COORDINADORES
Joan Balcells Padullés, Agustí Cerrillo-i-Martínez, Miquel Peguera Poch
Ismael Peña-López, María José Pifarré de Moner y Mònica Vilasau Solana

Big Data
Retos y Oportunidades

Actas del IX Congreso Internacional Internet, Derecho y Política
Universitat Oberta de Catalunya. Barcelona, 25-26 Junio, 2013

Big Data
Challenges and Opportunities

Proceedings of the 9th International Conference on Internet, Law & Politics
Universitat Oberta de Catalunya. Barcelona, 25-26 June, 2012

UOC
Universitat Oberta de Catalunya
www.uoc.edu

HUYGENS
EDITORIAL

Big Data: Retos y Oportunidades

Actas del IX Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 25-26 de junio de 2013

Big Data: Challenges and Opportunities

Proceedings of the 9th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 25-26 June, 2013

2013

UOC
Universitat Oberta de Catalunya
www.uoc.edu

HUYGENS EDITORIAL

BIG DATA: RETOS Y OPORTUNIDADES

BIG DATA: CHALLENGES AND OPPORTUNITIES

COORDINADORES

Joan Balcells Padullés, Agustí Cerrillo-i-Martínez, Miquel Peguera Poch
Ismael Peña-López, María José Pifarré de Moner y Mònica Vilasau Solana

© 2013, Huygens Editorial
La Costa, 44-46, át. 1ª
08023 Barcelona
www.huygens.es

ISBN: 978-84-695-8160-5
Editado en España

COMUNICACIONES SOBRE REGULACIÓN

Presentación

Joan Balcells Padullés
Agustí Cerrillo-i-Martínez
Miquel Peguera Poch
Ismael Peña-López
María José Pifarré de Moner
Mònica Vilasau Solana
Comité de dirección
IX Congreso, Internet, Derecho y Política

Se recogen en este volumen las actas de la novena edición del Congreso Internacional Internet, Derecho y Política (IDP 2013), celebrado en Barcelona los días 25 y 26 de junio de 2013. Bajo el título genérico de «*Big Data*: Retos y Oportunidades», el congreso ha tenido como foco principal los aspectos legales y políticos del nuevo fenómeno ligado a la ingente creación de datos de forma automática por el uso de Internet y otros dispositivos digitales. Con el término Big Data suele designarse el fenómeno del crecimiento exponencial en la generación y almacenamiento de datos y los problemas vinculados a su procesamiento, análisis y utilización. Estos datos proceden tanto de la web y de las redes sociales en particular, como de muchas otras fuentes, tanto en el sector público como en el privado, donde se capturan constantemente datos meteorológicos, financieros, de investigación científica, de salud pública, hábitos de los consumidores, o de geolocalización, por señalar sólo algunos campos. La generación de esta abrumadora cantidad de datos se ve facilitada por los dispositivos móviles, satélites, redes distribuidas de sensores, la conectividad de los objetos en el llamado Internet de las cosas, las etiquetas RFID, o el rastro del comportamiento online.

Esta avalancha de datos plantea dificultades para identificar y seleccionar adecuadamente la información relevante y requiere nuevos sistemas de estructuración y de visualización. A la vez ofrece enormes ventajas para mejorar los procesos de toma de decisiones, identificar patrones y tendencias en el mercado, prevenir epidemias y catástrofes naturales, establecer sistemas de alerta temprana, optimizar procesos empresariales, etc. Junto con la creciente capacidad de almacenamiento, los sistemas para cruzar datos y crear perfiles, las técnicas de reconocimiento facial, las posibilidades de rastreo de la navegación ofrecen tanto grandes oportunidades como riesgos evidentes.

Desde el punto de vista jurídico el fenómeno del *Big Data* plantea multitud de cuestiones en términos de privacidad y derecho al olvido, publicidad comportamental, seguridad y conservación de los datos, usos delictivos, propiedad intelectual, estrategias anticompetitivas de control de la información, protección de la anonimidad y libertad de expresión, responsabilidad de los intermediarios, garantías de los sistemas de computación en la nube, problemas medioambientales de los gigantescos centros de datos, etc.

Desde la política, el análisis del *Big Data* brinda nuevas oportunidades estratégicas para los actores políticos (administraciones públicas, movimientos sociales, intermediarios políticos como partidos o sindicatos, etc.), a la vez que abre nuevas perspectivas y añade nuevos métodos para el análisis académico del comportamiento social y político. Esto suscita también cuestiones normativas en el campo del gobierno y de la participación democrática relacionadas con temas de transparencia, acceso de los ciudadanos a la información, reutilización de la información del sector público, nuevos mecanismos de rendición de cuentas y control democrático, brecha digital, apropiación de la información por parte de los poderes públicos, etc.

Centrado en estas cuestiones, pero sin olvidar otros aspectos relevantes en los campos del derecho y la política que plantean desafíos acuciantes para el futuro de Internet, el Congreso Internacional Internet, Derecho y Política ha constituido un lugar de discusión, análisis, formulación de propuestas y planteamiento de líneas de acción.

El congreso, a su cierre, desfila ya hacia su décima convocatoria habiéndose consolidado como un punto de encuentro de investigadores, académicos y expertos de ámbito internacional en el que dar a conocer, analizar y debatir como las Tecnologías de la Información y la Comunicación están cambiando el paradigma de sociedad en el que vivimos y, con ello, el marco regulatorio y político que la acompañan.

En el presente libro de actas se publican las comunicaciones académicas enviadas por investigadores nacionales e internacionales al Congreso Internacional Internet, Derecho y Política y que tras superar un riguroso proceso de selección mediante revisión por pares fueron aceptadas para su presentación en el congreso. El congreso contó además con diversos ponentes invitados que intervinieron en conferencias y mesas redondas, tal como consta en el programa que se incluye a continuación de estas líneas.

El congreso Internacional Internet, Derecho y Política está impulsado y organizado por los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya (UOC) y la revista académica IDP – Revista de Internet, Derecho y Política. En la organización y desarrollo de la edición de 2013 ha participado la Autoridad Catalana de Protección de Datos, ha tenido como colaboradores la agenda Eventos Jurídicos, la firma Reputación Online Legal y la consultora Astrea, así como el destacado patrocinio del Grupo Francis Lefebvre.

Toda la información sobre el congreso se halla disponible en el sitio web http://edcp.uoc.edu/symposia/idp2013/

PROGRAMA

MARTES, 25 DE JUNIO

9.15 Acreditaciones

9.45 Bienvenida

Agustí Cerrillo, Director de los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya (UOC)

10.00 Panel (Propiedad Intelectual e Industrial)

Moderador: Miquel Peguera. Profesor de los Estudios de Derecho y Ciencia Política de la UOC

The Exceptions' Sun Also Rises: When Fair Use Is the Solution

Pedro Letai. Professor of IE Law School

3d Printing, the Internet and Patent Law – A History Repeating?

Marc Mimler. Queen Mary Intellectual Property Research Institute, Centre for Commercial Law Studies (CCLS), Queen Mary University of London

Intellectual Privacy: A Fortress for the Individual User?

Irina Baraliuc. Research Group on Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel (VUB), doctoral researcher

Discusión

11.00 Pausa-café

11:30 Conferencia

Slaves of Big Data. Are we?

Mireille Hildebrandt. Professor of Smart Environments, Data Protection and the Rule of Law at the Institute for Computing and Information Sciences (iCIS) at Radboud University Nijmegen

12:30 Panel (Regulación)

Moderador: Marc Vilalta Reixach. Profesor de los Estudios de Derecho y Ciencia Política de la UOC.

Regulating Code: Towards Prosumer Law?

Chris Marsden. Professor of Law, Law School, University of Sussex

Ian Brown. Senior Research Fellow at the Oxford Internet Institute, Oxford University

Regulation as a Mechanism to Encourage Competition in the Area of Telecommunications: Towards the Concept of Emulated Competition

Humberto Carrasco Blanc. School of Law, University of Edinburgh, Doctoral Research Student

El big data en las Administraciones Públicas: el difícil equilibrio entre eficacia de la actividad administrativa y garantía de los derechos de los ciudadanos

Julián Valero Torrijos. Profesor de Derecho Administrativo. Universidad de Murcia. Coordinador del grupo de investigación iDerTec (Innovación, Derecho y Tecnología)

Discusión

13:30 Lunch

15:00 Panel (Privacidad)

Moderadora: Clara Marsan. Profesora de los Estudios de Derecho y Ciencia Política de la UOC

Preserving Privacy in Times of Counter Cyber-Terrorism Data Mining

Liane Colonna. The Swedish Law and Informatics Research Institute. Stockholm University, Doctoral Candidate

La protección de la identidad personal frente a afirmaciones inciertas en la red

María Dolores Palacios González. Profesora Titular de Derecho civil de la Universidad de Oviedo

Análisis de la normativa europea sobre transferencia de datos contenidos en el registro de nombres de pasajeros (PNR) en el marco de la lucha contra el terrorismo internacional

Alicia Chicharro. Profesora contratada doctora de Derecho Internacional Público. Universidad Pública de Navarra

Discusión

16:00 Pausa

16:15 Panel de ponentes invitados (Derecho penal)

Moderadora: María José Pifarré. Profesora de los Estudios de Derecho y Ciencia Política de la UOC

Digital Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?

John Vervaele. Full Time Professor of Economic and European Criminal Law at Utrecht Law School (the Netherlands) and Professor of European Criminal Law at the College of Europe in Bruges (Belgium)

Los nuevos retos para la protección de la intimidad en la época del cloud

Ivan Salvadori. Professor of Criminal Law and Criminal Computer Law at the University of Barcelona and Postdoctoral Researcher at Università di Verona (Italy)

17:45 Fin del primer día

MIÉRCOLES, 26 DE JUNIO

9:15 Acreditaciones

9:30 Panel (Política)

Moderadora: Ana Sofía Cardenal. Profesora de los Estudios de Derecho y Ciencia Política de la UOC.

Abriendo brechas: centralización de las decisiones e interacción online en CIU, ERC y el PSC

Marc Esteve Del Valle. Doctorando del Programa de Sociedad de la Información y el Conocimiento UOC / IN3

Rosa Borge Bravo. Profesora Agregada de Ciencia Política UOC / IN3

To tweet or not to tweet? Social networking strategies in Catalan local governments

Joan Balcells. Profesor de los Estudios Derecho y Ciencia Política de la UOC.

