technologies, ETHICOMP 2001,* Gdansk, 18-20 June 2001.

24. DAVIES, S. G. (1998): «CCTV: A New Battleground for Privacy», in Norris, C. *et al.* (eds.): *Surveillance, Closed Circuit Television and Social Control Ashgate.* Aldershot, pp. 243-254.

25. DECEW, J. (1986): «The scope of privacy in law and ethics», in *Law and Philosophy,* vol. 5, n. 2, pp. 145-73.

26. DRESNER, M. (2002): «Privacy vs Public Safety». Privacy Law & Business: Data Protection & Privacy Information Worldwide, pp. 15-32.

27. DUBBELD, L. (2002): «Surveilling organisations, organising surveillance. Organisations, observers and the observed», in *ETHICOMP 2002,* Lisbon, Portugal, 13-15 November 2002.

28. ELGESEM, D. (2005): «Data protection and limits of centralised risk assessment».

29. FAIRWEATHER, N. B. (2001): «Privacy in the Age of Bigger Brother», in *The Social Impacts of Information and Communication Technologies, ETHICOMP 2001,* Gdansk, 18-20 June 2001.

30. FEKETE, L. (2001): «How to be a European non-European (The Problems of the Identity and Identification in Cyber-space)», in *The Social Impacts of Information and Communication Technologies, ETHICOMP 2001,* Gdansk, 18-20 June 2001.

31. FROOMKIN, M. (2000): «The death of privacy?», in *Stanford Law Review,* vol. 52, n. 5, pp. 1461-1543.

32. FURNELL, S. M. and KARWENI, T. (1999): «Security Implications of Electronic Commerce: a Survey of Consumers and Businesses». *Internet Research,* vol. 9, n. 5, pp. 372-382.

33. GREEN, S. (1999): «A plague on the Panopticon: surveillance and power in the global information economy». *Information, Communication and Society,* vol. 2, n. 1, pp. 26-44.

34. HAGGERTY, K. D. and ERICSON, R. V. (2000): «The Surveillant Assemblage», in *British Journal of Sociology,* vol. 51, n. 4, pp. 605-622.

35. HARTMAN, L. P. (2001): «Technology and ethics: privacy in the workplace». *Business and Society Review,* vol. 106 n. 1, pp. 1-27.

36. HINE, C. and JULIET, E. (1998): «Privacy in the Marketplace». *The Information Society,* vol. 14, n. 4, pp. 253-262.

37. HORRIGAN, J. B. (2002): «Online communities: Networks that nurture long-distance relationships and local ties», in *Pew Internet and American Life Project.*

38. HOWLEY, R., ROGERSON, S., FAIRWEATHER, B. and PRATCHETT, L. (2002): «The role of information systems personnel in the provision for privacy and data protection in organisations and within information systems», *ETHICOMP 2002,* Lisbon, Portugal, 13-15 November 2002.

39. HUGHES, J. (1995): «The Role of Ethnography in Interactive Systems Design», in *Interactions,* vol. 2, n. 2, pp. 57-65.

40. INTRONA, L. (1997): «Privacy and the computer: why we need privacy in the information society», in *Metaphilosophy,* vol. 28, n. 3, pp. 259-75.

41. INTRONA, L. and NISSENBAUM, H. (2000): «The Public Good Vision of the Internet and the Politics of Search Engines», in Rogers, R. (ed.): *Preferred Placement. Knowledge Politics on the Web,* Maastricht: Jan van Eyck Akademie Editions.

42. INTRONA, L. D. (1999): «Privacy, Autonomy and Workplace Surveillance», *Proceedings of the 4th ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communication Technologies,* Rome, 5-8 October 1999.

43. INTRONA, L. D. and NISSENBAUM, H. (2000): «Shaping the Web: Why the politics of search engines matters», in *The Information Society,* vol. 16, n. 3, pp. 169-185.

44. ITAI, K (2001): «Medical Informatics and Information Ethics- Privacy Policy in the Age of Taylor-Made Medicine», in *The Social Impacts of Information and Communication Technologies, ETHICOMP 2001,* Gdansk, 18-20 June 2001.