Albert Padró-Solanet. Profesor de los Estudios Derecho y Ciencia Política de la UOC.

Iván Serrano. Investigador del IN3 (UOC)

Casual Politics: From slacktivism to emergent movements and pattern recognition

Ismael Peña-López. Profesor de los Estudios de Derecho y Ciencia Política de la UOC.

Discusión

10:30 Pausa café

11:00 Conferencia

When does size matter? "Big data," the Web, and social science

Duncan Watts. Principal researcher at Microsoft Research and a founding member of the MSR-NYC lab.

12:00 Panel (Movimientos sociales)

Moderadora: Rosa Borge. Profesora de los Estudios de Derecho y Ciencia Política de la UOC.

Ponencia invitada: Tecnopolítica y 15M. Modelos, datos, hipótesis y análisis de la acción política en la sociedad red

Javier Toret. Investigador y activista. Autor de la investigación "Tecnopolítica y 15M", de próxima publicación

El estudio de la movilización social en la era del Big Data

Jorge L. Salcedo M. Investigador Grupo Democracia Elecciones y Ciudadanía UAB, Consultor de la UOC

Camilo Cristancho. Investigador Grupo Democracia Elecciones y Ciudadanía, Universitat Autónoma Barcelona

Spanish Indignados and the evolution of 15M: towards networked para-institutions

Ismael Peña-López. Profesor de los Estudios de Derecho y Ciencia Política de la UOC

Mariluz Congosto. Investigadora de la Universidad Carlos III de Madrid

Pablo Aragón. Investigador, Barcelona Media Foundation

Discusión

13:30 Lunch

15:00 Panel (Privacidad)

Moderadora: Maria Àngels Barbarà i Fondevila. Directora de la Autoridad Catalana de Protección de Datos

Redes sociales de Internet, responsabilidad no contractual por vulneración del derecho a la protección de datos personales (por el responsable del fichero de datos), y Derecho internacional privado

Alfonso Ortega Giménez. Profesor de Derecho internacional privado de la Universidad Miguel Hernández de Elche (Alicante).

Big Data and Social Control In The Perspective Of Proposed EU Reform On Data Protection

Alessandro Mantelero. Polytechnic University of Turin

Giuseppe Vaciago. University of Insubria

E-Health in the Age of Big Data: The EU Proposed Regulation on Health Data Protection

Panagiotis Kitsos. LLM, PhD. IT Law Team, Dept. of Applied Informatics. University of Macedonia, Researcher

Aikaterini Yannoukakou, Librarian MSc. IT Law Team, Dept. of Applied Informatics. University of Macedonia, PhD candidate

Discusión

16:15 Pausa

16:30 Panel (Privacidad)

Moderadora: Mónica Vilasau. Profesora de los Estudios de Derecho y Ciencia Política de la UOC.

El Uso del Big Data para generar comportamientos

Ramon Miralles. Coordinador de Auditoria y Seguridad de la Información. Autoridad Catalana de Protección de Datos

Automated Journalism: Artificial Intelligence Transforms Data into Stories — When data protection principles and privacy protect the right to express opinions freely and to receive accurate information

Cédric Goblet. Lawyer at the Brussels Bar

Big Data: A Challenge for Data Protection

Philipp E. Fischer. Ph.D. candidate (IN3, UOC Barcelona), LL.M. in intellectual property law (Queen Mary University of London / TU Dresden)

Ricardo Morte Ferrer. Abogado, Master of Laws (UOC). Tutor del Grado en Derecho (UOC). Legal adviser for the TClouds Project at the ULD, Kiel

El derecho a la protección de datos en la administración de justicia

Rosa Cernada Badía. Investigadora de la Universidad de Valencia

Discusión

18:00 Fin del congreso

COMUNICACIONES SOBRE PROPIEDAD INTELECTUAL E INDUSTRIAL

1

INTELLECTUAL PRIVACY: A FORTRESS FOR THE INDIVIDUAL USER?

Irina Baraliuc
Research Group on Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel (VUB), doctoral researcher

ABSTRACT: The digital environment poses numerous challenges to online copyright enforcement. The enforcement measures taken by copyright holders, intermediaries and public authorities might threaten the protection of fundamental rights of the individual, such as privacy and data protection. The concept of «intellectual privacy» potentially creates a framework, within which an individual can enjoy the fruits of creative acts online. It encompasses the protection of individual data concerning one's intellectual consumption and exploration, on one side, and the spatial, temporal and other circumstances pertaining to the freedom to enjoy copyrighted works, on the other side. In this paper, I will explore these various facets of intellectual privacy in its relation to copyright, by getting inspiration from the research conducted by US scholars on the topic. Since the concept was developed in the US, in order to see how the context would operate in the European environment, a necessary step would be to put it in the European legal context, taking particular account of already existing rights, such as privacy, protection of personal data, freedom of expression and information. These reflections prove that intellectual privacy –an embodiment of freedom of expression, privacy and data protection– is a relevant concept. Its instrumentality is determined by the fact that it can be used as a legal tool to shape a private space in the digital environment, within which an individual can enjoy and share copyright-protected content.

KEYWORDS: intellectual privacy, copyright, private space, Internet, fundamental rights.

1. CONTEXT

The copyright debate in 2012 was greatly marked by the ratification process[1] of the Anti-Counterfeiting Trade Agreement.[2] Among its most controversial provisions, there were those dealing with the enforcement of copyright in the digital environment, allegedly

1 Besides a rather obscure negotiation procedure, far from international organizations and the general public, the ratification process of ACTA was marked by popular disagreement (public protests, distributed denial-of-service attacks on Governmental websites, a petition signed by almost 3 million people), individuals worldwide fearing that the agreement would endanger their freedom of expression and information, privacy, etc. See also Baraliuc, I., Depreeuw, S., and Gutwirth, S. (2013). Copyright enforcement in the digital age: a post-ACTA view on the balancing of fundamental rights. *International Journal of Law and Information Technology, 21*(1), 92-104.

2 2011 Anti-counterfeiting trade agreement between the European Union and its member states, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of

imposing disproportional restrictions on fundamental rights and freedoms of individuals. The interaction of various fundamental rights (including the right to privacy, personal data protection, freedom of expression and copyright) has been on the agenda of the Court of Justice of the European Union (CJEU), which was concerned with reconciling these rights, in particular striking a fair balance between them. More recently, the balancing exercise involving copyright and the freedom of expression has become a matter for the European Court of Human Rights (ECtHR).[3] As seen in the recent jurisprudence, the interaction of copyright with fundamental rights is relevant not only for copyright enforcement purposes, but also for enabling an individual to pursue her interests and to develop herself. Needless to say, the digital environment offers tremendous opportunities for both situations, but also poses tremendous threats. When it comes to an individual, one should acknowledge that the freedom of intellectual exploration and development is restricted both by law and technology: on one side, there are the exclusive rights of the creators that need to be protected; on other side, the artistic works might come with technological measures attached primarily aimed at protecting those exclusive rights, but also posing other threats, such as unnecessary monitoring of user behaviour and collection and processing of personal data for purposes other than those related to protection of copyright. In this paper, I will explore the legal boundaries of a space in the digital environment within which a person can lawfully pursue her intellectual goals. First, I will examine the concept of «intellectual privacy», as it was developed by Cohen and Richards, both US scholars. The identified elements of the concept will allow finding their equivalents in the European law. In order to facilitate the shaping of intellectual privacy, the rights forming the concept under European law will be analysed in particular in relation and/or opposition to copyright, considering that intellectual privacy, being a privilege of the user, is often opposed to copyright, which protects the rights of authors and creators. Following, these reflections will be used to test how intellectual privacy sets the legal boundaries of a space within the digital environment, where an individual may lawfully enjoy copyright protected content, in order to foster her intellectual endeavours.

2. INTELLECTUAL PRIVACY IN THE APPROACH OF US SCHOLARS

The concept of intellectual privacy was introduced by Julie Cohen when examining the implications of Digital Rights Management (DRM) technologies on priva-

Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America.

3 *Ashby Donald and others v. France*, Appl. no. 36769/08, ECtHR, 10 January 2013; Inadmissibility decision in *Fredrik Neij and Peter Sunde Kolmisoppi v. Sweden,* Appl. No. 40397/12, ECtHR, 19 February 2013.

cy.[4] Cohen considers the relation between intellectual exploration, a broader term including the consumption of copyright-protected material, and the private physical space, where such consumption takes place, significant for the intellectual privacy. An individual's interests of intellectual privacy are based on her informational privacy interests. While technology enables the collection of data about intellectual consumption and exploration, surveillance and disclosure of such data affects how an individual user will consume content online, thus threating the rights of integrity and self-determination.[5] As a consequence, legal rules have emerged to prevent the disclosure of this data. The intellectual privacy interests lie also in spatial aspects, namely circumstances related to when and where the intellectual consumption occurs. In this sense the law protects the private space, which includes the physical home of an individual, but also spaces within public space where she has reasonable expectations of privacy.[6] This creates a space where an individual can act, including consume and explore her intellectual interests. The individual enjoys a certain freedom that in non-private spaces is either lacking or restricted.

Neil Richards broadens the concept of intellectual privacy, defining it as the ability to develop ideas and beliefs without interference of public and private entities[7] consisting of a number of legal protections that have as their core the most private area of an individual and extending to acts of intellectual consumption and communication.[8] Intellectual privacy is distinct from other concepts of privacy (i.e. informational and spatial privacy taken separately), since it is concerned with how cognitive processes are constructed.[9] Compared to Cohen, Richards enlarges the concept, anchoring it in the First Amendment[10] theory, its core being the freedom of thought and belief. He argues that surveillance and interference of others restrict one's ability to make up one's mind and develop new ideas.[11] The traditional First Amendment theory is focused on the protection of expressing ideas that already exist, being not particularly concerned with how these ideas came to existence. Later theories have considered the freedom of thought as a part of the background for the freedom of speech.[12] Another element of the concept

4 Cohen, J. E. (2003). DRM and Privacy. *Berkeley Technological Law Journal, 18*, 575-617.

5 *Ibidem*, 577.

6 *Ibid.,* 578-579.

7 Richards, N. (2008). Intellectual Privacy. *Texas Law Review*, *87*, 387-445, 389.

8 *Ibidem*, 408.

9 *Ibid.*, 391.

10 The First Amendment stipulates that «Congress shall make no law (…) abridging the freedom of speech».

11 Richards, 389.

12 Such as the democratic self-governance theory; Richards, 396.

is the spatial privacy, as seen in Cohen's approach. The next element, freedom of private intellectual exploration, concerns the ability to develop new ideas by «reading, thinking and discovering new truths»[13] (in Cohen's approach the informational privacy dimension). The latter has not been recognized as such in the American legal theory; yet it has manifested itself in a number of cases dealing with the right to receive information and ideas, defined by the court as fundamental for the society.[14] Richards justifies the lack of a wide recognition of this freedom with the way social norms and institutions have constructed this freedom, without requiring a necessary legal protection of it.[15] The fourth and the last element of Richard's concept is the freedom of confidential communications, concerned both with interception of communication by third parties, and breach of confidence by one's confidants,[16] thus protecting the sharing of ideas, before the individual decides to do so.

The elements of the concept of intellectual privacy as described in the two approaches – the slightly narrower one of Cohen and the one based on freedom of thought of Richards – are (1) informational privacy, (2) spatial privacy, (3) freedom of thought and freedom of expression, and (4) confidentiality of communication.

3. INTELLECTUAL PRIVACY IN THE EUROPEAN CONTEXT

The development of a legal theory of intellectual privacy requires an «act of legal imagination»; its construction should be based on various legal doctrines and traditions, due to the fact that its dimensions do not belong to a single legal doctrine.[17] In this paper, this exercise will be done for the European legal context. In order to set the concept in the European legal framework, it is necessary to see what rights correspond to the above identified elements. First, the informational dimension, which deals with the collection of data concerning the intellectual activity of an individual, will correspond to the data protection right, as long as such data can be related to an individual,[18] or to the right of privacy. The spatial privacy will also correspond to the right of privacy, which provides the individual with a freedom to «experience them-

13 *Ibidem*, 387.

14 *Ibid.*, 417.

15 *Ibid.*, 419. The example given by Richards is that of public libraries, where an individual enjoys the freedom to choose what she reads and to read in private.

16 *Ibid.*, 422.

17 Cohen, 588. Cohen identifies the areas of US law that may define the concept, in the context of application of DRM technologies.

18 Personal data is defined as «any information relating to an identified or identifiable natural person.» Article 2(a), Directive 95/46/EC of the European Parliament and of the Council of 24

selves (…) as they please, void of any interference».[19] The right to privacy will also include the dimension of confidentiality of communications.[20] Finally, the freedom of thought and freedom of expression are reflected as such in the European law. In the following sections, these fundamental rights will be examined in relation to copyright, a fundamental right itself,[21] considering the tensions that may arise when these rights clash with each other, with a particular focus on how they are enacted in the digital environment. The analysis will be based on the Charter of Fundamental Rights of the European Union (hereinafter EU Charter), the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter ECHR), the European Directives in the field of privacy, data protection and intellectual property and the jurisprudence of the Court of Justice of the European Union (hereinafter CJEU) and of European Court of Human Rights (hereinafter ECtHR).

3.1. Privacy and data protection

The right to privacy and the right to protection of personal data are fundamental rights[22]. Data protection enjoys regulation in the EU directive, while it is fair to say that the right to privacy is rather constructed by judicial authorities and academia. The right to privacy, as enshrined in the ECHR, protects private and family life, one's home and correspondence. However, the ECtHR has expanded the right on numerous judicial occasions to include a wide range of issues, such as integrity, secrecy of correspondence and communication, protection of the domicile, protection of personal data, wiretapping, identity, etc., affirming that it was neither possible nor necessary to determine the content of privacy in an exhaustive way.[23] But how do these rights interact with copyright?

October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), OJ L 281.

19 Gutwirth, S. (2002). *Privacy and the information age*. Rowman & Littlefield Publishers.

20 The right to privacy, as stipulated both in the EU Charter and in the ECHR, covers the right to respect one's communications.

21 Protection of intellectual property in Article 17(2) of EU Charter and protection of property in Article 1 of the Protocol 1 to ECHR (see also *Anheuser-Busch Inc. v. Portugal*, Appl. No. 73049/01, §134, ECtHR 2004-XII).

22 Right to privacy in Article 8 of ECHR and Article 7 of EU Charter; right to protection of personal data in Article 8 of EU Charter.

23 «[The Court] reiterates that 'private life' is a broad term not susceptible to exhaustive definition (see, for example, *Glor v. Switzerland*, Appl. No. 13444/04, § 52, ECHR 2009; *Tysiąc v. Poland*, Appl. No. 5410/03, § 107, ECHR 2007-I; *Hadri-Vionnet v. Switzerland*, Appl. No. 55525/00, § 51, 14 February 2008; *Pretty v. the United Kingdom*, Appl. No. 2346/02, § 61, ECHR 2002-III; and *S. and Marper v. the United Kingdom [GC]*, Appl. Nos. 30562/04 and 30566/04, § 66, ECHR 2008).

Since its early development, copyright protection did not extend to the private sphere of individual; an authorization of the right-holder to use copyrighted works, which was enabling an individual to take part in the intellectual life and personal development, was therefore not needed.[24] Such view was generally accepted among the European scholars in the beginning of the twentieth century, but it has been gradually altered once new technologies were emerging. The digital environment challenges the relationship between copyright and privacy, at the same time make it very complex, considering that the rapid technological development constantly and increasingly challenges the law.

The application of exclusive rights of copyright holders in the private sphere of an individual is restricted by the right to privacy. Historically, this exception was justified by the fact that the copyright-holders would exercise no control in the private sphere provided that they had no profit motives and it is reflected in the manner of formulation of exclusive rights in the international conventions, focusing solely on activities that take place in the public.[25] One of the most obvious manifestations of the copyright-privacy nexus would be the private use exception. The private use should not be seen as right of the user in itself, but it is rather an exception to the exclusive right of reproduction of the latter. Moreover, in the European legal framework, the adoption of this exception by the Member States does not have a mandatory character and it triggers the condition of the fair compensation of right-holders.[26] The private use includes the use of a work in the private sphere of an individual, including close friends and family,[27] but its precise scope and content is determined in the national law. This exception is being complicated when it is applied in the digital environment, since technology blurs the boundary between private and public realms, but also complicates the approach towards who are one's friends that form a private space. From a different point of view, the private use exception in the analogue environment may be explained by the fact that it would have been too difficult to exercise control over the various private uses. However, the digital environment eases the monitoring of private uses on a massive scale, thus, the justification of this exception, should it be maintained, needs to be grounded in matters

24 Guibault, L. (2002). *Copyright limitations and contract. An Analysis of the Contractual Overridability of Limitations on Copyright.* The Hague: Kluwer Law International, 48.

25 Senftleben, M. R. (2004). *Copyright, limitations, and the three-step test: an analysis of the three-step test in international and EC copyright law*. Kluwer Law International. 32.

26 Article 5(2)b, Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society (Infosoc Directive). OJ L 167.

27 Walter, M. M. and von Lewinski, S. (2010). *European Copyright Law: A Commentary.* Oxford: Oxford University Press 1032.

other than market failure.[28] Thus, besides the right to privacy, the private use exception may be grounded also in the right to freedom of expression,[29] which shall be examined further in the next section.

Another facet of the copyright-privacy nexus in the digital environment is shaped by the ability of current technologies to monitor and control how individuals use copyright-protected content.[30] First, this is expressed through the implementation of technological protection measures by the copyright holders aimed at blocking access or preventing certain uses.[31] Technologies such as DRM are able of collecting and processing certain personal data relating to the purchase of copyright-protected works, but internet systems may also register data of persons that do not acquire the works, but are only browsing the internet, exploring the possibility of such purchase.[32] Such activities may affect the autonomy of an individual in exploring potential works of interest. The awareness of being monitored has proved to add an undesired scrutiny to the behaviour of an individual and thus it will restrict her options in exploring new opportunities for her intellectual behaviour. Second, the electronic rights-management information systems, together with the technological protection measures, are designed to control and monitor uses.[33] Since such systems may process personal data concerning individual consumption, it is suggested that they should incorporate privacy safeguards according to the Data Protection Directive.[34] Third, internet service providers have the technological ability to monitor electronic communications of individual users. For copyright enforcement purposes, a national court may order disclosure of such data, provided that the infringements have occurred on a commercial scale (a term which lacks a precise legal definition).[35]

In the recent year, the CJEU has been very active in the area of copyright, covering a wide range of issues. For the purpose of this research, it is necessary to examine the

28 Senftleben, 30-31.

29 Senftleben, 33; Bygrave L. A. and Koelman K. J. (2000) Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems. In Hugenholtz P. B. (ed.), *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (pp. 59-124). The Hague, London, Boston: Kluwer Law International.

30 Guibault, 55; Bygrave and Koelman, 108.

31 Walter and von Lewinski, 1065.

32 Bygrave L.A. (2003) Digital Rights Management and Privacy – Legal Aspects in the European Union. In Becker E., Buhse W., Gunnewig D., Rump N. (eds.), *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, (pp. 418-446). Springer. 421.

33 Walter and von Lewinski, 1077.

34 Recital 57 of Data Protection Directive.

35 Article 8 of the Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. OJ L 157.

case-law concerning the collision of copyright and certain fundamental rights, in particular privacy, data protection and freedom of expression, which has been dealt with in the *Promusicae*, *Bonnier*, *Scarlet* and *Netlog* cases:

- An early court case dealing with the relationship between copyright (in particular enforcement) and protection of personal data and privacy was the *Promusicae* case. In its judgement,[36] CJEU analysed the list of exceptions[37] to confidentiality of communications and traffic data[38] stipulated in the e-Privacy Directive. Read together with the exception to safeguard the protection of the data subject or of the rights and freedoms of others in the Data Protection Directive,[39] the Court concluded that Member States are not precluded from imposing the obligation to disclose personal data in the framework of civil proceedings,[40] nor are they compelled to do so.[41] Considering the various fundamental rights involved, the court needs to reconcile these rights, in particular the right to privacy and the right to intellectual property.[42] The provisions of the concerned Directives are quite general, which does not facilitate such a balancing exercise; therefore, the national courts will have to strike the balance between the competing fundamental rights, taking into account that the interpretation of them should be in accordance with the fundamental rights.[43]
- Later, in the *Bonnier* case,[44] CJEU ruled that if there is clear evidence of an infringement an order may be issued to disclose personal data to a copyright holder entitled to act, taking into account the conflicting interests and the principle of proportionality. This strikes the fair balance between the protection of intellectual property and the protection of personal data.[45] Thus, CJEU reinforces the

36 Judgment of the Court (Grand Chamber), 29 January 2008, Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU.*

37 Article 15(1), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive). OJ L 201.

38 Article 5(1), e-Privacy Directive.

39 Article 13(1)g, Data Protection Directive.

40 *Promusicae*, §54.