45. JARVENPAA, S. and LEIDNER, D. (1998): «Communication and Trust in Global Virtual Teams», in *JCMC,* vol. 3, n. 4.

46. JIMROGLOU, K. M. (1999): «A camera with a view: JenniCAM, visual representation, and cyborg subjectivity», in *Information, Communication and Society,* vol. 2, n. 4, pp. 439-453.

47. KAKALIK, J. S. and WRIGHT, M. A. (1996): «Responding to privacy: Concerns of consumers». *Review of Business,* Fall, 1996, pp. 15-18.

48. KING, C (2001): «Students' Expectation of Privacy: Legal and Ethical Considerations», in *The Social Impacts of Information and Communication Technologies, ETHICOMP 2001,* Gdansk, 18-20 June 2001.

49. KING, C. G. (2001): «E-Commerce: The privacy invasion», *Proceedings of the International Association of the Management of Technology,* Lausanne, Switzerland, on CD.

50. KLEINBERG. J. (2000): «The small-world phenomenon: an algorithm perspective», in *Proceedings of the thirty-second annual ACM symposium on Theory of computing,* New York, NY: ACM Press, pp. 163-170.

51. KRAUT, R., KIESLER, S., BONEVA, B., CUMMINGS, J., HELGESON, V. and CRAWFORD, A. (2002): «Internet paradox revisited». *Journal of Social Issues,* vol. 58, n. 1, pp. 49-74.

52. LAW, J. (2000): «Networks, Relations, Cyborgs: on the Social Study of Technology», in *Centre for Science Studies, Lancaster University Working Paper Series*. Available at: http://www.lancaster.ac.uk/sociology/research/publications/papers/lawnetworks-relations-cyborgs.pdf, retrieved. [27/11/2012].

53. LIU, C. and ARNETT, K. (2002): «An Examination of Privacy Policies in Fortune 500 Web Sites», in *Mid-American Journal of Business,* vol. 17, n. 1, pp. 13.

54. MACKENZIE, D. and WAJCMAN, J. (1999): «Introductory essay: the social shaping of technology», in D. MacKenzie, D. and J. Wajcman (eds.): *The Social Shaping of Technology,* Buckingham: Open University Press, pp. 3-27.

55. MAKEDON, F., FORD, J. C., SHEN, L., STEINBERG, T., SAYKIN, A. J., WISHART, H. A. and KAPADAKIS, S. (2002): «MetaDL: A Digital Library of Metadata for Sensitive or Complex Research Data» presented at *European Conference on Digital Libraries* (ECDL2002) Rome, Italy.

56. MAKEDON, F., KAPADAKIS, S., STEINBERG, T., YE, S. and SHEN, L. (2003): «Data brokers: Building collections through automated negotiation», Dartmouth College Computer Science Department, Hanover, NH, *Technical Report DEVLAB-SCENS-03-02,* March 2003.

57. MANN, S. (1998): «'Reflectionism' and 'diffusionism': new tactics for deconstructing the video surveillance superhighway», in *Leonardo,* vol. 31, n. 2, pp. 93-102.

58. MARTINS, P. and CERQUEIRA, F. (2002): «The Ethical Impact of Human Labour Surveillance on the Organisations», in *ETHICOMP 2002,* Lisbon, Portugal, 13-15 November 2002.

59. MARX, G. (1996): «Electric Eye in the Sky: Some Reflections on the New Surveillance and Popular Culture», in David Lyon and Elia Zureik (eds.): *Computers, Surveillance and Privacy University of Minnesota Press.* Minneapolis/London, pp. 193-233.

60. MASON, D., BUTTON, G., LANKSHEAR, G. and COATES, S. (2002): «Getting real about surveillance and privacy at work», in Woolgar, S. (ed.): *Virtual Society? Technology, Cyberbole, Reality.* Oxford.

61. MILBERG, S. J., BURKE, S. J., SMITH, H. J. and KALLMAN, E. A. (1995): «Values, personal information, privacy and regulatory approaches», *Communications of ACM,* vol. 38, n. 12, pp. 65-74.