41 *Ibidem*, §55.

42 *Ibid.*, §65.

43 *Ibid.*, §68.

44 Judgement of the Court (Third Chamber) of 19 April 2012 in Case C-461/10 *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB.*

45 *Bonnier*, §60.

right holders to make use of the available remedies against directly infringing users.

- In the *Scarlet* case,[46] CJEU examined whether an injunction can be imposed on an internet service provider (ISP) to introduce a filtering system of all electronic communications, applied indiscriminately to all its customers, as a preventive measure, for an unlimited period, to which copyright holders are entitled in order to protect their rights from infringement. In applying such injunctions, national courts ought to respect the limitations arising from the e-Commerce Directive, including the prohibition to adopt measures requiring an ISP to carry out general monitoring of communication.[47] Since the injunction to install a filtering system will analyse all communications and collect and identify IP addresses, which are personal data,[48] and since such a system is not able of making a distinction between lawful and unlawful content, which might lead to blocking of lawful communications leading to undermined freedom of information,[49] the Court concluded that the deployment of such a filtering system will not strike a fair balance between the right to intellectual property, on one hand, and the right to protection of personal data and the freedom of expression, on other hand.[50]
- In a similar judgement, in *Netlog* case,[51] CJEU ruled that Member States are precluded from imposing an injunction on a hosting service provider «to install a system for filtering information which is stored on its servers by its service users, which applies indiscriminately to all of those users, as a preventative measure, exclusively at its expense, and for an unlimited period, which is capable of identifying electronic files containing musical, cinematographic or audio-visual work in respect of which the applicant for the injunction claims to hold intellectual property rights, with a view to preventing those works from being made available to the public in breach of copyright»,[52] since such a measure would not

46 Judgment of the Court (Third Chamber) of 24 November 2011 in case C-70/10 *Scarlet Extended SA v Société Belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*; Scarlet is an Internet Service Provider, which does not offer downloading or file sharing services.

47 Article 15(1), Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive).

48 *Scarlet*, §51.

49 *Ibidem*, §52.

50 *Ibid.*, §53.

51 Judgement of the Court (Third Chamber) of 16 February 2012 in Case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*; Netlog NV is an online social network.

52 *Netlog*, §26.

strike a fair balance between the right to intellectual property and the applicable fundamental rights.[53]

These decisions show that, while the copyright holders have a series of measures to enforce and to prevent infringement of their exclusive right, a fair balance needs to be struck between copyright and the fundamental rights of the individuals, which is usually left to the national judicial authorities.

3.2. Freedom of thought and freedom of expression

The right to freedom of thought is provided in Article 10(1) of the EU Charter that is identical with the text of Article 9(1) ECHR, which covers also the rights of freedom of conscience and religion. ECtHR has repeatedly proclaimed that freedom of thought is one of the foundations of a democratic society.[54] The internal dimension[55] of this right includes, among others, the freedom to develop and hold ideas free from state intervention,[56] and it has proved not to be particularly controversial. Its 'internal' nature does not allow posing any limitations on it,[57] making it absolute[58] and unconditional, since it concerns ideas and thoughts in one's conscience, which cannot be as such disturbed by externalities.[59] The latter seems to come in contradiction with Richards' fear that the freedom of thought, at the core of intellectual privacy, might be endangered by the interference of public or private entities. However, the fact that the ideas and thoughts are free in one's conscience (before they are expressed) does not deem the protection of such freedom as unnecessary.[60] It has been stated that surveillance may have a considerable impact on an individual, and being aware of surveillance may inhibit and hinder the development of ideas. Article 9 of ECHR is predominantly concerned with religious

53 *Ibidem*, §§47, 51, 52.

54 *Kokkinakis v. Greece,* Appl. No. 14307/88, ECHR, 25 May 1993, Ser. A, vol. 260-A, §31 via EU Network of independent experts on fundamental rights. (2006). *Commentary of the Charter of Fundamental Rights of the European Union.* (Commentary of the EU Charter) Retrieved 04 March 2013 from http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf, 107; Renucci, J.-F. (2005). Article 9 of the European Convention on Human Rights – Freedom of thought, conscience and religion. Human Rights Files, No. 20, 8.

55 The other dimensions – the external and the collective – are of religious nature, therefore are left out of the scope of the present research.

56 Murdoch, J. (2012). Protecting the right to freedom of thought, conscience and religion under the European Convention of Human Rights. Council of Europe human rights handbooks, 18.

57 Commentary of the EU Charter, 109.

58 *Ibidem.*

59 Renucci, 10.

60 *Ibidem,* 11.

aspects (as seen also in the jurisprudence of ECtHR); however, its scope is quite wide and it covers also personal, political, philosophical and moral conceptions of a certain level of «cogency, seriousness, cohesion and importance».[61] While considered by Richards as the indispensable feature for an individual to develop ideas freely, the freedom of thought, as constructed in the law of the ECHR and of the EU Charter, does not provide any protections to its internal dimension, but rather to the external dimension, i.e. to manifestation and expression. The external dimension of the right enshrined in Article 9 of ECHR concerns manifestation of religious beliefs and convictions and therefore it is of less interest for this research, in contrast to the freedom of expression, discussed further.

Freedom of expression was qualified by the ECtHR as «one of the basic conditions for the progress of democratic societies and for the development of each individual».[62] This right has two dimensions: the freedom to seek and receive information and the freedom to impart information.[63] This freedom, provided in Article 11 of the EU Charter and Article 10 of ECHR, presents more interest in the context of its relation with copyright. On one side, freedom of expression and copyright protection are part of a continuous cycle of «discovery, enlightenment and creation», being essential for and evolving «environment of information, knowledge and culture»[64] and having the same goal to promote speech.[65] On other side, the protection of copyright's exclusive rights clash with the freedom of expression of the individuals who use the copyright protected content to express a personal message and with the freedom of information of the individuals who use the information contained in copyright protected content.[66] The law has responded to this issue by setting boundaries to copyright protection, by establishing limitations on exclusive rights,[67] by setting the idea/expression dichotomy (copyright law protects expression and not underlying ideas, thus lowering the impact of copyright on freedom of expression)[68] and by limiting the term of co-

61 *Ibid.,* 12.

62 *Handyside v. the United Kingdom*, Appl. No. 5493/72, ECHR 7 December 1976, Series A No. 24 §49.

63 Senftleben, 24.

64 Akester, P. (2010). The New Challenges of Striking the Right Balance Between Copyright Protection and Access to Knowledge, Information and Culture. *European Intellectual Property Review*, *32*(8), 372-381, 373.

65 Hugenholtz, P. B. (2001). Copyright and freedom of expression in Europe. In Cooper Dreyfuss R., Leenheer Zimmerman D. and First H. (eds.), *Expanding the Boundaries of Intellectual Property. Innovation Policy for the Knowledge Society* (343-363). Oxford: Oxford University Press.

66 Guibault, 28.

67 Guibault, 29; Senftleben, 23.

68 Guibault, 30.

pyright protection[69] (so that an individual can freely enjoy copyright protected works in the public domain). The limitations of the freedom of expression may be regarded as justifying the respect of creators' rights; in turn, the limitations on copyright may be regards as justifying the respect of the freedom of expression of individuals. The limitations on copyright may be divided in two categories: (a) those based on the informational character of the protected content and (b) those concerning the use of the protected content without the consent of the right-holder. [70] Among these limitations, the right to quote might be one of the most important ones in the context of guaranteeing the freedom of expression, being also the foundation for other rights.[71]

Recently, the relation between copyright and the freedom of expression in the digital environment has come to the attention of ECtHR for the first time in its history:

- In Ashby Donald and others v. France,[72] the Court has confirmed that a copyright enforcement measure may be regarded as interfering with the right of freedom of expression and information.[73] Such interference is legitimate if it is prescribed by law, pursues a legitimate aim and it is necessary in a democratic society.[74] In this case, the Court confirmed that the conviction was prescribed by the French intellectual property laws and it pursued the legitimate aim of protecting others.[75] In determining whether the interference was necessary in a democratic society, the Court stated that the states should enjoy a wide margin of appreciation, in particular because the case concerned content of rather commercial nature[76] and because the balancing of eventually competing interests is a difficult exercise.
- This case was promptly followed by the inadmissibility decision in Neij and Sunde Kolmisoppi v. Sweden case.[77] The ECtHR confirmed that the freedom

69 Akester, 374; Hugenholtz, 343-363.

70 Guibault, 31-32.

71 Guibault, 32.

72 *Ashby Donald and others v. France,* supra note 3. The case concerned the conviction of three fashion photographers for copyright infringement in relation to publication on Internet of pictures taken at fashion shows without the permission of the concerned fashion houses.

73 Voorhoof, D., Hoedt-Rasmussen, I. (2013)/ *ECHR: Copyright vs. freedom of expression*. Kluwer Copyright Blog. Retrieved 4 March 2013 from http://kluwercopyrightblog.com/2013/01/25/echr-copyright-vs-freedom-of-expression/.

74 Article 10(2) ECHR.

75 *Ashby Donald and others v. France,* §36.

76 *Ibidem*, §39.

77 *Neij and Sunde Kolmisoppu v. Sweden,* supra note 4. The case concerned the conviction of two co-founders of the world's largest file sharing services The Pirate Bay seen by the applicants as interference with their right to freedom of expression.

of expression covers also the means of sharing and receiving information, the internet playing a significant role «in facilitating the sharing and dissemination of information».[78] The Court further confirmed that the interference with the applicants' freedom was prescribed by law, namely Swedish Copyright Act and Penal Code, thus pursuing a legitimate aim of protecting the right of others and preventing crimes. The Court focused on the test of «necessity in a democratic society». Since such test cannot be applied in absolute terms, it had to perform a balancing exercise weighing, on one side, the interest of sharing information and, on the other side, the interest in protecting the right of copyright-holders. The protection of copyright[79] may require positive measures by the state, thus the state enjoys a wide margin of appreciation in balancing the competing rights. While the Court does not reflect on the essential elements to be taken into account in the balancing exercise, it states that the margin of appreciation depends, among others, on the type of information: in this case the protection offered to the distributed material (both of lawful and unlawful nature) cannot reach the protection offered to political expression and debate.[80]

The implications of these two cases are manifold. The ECtHR acknowledged that copyright enforcement measure may constitute an interference with the freedom of expression. Since both copyright and the freedom of expression are protected by ECHR as fundamental rights, the states should perform the balancing of the competing interests. However, the Court did not go further and reflect on the criteria that need to be taken into account by the national courts in performing this exercise. On another note, it is interesting to observe the importance given by ECtHR to the nature of the information at issue (one of the aspects taking into account in the test of necessity in a democratic state). First, information of commercial nature is considered of not being of general interest and not contributing to a public debate. Second, the content distributed via «The Pirate Bay» (which may be interpreted as the copyright protected music, films and games or torrent files linking to them) cannot enjoy the same level of protection as political expression and debate. This becomes problematic when viewed through the lens of intellectual privacy: information of both commercial nature (that also enjoys copyright protection) and of artistic nature does not outweigh information of political nature in the intellectual development of an individual and her participation in the society.

78 *Ibidem* with reference to *Times Newspapers Ltd v. the United Kingdom* (Nos. 1 and 2) Appl. Nos. 3002/03 and 23676/03, ECtHR, 2009 and *Ashby Donald and others v. France.*

79 As provided in Article 1 of Protocol 1 to the convention for the Protection of Human Rights and Fundamental Freedoms of 1952.

80 *Neij and Sunde Kolmisoppu v. Sweden.*

4. SHAPING THE SPACE FOR INTELLECTUAL EXPLORATION AND CONSUMPTION

The above reflections lead to a European legal concept of intellectual privacy that is comprised of the fundamental human rights to freedom of expression, privacy and data protection. These rights contribute to the construction of a (private) space in the digital realm where an individual may exercise acts of intellectual exploration and consumption. Such a digital space cannot be seen as a fixed stable space with clear impermeable boundaries. It can be easily imagined as a bubble[81] contoured by thresholds rather than boundaries. The bubble is configured and continuously reconfigured by the activity of individuals and the fundamental rights they enjoy. It is further contoured by how these rights correlate to another competing fundamental right, namely copyright. While freedom of expression, privacy and data protection may create a wide space for the user, copyright comes to limit and redefine these rights. Thus, an individual may enjoy a copyright-protected work in her private space together with close friends and family, without being necessary to obtain the authorization of the copyright-holder. While exploring and enjoying such works, an individual may be protected from unnecessary general monitoring of her communications and unnecessary collection of her personal data. In the process of intellectual exploration, she is free to receive and impart information, such as artistic works when they are in the public domain, ideas that are not protected by copyright law or quotes from copyright-protected works. When the individual shares copyright-protected works, this individual freedom is restricted by copyright enforcement measures available to the creators to protect their exclusive rights.

This research focused on the legal aspects of intellectual privacy and aimed at mapping out the basic legal elements of the concept, considering only occasionally the technological implications. Given the constantly emerging and changing technologies, a next step would be to consider the web architecture in the shaping of the individual space of intellectual exploration and consumption and explore other aspects of the interaction between freedom of expression, privacy and data protection, on one side, and copyright, on the other side.

Finally, the name of the concept «intellectual privacy» does not necessarily immediately infer that the right does also include, besides privacy, freedom of expression and protection of personal data. One may want to replace «privacy» with a more encompassing concept, such as «freedom», «self-determination» or «autonomy». The term «intellectual autonomy» could reflect to a greater extent than other mentioned terms

81 Beslay L. and Hakala H. (2007) Digital Territory: Bubbles. In Kidd P. T. (ed.), *European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society* (pp. 69-78). Cheshire Henbury.

the underlying thought of fostering intellectual exploration and consumption by the individuals, as a feature of the human nature.

5. BIBLIOGRAPHY

Akester, P. (2010). The New Challenges of Striking the Right Balance between Copyright Protection and Access to Knowledge, Information and Culture. *European Intellectual Property Review*, *32*(8), 372-381.

Baraliuc, I., Depreeuw, S., and Gutwirth, S. (2013). Copyright enforcement in the digital age: a post-ACTA view on the balancing of fundamental rights. *International Journal of Law and Information Technology*, *21*(1), 92-104.

Beslay L. and Hakala H. (2007). Digital Territory: Bubbles. In Kidd P. T. (ed.), *European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society* (pp. 69-78). Cheshire Henbury

Bygrave L. A. (2003). Digital Rights Management and Privacy – Legal Aspects in the European Union. In Becker E., Buhse W., Gunnewig D., Rump N. (eds.), *Digital Rights Management: Technological, Economic, Legal and Political Aspects* (pp. 418-446). Springer.

Bygrave L. A. and Koelman K. J. (2000). Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems. In Hugenholtz P. B. (ed.), *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (pp. 59-124). The Hague, London, Boston: Kluwer Law International.

Cohen, J. E. (2003). DRM and Privacy. *Berkeley Technological Law Journal, 18*, 575-617.

EU Network of independent experts on fundamental rights. (2006). Commentary of the Charter of Fundamental Rights of the European Union. Available http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf.

Guibault, L. (2002). *Copyright limitations and contract. An Analysis of the Contractual Overridability of Limitations on Copyright.* The Hague: Kluwer Law International.

Gutwirth, S. (2002). *Privacy and the information age.* Rowman & Littlefield Publishers.

Hugenholtz, P. B. (2001). Copyright and freedom of expression in Europe. In Cooper Dreyfuss R., Leenheer Zimmerman D. and First H. (eds.), *Expanding the Boundaries of Intellectual Property. Innovation Policy for the Knowledge Society* (pp. 343-363). Oxford: Oxford University Press.

Murdoch, J. (2012). *Protecting the right to freedom of thought, conscience and religion under the European Convention of Human Rights*. Council of Europe human rights handbooks.

Renucci, J.-F. (2005). *Article 9 of the European Convention on Human Rights – Freedom of thought, conscience and religion.* Human Rights Files, No. 20.

Richards, N. (2008). Intellectual Privacy. *Texas Law Review, 87*, 387-445.

Senftleben, M. R. (2004). *Copyright, limitations, and the three-step test: an analysis of the three-step test in international and EC copyright law*. Kluwer Law International.

Walter, M. M. and von Lewinski, S. (2010). *European Copyright Law: A Commentary*. Oxford: Oxford University Press.

2

THE EXCEPTIONS' SUN ALSO RISES: WHEN FAIR USE IS THE SOLUTION

Pedro Letai
Professor of IE Law School

One generation passeth away, and another generation cometh; but the earth abideth forever…
The sun also ariseth, and the sun goeth down, and hasteth to the place where he arose…
The wind goeth toward the south, and turneth about unto the north; it whirleth about continually,
and the wind returneth again according to its circuits… All the rivers run into the sea; yet the sea is not full;
unto the place from whence the rivers come thither they return again.

Ecclesiastes

ABSTRACT: The paper would analyze the law and economics of introducing flexibility in the system of exceptions and limitations on European Copyright Law. Such flexibility would exist in an open norm, on the basis of which the courts can decide whether certain uses of copyrighted material are permissible or not, instead of explicitly defining this in the law.

First, it would assess problem areas where the lack of flexibility creates legal disputes and potential barriers to innovation and commercialization. Second, it would analyze the economic rationale and economic effects of introducing flexibility.

Exceptions and limitations in the current copyright system are meant to balance the protection granted to rights owners with the public interest's need to make certain unauthorized uses. However, this paper would identify a number of situations that do not fit well within the current set of exceptions and limitations and attributes this to a lack of flexibility.

Several of these problem areas have given rise to court proceedings with varying outcomes. The interpretation given by courts to existing exceptions and limitations –such as the quotation right, the exception for transient and incidental copying, the private copying exception, and the incidental use exception– is usually too narrow to respond to new technological developments, new developments in the creation process, or new commercialization models. These types of uses generally do not fit the narrowly defined exceptions and limitations and therefore lack legal basis. The same is true for things not yet invented.

KEYWORDS: Copyright; Exceptions; Limitations; Law&Economics; European Law; Intellectual Property.

1. INTRODUCTION

This study analyses the law and economics of introducing flexibility in the system of exceptions and limitations in Continental copyright law. Flexibility would exist in

an open norm, on the basis of which the courts can decide whether certain uses of copyrighted material are permissible or not, instead of explicitly defining this in the law. The paper assesses problem areas where the lack of flexibility creates legal disputes and potential barriers to innovation and production. The core of the study concerns the analysis of the economic rationale and effects of introducing flexibility in the European legal order in the form of an open norm.

Exceptions and limitations in the current copyright system are meant to balance the protection granted to rights owners with the public interest's need to make certain unauthorized uses.

The interpretation given by courts to existing exceptions and limitations –such as the quotation right, the exception for transient and incidental copying, the private copying exception, and the incidental use exception– is usually too narrow to respond to new technological developments, new developments in the creation process, or new commercialization models. These types of uses generally do not fit the narrowly defined exceptions and limitations and therefore lack legal basis. The same is true for things not yet invented.

Because the law is not flexible in itself, courts have increasingly found inventive ways to create legal space for uses that are not covered by the exhaustive list of exceptions. In these cases flexibility with specific evaluation criteria could have been more satisfactory from a legal perspective.

Flexibility could be obtained by introducing an open norm in the Continental copyright system. This paper defines such an open norm for the purpose of analyzing the effects of more flexibility in copyright law. The norm has two main properties. First, it would coexist with the exhaustive list of exceptions and limitations in the current Continental copyright acts. Second, a use of a work would only benefit from the open norm if it passes the so-called three-step test, which takes the interests of the author or right holder into account.