62. MOHAMMED, E. (1999): «An examination of surveillance technology and their implications for privacy and related issues - the philosophical legal perspective», *The Journal of Information, Law and Techn*ology, n. 2.

63. MOOR, J. (1997): «Towards a theory of privacy in the information age», in *Computers and Society,* vol. 27, n. 3, pp. 27-32.

64. MOORE, A. D. (2000): «Employee monitoring and computer technology: evaluative surveillance v. Privacy», *Business Ethics Quarterly,* vol. 10 n. 3, pp. 697-709.

65. NAVES, F. (2002): «Adoption of Ethics by small and medium enterprises (SMEs) in Portugal: From Legal Issues to Privacy», *ETHICOMP 2002,* Lisbon, Portugal, 13-15 November 2002.

66. NIE, N. H. (2001): «Sociability, interpersonal relations, and the Internet: Reconciling conflicting findings», *American Behavioral Scientist,* vol. 45, n. 3, pp. 420-35.

67. NORRIS, C. and ARMSTRONG, G. (1998): «Introduction: Power and Vision», in Norris, Clive *et al.* (eds.): *Surveillance, Closed Circuit Television and Social Control,* Ashgate. Aldershot, pp.3-18.

68. O'SHEA, W. (2003): Six Degrees of sexual frustration: Connecting the dates with Friendster.com, *Village Voice,* July 4-10. http://www.villagevoice.com/news/0323, oshea, 44576, 1.html

69. OZ, E., GLASS, R. and BEHLING, R. (1999): «Electronic workplace monitoring: what employees think», *Omega, International Journal of Management Science,* vol. 27, n. 2, pp. 167-177.

70. PRIOR, M. (2002): «Big brother at work: so what? A study of the attitudes of young people to workplace surveillance», *ETHICOMP 2002,* Lisbon, Portugal, 13-15 November 2002.

71. RICHARD G. PLATT, BRUCE MORRISON (1995): «Ethical and social issues of the Internet».

72. REAGLE, J. and CRANOR, L. F. (1999): «The platform for privacy preferences», in *Communications of the ACM,* vol. 42, n. 2, pp. 48-55.

73. REAGLE, J. and CRANOR, L. F. (1999): «Beyond Concern: Understanding Net Users' Attitudes about Online Privacy», *AT&T Labs-Research technical report.* Available at: www.research.att.com/ library/trs/TRs/99/99.4.

74. ROTMAN, D., PREECE, J., HAMMOCK, J., PROCITA, K., HANSEN, D. L., PARR, C., LEWIS, D. and JACOBS, D. W. (2012): «Dynamic changes in motivation in collaborative citizen-science projects», in S. E. Poltrock, C. Simone, J. Grudin, G. Mark and J. Riedl (eds.): CSCW, 217-226.

75. RUDRASWAMY, V. and VANCE, D. A. (2001): «Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment», *Logistics Information Management,* n. 14, pp. 127-137.

76. SEWELL, G. and WILKINSON, B. (1992): «Someone to watch over me': surveillance, discipline and the just-in-time labour process», *Sociology,* vol. 26, n. 2, pp. 271-289.

77. SIEGETSLEITNER, A. and WEICHBOLD, M. (2001): «Personal Privacy Protection in an Austrian Online Survey: A Case Study», in *The Social Impacts of Information and Communication Technologies, ETHICOMP 2001,* Gdansk, 18-20 June 2001.

78. SMIATACZ, M. (2001): «Erosion of Privacy in Computer Vision Systems», in *The Social Impacts of Information and Communication Technologies, ETHICOMP 2001,* Gdansk, 18-20 June 2001.

79. SOLOVE, D. J. (2002): «Conceptualizing privacy», in *California Law Review,* vol. 90, n. 4, pp. 1087-1155.

80. SPIEKERMANN, S., GROSSKLAGS, J. and BERENDT, B. (2002): «E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behaviour», in *3rd ACM Conference on Electronic Commerce* - EC'01, pp. 38-47.