The first category of economic effects of introducing an open norm is that for some known uses that otherwise require licensing, the open norm would allow unlicensed use. This potentially reduces the reward to the creator of a work and therefore decreases the incentive to create. By contrast, it is also likely to reduce the creator's costs of using another work as an input when producing a new work, and therefore to increase the incentive to create. It is difficult to predict which of these two opposing effects ultimately turns the scale in specific markets. Traditional creators generally worry about the negative effect on their reward and seem to believe that the first effect dominates. For businesses that use large numbers of protected works as an input for their services, such as Google, the opposite is true. They emphasize the benefits of reduced input costs and are likely to improve their legal position with an open norm. Collective rights management organizations in turn fear that their bargaining power vis-à-vis users like UCC-platforms, such as YouTube, would suffer from an open norm.

However, given the design of the open norm, it is unlikely that rewards for creators are significantly affected. In case of severe adverse effects on the rights holder, the open norm does not apply. The shift in bargaining power from rights holders to user –platforms– is limited to cases that are currently licensed and where parties are sufficiently confident that the use benefits from the open norm.

The second category of economic effects of introducing an open norm is that the legal delineation between infringement and permissible use becomes capable of accommodating developments in technology and society. This enables entrepreneurs to develop new products and services that rely on currently unforeseen use of protected material. On the downside, flexibility may reduce legal certainty in the short run, until jurisprudence on the practice of flexible copyright has developed.

In sum, the main effects of introducing an open norm seem to be of a legal nature: it changes the legal position of some businesses and therefore affects the costs these businesses make to comply with copyright. Tomorrow's inventions are likely to be facilitated by an open norm. Since most businesses seem currently not chilled by the lack of flexibility, the effect on products and services available in the market is likely to be secondary to the legal effects.

2. DEFICIENCIES IN THE CURRENT EU SYSTEM OF EXCEPTIONS AND LIMITATIONS

With the Information Society Directive the European legislator pursued two goals: first, to bring the laws on copyright and related rights in the European Union in line with the WIPO Internet Treaties, in order to set the stage for joint ratification of the Treaties by the Member States and the European Community. The second, largely unrelated goal of the Directive was to harmonize certain aspects of substantive copyright law across the board, including limitations and exceptions[1]. The harmonization of exceptions and limitations proved to be a highly controversial issue. The difficulty of choosing and delimiting the scope of the limitations on copyright and related rights that would be acceptable to all Member States also proved to be a daunting task for the drafters of the Information Society Directive[2]. Between the times when the proposal for a Directive was first introduced in 1997 and the times when the final text was adopted in 2001, the amount of admissible limitations went from seven to twenty.

---

1 Hugenholtz, P.B. (2000). Why the Copyright Directive is Unimportant, and Possibly Invalid. *EIPR, 2000-11, pp. 501-502.*

2 Explanatory Memorandum to the Proposal for the Information Society Directive, p. 35.

When the time came to devise the limitations on copyright and related rights in the Information Society Directive, the European legislator could therefore rely only on the six express limitations contained in the Berne Convention and on the open norm of the three-step test, according to which limitations must (i) be confined to special cases; (ii) they must not conflict with normal exploitation of the protected subject-matter; and (iii) they must not unreasonably prejudice the legitimate interests of the author. Until the adoption of the Information Society Directive, the exceptions and limitations were harmonized at the European level only in respect of neighboring rights and of the use of computer programs and databases. The existing *acquis communautaire* with respect to exceptions and limitations offered little additional concrete hold upon which the Commission could base new limitations. The limitations listed in the Information Society Directive apply to all categories of works and are modeled either on the provisions of the Berne Convention or on the provisions found in the legislation of many Member States. Article 5 of the Information Society Directive contains a detailed list of limitations on the exclusive rights granted under articles 2 to 4 of the Directive, namely the reproduction right, the right of communication to the public and the distribution right.

The European legislator's decision to restrict the exceptions and limitations to those cases enumerated in article 5 of the Information Society Directive has given rise to severe criticism in the literature. At least three reasons may be advanced cautioning the use of an exhaustive list. First, as the Legal Advisory Board (LAB) already pointed out early on, harmonization does not necessarily mean uniformity. According to the LAB, rules at EC level should allow distinctive features found in national legislations to subsist, as long as they do not hinder the internal market. Second, previous efforts at the international level to come up with an exhaustive catalogue of limitations on copyright and related right have consistently failed. The Berne Convention provides a clear illustration of such unsuccessful efforts, for the possibility of introducing a complete and exhaustive list of exemptions into the Berne Convention had been considered at the Stockholm Conference. The proposal was rejected for two main reasons: (i) because in order to encompass all the principal exemptions existing in national laws, such a list would have had to be very lengthy, and it would still not have been comprehensive; and (ii) since not every country recognized all the possible exemptions, or recognized them only subject to the payment of compensation, experts feared that by including an exhaustive list of limitations, States would be tempted to adopt all the limitations allowed and abolish the right to compensation, which would have been more prejudicial to the rights owners[3].

3 Ricketson, S. and Ginsburg, J.C. (2006). *International Copyright and Neighbouring Rights*. Oxford: Oxford University Press, p. 761.

A third, and probably decisive argument against an exhaustive list of limitations, is that a fixed list of limitations lacks sufficient flexibility to take account of future socio-economic and technological developments. A dynamically developing market, such as the market for online content, requires a flexible legal framework that allows new and socially valuable uses that do not affect the normal exploitation of copyright works to develop without the copyright owners' permission, and without having to resort to a constant updating of the Directive, which might take years to complete[4].

Not only is the list of exceptions and limitations contained in article 5 of the Directive exhaustive, but all but one exception are optional. The regime of limitations established by the Information Society Directive leaves Member States ample discretion to decide if and how they implement the limitations contained in article 5 of the Directive. This latitude not only follows from the fact that all but one of the twenty-three limitations listed in the Directive are optional, but more importantly from the fact that the text of the Directive does not lay down strict rules that Member States are expected to transpose into their legal order. Rather, articles 5(2) to 5(5) of the Directive contain two types of norms: one set of broadly worded limitations, within the boundaries of which Member States may elect to legislate; and one set of general categories of situations for which Member States may adopt limitations. The outcome is that Member States have implemented the provisions of articles 5(2) to 5(5) of the Directive very differently, selecting only those exceptions that they consider important. With such a mosaic of limitations throughout the European Community, the aim of harmonization most likely has not been achieved, and legal uncertainty persists. The assessment of the boundary between infringing and non-infringing conduct, remains therefore highly uncertain and unpredictable. The fact that Member States have implemented the same limitation differently, giving rise to a variety of different rules applicable to a single situation across the European Community, could ultimately constitute a serious impediment to the establishment of cross-border services.

A number of situations arise that do not fit well within the current set of exceptions and limitations in the copyright system. Among these uses are the activities of search engines, either for the display of thumbnails in search results or for the dissemination of news articles; the use of works in 'user created content'; cloud computing; data mining; distance learning; and other transformative uses, such as those of documentary filmmakers. Several cases have given rise to court proceedings. The interpretation given by courts to existing exceptions and limitations like the quotation right, the exception for transient and incidental copying, the private copying exception, and the incidental use exception is usually too narrow to respond to new technological developments, or new behavioral patterns in

4 Hugenholtz, P.B. (2000). Why the Copyright Directive is Unimportant, and Possibly Invalid. *EIPR, 2000-11, pp. 501-502.*

the creation process or commercialization models. The majority of these types of uses are considered to fall outside the scope of the narrowly defined exceptions and limitations on copyright, with the consequence that such uses either may not take place at all and if they do, their legal basis is uncertain at best. Where such new forms of uses have led to legal disputes based on claims of copyright infringement, the outcome has been variable between the Member States both in terms of final solution and in terms of motivation. Because the system of the law is not flexible in itself, courts have increasingly come up with inventive ways to create space in the law for the uses that are not covered by the exhaustive list of exceptions, but which they felt should not be prohibited by copyright. The lack of flexibility of the present system of limitations and exceptions can be demonstrated by the way courts in several Member States have in recent years struggled to, nevertheless, protect the general social, cultural and economic interest by allowing certain free uses not expressly recognized in the law. Although the outcome of many legal disputes may be socially desirable, the paths followed by the courts towards a solution are often open to discussion, especially if they reverse the normal burden of proof between rights owners and users, towards a regime where rights owners have to take extra measures to indicate that the rights are reserved, which may encroach upon copyright law's principle of exclusivity. In these cases the application of a well-defined open norm with specific evaluation criteria could have provided more satisfaction from a legal perspective.

Technological change is not likely to slow down. Technological developments are expected to bring about new, innovative services the success of which will be growing, or services that are still 'under construction' or have not even been invented yet. These services are potentially problem areas as well, already appearing at the horizon or still lying further in the future. Either way, it is at this point difficult to foresee how far these developments will go. Therefore, a rigid system with an exhaustive list of static exceptions will continue to create new controversies with respect to future use of copyrighted material, which may hamper innovation.

Things not yet invented are of course hard to describe or predict. What one can predict, however, is that it is very likely that such technologies or services will struggle to develop under the current system of exceptions and limitations. The UK needs to explore with its EU partners a new mechanism in copyright law to create a built-in adaptability to future technologies which, by definition, cannot be foreseen in precise detail by today's policy makers. This latter change will need to be made at EU level, as it does not fall within the current exceptions permitted under EU law. The alternative, a policy process whereby every beneficial new copying application of digital technology waits years for a bespoke exception, will be a poor second best[5].

5 Hargreaves, I. (2011). Digital Opportunity. A Review of Intellectual Property and Growth. *Hargreaves Review*, p. 47.

3. DEFINING AN INSTRUMENTAL OPEN NORM FOR ECONOMIC ANALYSIS

An open norm should introduce sufficient flexibility to allow certain types of innovative uses and remove undesirable legal barriers for creative re-use and commercial exploitation and for the development of new online business models. By letter of the law, the current system of copyright exceptions and limitations does not seem to permit various types of socially, culturally and economically legitimate uses by search engines, digital education services and documentary filmmakers or for enabling cloud computing, data mining or user created content.

Although the lawfulness of the uses mentioned is not yet frequently challenged in court and, if it is, the courts often show flexibility by applying external legal constructs to allow certain free uses that are not explicitly permitted by copyright law, the current inflexibility of copyright exceptions and limitations undeniably creates legal problems. An ever-growing discrepancy between what is tolerated in practice and what is legally permitted entails the risk of undermining copyright law's social legitimacy, at least in the long run[6]. From a legal perspective, therefore, there is sufficient reason for closing these existing discrepancies. Introducing an open norm would have the benefit of remedying the situation for current and future occasions. Once implemented, it would prevent the legislator from having to change the law each and every time it would need to accommodate a new technology or service. An obvious prerequisite is that, should an open norm be introduced, due account ought to be taken of the legitimate interests of the relevant right holders.

The question remains what the economic consequences of the introduction of an open norm would be. This requires an a priori concretization of such norm. In general, an open norm can take different forms, varying from a narrow provision offering flexibility for a specific type of use to a generic open norm providing flexibility for a virtually undetermined range of uses. To be able to assess the economic consequences of an open norm, therefore, the contours of what an open norm might look like must first be identified.

In order to arrive at an open norm that would offer sufficient flexibility for enhancing innovation and removing undesirable legal barriers for creative re-use and commercial exploitation and for the development of new online business models, a number of proposals and existing models are examined. There are basically two ways for introducing flexibility: one option is to seek flexibility within the boundaries of the existing framework of the law; a second possibility is to introduce a new open norm at the EU level.

---

6 Hugenholtz, P.B. and Senftleben, M.R.F. (2011). Fair Use in Europe. In Search of Flexibilities. Amsterdam, p.10.

A third possibility would be to use the existing policy space in EU and international copyright law to introduce or enhance flexibilities in national copyright law. At first sight, the policy space at the EU level seems rather limited, given the closed list of permitted exceptions and limitations under the Information Society Directive[7]. However, in many cases the exceptions and limitations enumerated in the Directive are not precisely circumscribed, but formulated as categorically worded prototypes that leave the national legislators considerable margins of implementation[8]. Moreover, the right of adaptation has remained a largely unharmozised terrain of EU copyright law and that, as a result, there seems to be sufficient room for national legislators to provide for an exception or limitations permitting particular types of transformative uses, e.g., in the context of UCC[9].

One way of introducing more flexibility in national copyright law is for national legislators to explore the existing policy space under the distinct exception prototypes and/or to introduce a specific exception or limitation permitting the production and dissemination of particular types of adaptations[10]. While an approach of the kind suggested here would certainly add flexibility to the existing regime of exceptions and limitations in national copyright law, it does not establish a truly open- ended norm. At most, it could inspire national governments, within the confines of one or more existing exceptions or limitations, to introduce a set of distinctive open norms for specific purposes or uses for which flexibility is identified as being critical.

The eventual open norm could be comprised of (i) the substantive elements of the distinct exception prototypes with flexible features included in the Information Society Directive, plus (ii) the last two steps of the three-step test, because the cases covered by this rule are to be regarded as certain special cases, they deemed it unnecessary to also include the first step.

It can be read as follows:

'It does not constitute an infringement to use a work or other subject-matter for non-commercial scientific research or illustrations for teaching, for the reporting of current events, for criticism or review of material that has already been lawfully made available to the public, or quotations from such material serving compara-

7 Hugenholtz, P.B. and Senftleben, M.R.F. (2011). Fair Use in Europe. In Search of Flexibilities. Amsterdam, pp. 1-30.

8 Hugenholtz, P.B. and Senftleben, M.R.F. (2011). Fair Use in Europe. In Search of Flexibilities. Amsterdam, pp. 14 et seq.

9 Hugenholtz, P.B. and Senftleben, M.R.F. (2011). Fair Use in Europe. In Search of Flexibilities. Amsterdam, pp. 26-27.

10 Hugenholtz, P.B. and Senftleben, M.R.F. (2011). Fair Use in Europe. In Search of Flexibilities. Amsterdam, p.2 and pp. 29-30.

ble purposes, for caricature, parody or pastiche, or the incidental inclusion in other material, provided that such use does not conflict with a normal exploitation of the work or other subject-matter and does not unreasonably prejudice the legitimate interests of the right holder[11].

While coming close to an open-ended defense, the proposed norm inevitably remains semi-open. That is, it cannot go beyond the express boundaries set by the closed list of permissible exceptions and limitations under current EU copyright law and, consequently, 'can hardly empower judges to identify new use privileges on the mere basis of abstract criteria, such as those constituting the three-step test[12].

Whereas the existing legal framework enables the legislature and the courts to introduce or enhance flexibility in copyright law in a number of ways, it does not permit them to adopt a generic open norm offering flexibility for a variety of unspecified unauthorized uses. Under the current framework of exceptions and limitations at the EU level, Member States can introduce a semi open norm at best.

As a consequence, if the legislator would want to introduce or enhance flexibility in current national copyright law unilaterally, that is, without having to rely on the EU legislator, then it can only do so by exploring the existing policy space under EU law.

The present study seeks to examine the economic consequences of the introduction of a generic open norm. Because under the current EU framework the introduction of a generic open norm is not permitted, the concretization of the open norm must occur at a level that exceeds the existing EU legal framework.

3.1. Towards a Generic Open Norm

There are a few models that may serve as inspiration for adopting an open norm that would enable the legislator to introduce flexibility for a variety of unspecified unauthorized uses. It must be emphasized that these models go beyond what is permitted by the current legal framework of exceptions and limitations at the EU level. Adopting such a model would thus require legislative action by the EU legislator. This section examines two types of models that exceed the existing EU legal framework. First, it looks at the option of introducing an open norm along the lines of the US fair use doctrine. Second, it analyses the possibility of adopting an open norm as recently proposed in the Wittem Group's European Copyright Code.

---

11 Hugenholtz, P.B. and Senftleben, M.R.F. (2011). Fair Use in Europe. In Search of Flexibilities. Amsterdam, pp. 17-18.

12 Hugenholtz, P.B. and Senftleben, M.R.F. (2011). Fair Use in Europe. In Search of Flexibilities. Amsterdam, p.17.

3.1.1. An Open-Ended Fair Use Exemption

Proposals for introducing an open norm in the area of copyright exceptions and limitations often take as example the existing fair use exceptions in the United States and a few other countries. The fair use doctrine was developed by US courts in the twentieth century without the aid of specific statutory guidance. In 1976 it was codified in the US Copyright Act. Later, it found its way into the copyright laws of other jurisdictions. The relevant provision of the US Copyright Act (17 U.S.C. § 107) reads as follows:

> *'the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include:*
>
> - *the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;*
> - *the nature of the copyrighted work;*
> - *the amount and substantiality of the portion used in relation to the copyrighted work as a whole;*
>
> *and*
>
> - *the effect of the use upon the potential market for or value of the copyrighted work.*
>
> *The fact that a work is unpublished shall not itself consideration of all the above factors.'*

The US fair use exception is characterized by the open-ended list of purposes for which the use of a work may be regarded as fair, marked by the words 'such as', and by the four factors set out to be considered in determining whether or not a particular use is fair.

In Europe, the fair use doctrine is often perceived as a purely American concept, very distinct from the European civil law style exhaustive enumeration of exceptions and limitations and even from the common law concept of fair dealing. The consultation on the Green Paper on Copyright in the Knowledge Economy reveals that, while some stakeholders embrace fair use as an instrument introducing flexibility to accommodate new, innovative uses in the digital environment, others are very critical about it, stating that transplanting the US fair use system, which developed through decades of jurisprudence, would be highly problematic and run contrary to the legal traditions of most EU Member States. Consequently, in Europe, proposing an open norm along the same lines as the US fair use doctrine is rather controversial.

3.1.2. An Open Norm as Formulated by the Wittem Group

One proposal that introduces a flexible open norm while keeping close to the legal traditions in Europe is the European Copyright Code, a model law drafted by a group of European scholars that named themselves the Wittem Group[13]. Chapter 5 of the Code lays down a semi-open structure of copyright exceptions and limitations. First, it explicitly enumerates the permissible exceptions and limitations and groups them by reference to their objectives and rationales, covering uses with minimal economic significance (Article 5.1), uses for the purpose of freedom of expression and information (Article 5.2), uses permitted to promote social, political and cultural objectives (Article 5.3) and uses for the purpose of enhancing competition (Article 5.4). Next, in Article 5.5, it extends the scope of these specifically enumerated exceptions and limitations by permitting any other use that is similar to the uses enumerated in Articles 5.1 to 5.4(1), subject to the application of the corresponding requirements of the relevant exception or limitation and the three-step test. In line with the 'Declaration on a Balanced Interpretation of the «Three-Step Test» in Copyright Law' (see Section 3.2.2), a fourth element is added, namely the requirement to take account of the legitimate interests of third parties. The provision is formulated as follows:

> *'Art. 5.5 – Further limitations*
>
> *Any other use that is comparable to the uses enumerated in art. 5.1 to 5.4(1) is permitted provided that the corresponding requirements of the relevant limitation are met and the use does not conflict with the normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author or right holder, taking account of the legitimate interests of third parties.'*

By combining a set of clearly defined exceptions and limitations with an open-ended norm that extends the available exceptions and limitations to similar uses, the European Copyright Code reflects 'a combination of a common law style open-ended system of limitations and a civil law style exhaustive enumeration'[14]. Hence, this seems to better fit the European legal tradition than the US fair use doctrine. Moreover, the semi-open structure of exceptions and limitations suggested in the Code 'guarantees both a level of legal security and fairness, by combining relatively precise norms with sufficient flexibility to allow a fair outcome in hard and/or unpredictable cases'[15]. As sta-

---

13 *European Copyright Code*, http://www.copyrightcode.eu/. The Drafting Committee consisted of L. Bently, T. Dreier, R. Hilty, P.B. Hugenholtz, A. Quaedvlieg, A. Strowel and D. Visser. J. Bing, R. Clark, F. Gotzen, E. Mackaay, M. Ricolfi, E. Traple, M. Vivant and R. Xalabarder were in the Advisory Board.

14 *European Copyright Code*, explanatory footnote 48.

15 Hugenholtz, P.B. and Senftleben, M.R.F. (2011). Fair Use in Europe. In Search of Flexibilities. Amsterdam, p.9.

ted in the Code, this 'is indispensable in view of the fact that it is impossible to foresee all the situations in which a limitation could be justified'[16].