81. SIPIOR, J. C. and WARD, B. T. (1995): «The ethical and legal quandary of email privacy», *Communnications of ACM,* vol. 38, n. 12, pp. 48-54.

82. STURGES, P. and ILIFFE, U. (2001): «Privacy in the Digital Library», in *The Social Impacts of Information and Communication Technologies, ETHICOMP 2001,* Gdansk, 18-20 June 2001.

83. SUTCLIFFE, A. G. (2000): «Requirements Analysis for Socio-Technical System Design», in *Information Systems,* vol. 25, n. 3, pp. 213-233.

84. SYVERSON, P. (2003): «The paradoxical value of privacy», in *2n Annual Workshop on Economics and Information Security* - WEIS'03.

85. TAYLOR, C. R. (2002): «Private demands and demands for privacy: Dynamic pricing and the market for customer information». Department of Economics, Duke University, Duke Economics Working Paper 02-02, 2002.

86. THOMPSON, P. and ACKROYD, S. (1995): «All quiet on the workplace front? A critique of recent trends in British industrial sociology», in *Sociology,* vol. 29 n. 4, pp. 615-633.

87. VILA, T., GREENSTADT, R. and MOLNAR, D. (2003): «Why we can't be bothered to read privacy policies: Models of privacy economics as a lemons market», in *2nd Annual Workshop on Economics and Information Security* - WEIS'03.

88. VILLER, S. and SOMMERVILLE, I. (2000): «Ethnographically Informed Analysis for Software Engineers», in *International Journal of Human-Computer Studies,* vol. 53, n. 1, pp. 169-196.

89. VOLOKH, E. (2000): «Personalization and Privacy», *Communications of the ACM,* vol. 43, n. 8, August 2000, pp. 84-88.

90. WANG, H. (1998): «Consumer privacy concerns about Internet marketing», in *Communications of the ACM*. Available at: http://www.researchgate.net/profile/Huaiqing_Wang/publication/220423357_Consumer_Privacy_Concerns_about_Internet_Marketing/links/0912f510b6206d1887000000.pdf

91. WANG, P. and PETRISON, L. A. «Direct marketing activities and personal privacy: A consumer survey», *J. Direct Marketing,* vol. 7, n. 1, pp. 7-19.

92. WEISBAND, S. P. and REINIG, B. (1995): «Managing user perceptions of email privacy», *Communications of the ACM,* vol. 38, n. 12, pp. 40-47.

Las redes sociales se han convertido en una herramienta de comunicación y contacto habitual para millones de personas en todo el mundo. De hecho, se calcula que más de un 75% de las personas que se conectan habitualmente a Internet cuentan con al menos un perfil en una red social. La autora plantea en el texto si las empresas propietarias de estos servicios ofrecen una información suficiente a los usuarios sobre qué datos recogen, para qué los van a utilizar y si van a ser cedidos a terceros. En una reflexión posterior, propone como posibles soluciones el hecho de que estas empresas pudieran implantar directrices técnicas compartidas y una adaptación normativa, fundamentalmente con la privacidad desde el diseño, la privacidad por defecto y el consentimiento informado. Así, el resultado sería un sistema de información por capas, en el que el usuario fuera conociendo gradualmente las condiciones del tratamiento de su información personal.

Este libro explica el funcionamiento de una red social, comenzando por la creación del perfil de usuario en el que se suministran datos, y analiza cómo la estructura del negocio está basada en la monetización de los datos personales, con sistemas como el *targeting* (catalogando al usuario según sus intereses, características y predilecciones) y el *tracking down* (cruzando información dentro y fuera de la red). La autora distingue entre intimidad y vida privada, introduciendo conceptos como TIC, Internet, sociedad de la información, web 2.0 y redes sociales, con la teoría de los seis grados de separación y sus características, historia y orígenes. Plantea la evolución de la distinción entre espacio público y privado, y la relatividad de las teorías actuales, estudiando también la evolución del comportamiento de los usuarios y hasta qué punto pueden estos desarrollar estrategias de autoprotección.

ISBN 978-84-340-2311-6