At the same time, the flexibility offered is not unlimited. First, the reference to 'comparable uses' ensures that 'the courts can only permit uses not expressly enumerated insofar as a certain analogy can be established with uses that are mentioned by the Code'[17]. This implies that uses that are permitted under the proposed Article 5.5 are not necessarily without compensation. If the use is analogous to a use permitted by a limitation that is subject to the payment of compensation, the use under the open norm would inevitably also be subject to the payment of compensation. This is the consequence of the analogy that is assumed in the open norm of Article 5.5 and the condition that the corresponding requirements of the relevant limitation must be met.

Accordingly, the various uses identified in Chapter 2 that do not fall under a specified exception or limitation would be permissible only if it can be established that they are somehow comparable with one or more expressly enumerated exemptions[18]. Taking the use of thumbnails by search engines as an example, the courts could permit such use under the proposed Article 5.5 if they find that there is a certain analogy with the incidental use of works (Article 5.1 under (2)), the use of works for quotations (Article 5.2(1) under d), or any other use listed in Articles 5.1 to 5.4(1). Likewise, the other uses mentioned in Chapter 2 could be put to the test of the proposed Article 5.5 provided that a certain analogy can be established with uses permitted by one of the expressly enumerated exemptions. This will depend on the particular circumstances of each case.

Second, Article 5.5 would only permit comparable uses that do not conflict with the normal exploitation of the work and that do not unreasonably prejudice the legitimate interests of the author or right holder, taking account of the legitimate interests of third parties. These criteria ensure that the courts can balance the interests of stakeholders on both sides of the equation.

3.2. Conclusion

It can be concluded from the previous analysis that, if the aim is to arrive at an open norm that would offer flexibility for enhancing innovation and removing undesirable legal barriers for creative re-use and commercial exploitation and for the development of new business models, the model that could best be pursued is the one proposed in the Wittem Group's European Copyright Code. Although it would require legislative

16 *European Copyright Code*, explanatory footnote 48.

17 *European Copyright Code*, explanatory footnote 48.

18 As the explanatory footnote in the *European Copyright Code* (footnote 55) indicates, 'art. 5.5 does not allow new limitations by blending the criteria of articles 5.1 to 5.3'.

action by the EU legislator, it has several benefits over the other models examined. First, by combining a set of specifically enumerated exceptions and limitations with a generic open norm offering flexibility for any use that is comparable to the uses specifically listed, the European Copyright Code has prevalence over the models that national legislators are permitted to adopt under the current legal framework, which at best are semi open and therefore do not meet the minimum requirement of establishing an open norm. Second, the system proposed in the European Copyright Code keeps closest to the European legal traditions. Therefore, it has a better chance of getting accepted in Europe than the US-style fair use doctrine or the related provision tentatively suggested by the Irish Copyright Review Committee in its 2012 consultation paper on 'Copyright and Innovation'.

In line with the model set forth in the European Copyright Code, this study uses an open norm that would coexist with the specifically enumerated exceptions and limitations in the current legislation. It would authorize any other use that is comparable to the uses expressly permitted under the exceptions and limitations listed, subject to the application of the corresponding requirements of the relevant exception or limitation and the operation of the three-step test. This means that all existing exceptions and limitations, such as incidental use, the quotation right, the parody exception, the private-copyright exception, and so on, would remain intact and their scope would be extended by an open-ended rule. Similar to the proposal of the Wittem Group, this rule could be formulated as follows:

> *'Any other use that is comparable to the uses enumerated in Chapter 6 of this Act is permitted provided that the corresponding requirements of the relevant limitation are met and the use does not conflict with the normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author or right holder, taking account of the legitimate interests of third parties.'*

An open-ended provision of this kind seems to provide sufficient flexibility to respond to cultural and technological change (by permitting new, innovative and yet unforeseeable uses), while taking due account of the legitimate interests of authors, right holders and users. By also bringing third parties into the equation, the norm seems to be built upon a balanced interpretation of the three step test as proposed in the 2008 Declaration initiated by the Max Planck Institute for Intellectual Property and the School of Law at Queen Mary (Section 3.2.2). If the relevant steps of the three step test included in the proposed rule would indeed be interpreted in a balanced way, this could add to the flexibility that the open norm endorses. Moreover, it would offer guidance to the legal interpretation of the rule, thus enhancing legal certainty for all stakeholders involved.

It must be emphasized that the concretized norm does not imply that uses permitted are without compensation. If the use is comparable to a use permitted by a limitation that is subject to the payment of compensation, the requirement that the

corresponding requirements of the relevant limitation must be met ensures that the use under the open norm would inevitably also be subject to the payment of compensation. Furthermore, to address possible right holder's concerns, it could be provided by law or duly explained in the Explanatory Memorandum accompanying the proposal that it would be the burden of the party invoking the open norm to establish why the defense should be honored.

The open norm that is concretized in this paper is to be regarded as an instrumental legal variable providing the necessary legal framework for economic analysis only. It is not to be interpreted as the preferred model for future legislation. Identifying the most suitable legal model is not the object of this study.

4. ECONOMIC EFFECTS OF INTRODUCING COPYRIGHT FLEXIBILITY

There is a substantial literature on the economic consequences of fair use in the United States. For instance, the economic contribution of industries in the United Stated that rely on fair use and related exceptions can be divided into core and non-core industries. The former are industries that are wholly engaged in creation, production and manufacturing, performance, broadcast, communication and exhibition, or distribution and sales of works and other protected subject matter[19]. They conclude that in 2007 these industries are responsible for 16.2 % of total GDP in terms of value added. These industries employ some 17.5 million people, grow relatively fast and have a fast expanding export base. Many industries that rely on copyright protection in their business model can also righteously be claimed to rely on fair use. Think for instance of media and entertainment industries, that rely on fair use as an input and rely on protection of their output. However, this literature is of limited value for an assessment of the economic consequences of introducing flexible copyright within –or as an extension of– the EU system of exceptions and limitations. The reason for this is that comparing the economic value of fair use to a rigid copyright system with no exceptions or limitations is rather irrelevant. That is, the counterfactual in most fair use studies is not comparable to European copyright law with its closed list of exceptions and limitations.

The specification of the open norm is instrumental to the assessments of economic effects. Firstly, current exceptions and limitations remain in place. This implies that uses that currently benefit from an exception or limitation would continue to benefit from that exception or limitation in a system with an open norm. Secondly, a use of a work would only benefit from the open norm if it does not conflict with the normal exploi-

19 Rogers, T. and Szamosszegi, A. (2010). *Fair use in the U.S. economy: Economic contribution of Industries relying on Fair Use*. Washington, DC: Computer & Communications Industry Association (CCIA).

tation of the work and does not unreasonably prejudice the legitimate interests of the author or right holder.

5. CONCLUSION

The economic literature on fair use generally bears little significance to the open norm in a European context, since an all-or-nothing interpretation of fair use is misleading in the context of the existing system of exceptions and limitations.

In this paper the introduction of an open norm was analyzed from two angles. It constitutes for specific cases a mild reduction of protection, subject to the application of the open norm-test by the courts on a case-by-case basis. As such, it may give rise to a reduction in reward for creators who want to commercialize their work. This paper concludes that this effect is likely to be limited, because the open norm is designed in such a way that it does not apply when it would lead to a significant decline in reward to the creator. Moreover, a large part of the uses that would benefit from the open norm are expected not to generate reward to creators in the present situation.

Therefore, the introduction of an open norm might well be a Pareto improvement; some actors benefit from it while nobody suffers from it. The benefit that was investigated in this study is for professionals and amateurs that use protected works to create new works. However, many of the acts that we identified as beneficiaries of an open norm seem not to be deterred by the lack of it.

The chilling effect of the lack of flexibility was not supported by the available data, even though it is worth mentioning that such chilling effect is by nature hard to observe. These acts currently have a weak legal basis, but courts have in some instances found artifices to accommodate them.

At first sight, the main effect of an open norm for producers of new works thus is an improved legal position. Yet, the benefits of this improved legal position may not materialize on the short run. To acquire legal certainty, actors involved must 'try' the open norm in court and allow for case law to develop.

Whether the effect of an open norm indeed is a Pareto improvement which leaves no party worse off in each specific case cannot be foreseen. The open norm may shift the balance in bargaining power for practices that are currently licensed, such as contracts between collective rights organizations and UCC-platforms. This effect is however limited to cases where both parties believe that the licensed use might benefit from the open norm; bargaining power is not expected to change in clearly commercial transactions. Other strategic effects that could not be assessed in this study are the externalities arising when courts start to look at other court cases to decide on the outcome. This has also been termed circularity. The risk attitudes of users then become important: When a user feels uncomfortable with relying on an open norm and buys a license instead, this

action may perhaps make it more difficult for another user to rely on an open norm in a similar case.

At first sight, the main effect of an open norm for producers of new works thus is an improved legal position. Yet, the benefits of this improved legal position may not materialize in the short run. To acquire legal certainty, actors involved must try the open norm in court and allow for case law to develop. Whether the effect of an open norm is a Pareto improvement, which leaves no party worse off in each specific case, cannot be foreseen. The open norm may shift the balance in bargaining power for practices that are currently licensed, such as contracts between collective rights organizations and UCC-platforms. This effect is, however, limited to cases where both parties believe that the licensed use might benefit from the open norm; bargaining power is not expected to change in clearly commercial transactions.

Thus, the main effects of introducing an open norm are of legal nature: it changes the legal position of some businesses and therefore affect the costs these businesses make to comply with copyright. These costs may only decrease on the longer run. The effect on products and services available in the market is likely to be secondary to these legal effects.

6. BIBLIOGRAPHY

Hargreaves, I. (2011). Digital Opportunity. A Review of Intellectual Property and Growth. *Hargreaves Review*.

Hugenholtz, P.B. (2000). Why the Copyright Directive is Unimportant, and Possibly Invalid. *EIPR, 2000-11*.

Hugenholtz, P.B. and Senftleben, M.R.F. (2011). Fair Use in Europe. In Search of Flexibilities. Amsterdam.

Ricketson, S. and Ginsburg, J.C. (2006). *International Copyright and Neighbouring Rights*. Oxford: Oxford University Press.

Rogers, T. and Szamosszegi, A. (2010). *Fair use in the U.S. economy: Economic contribution of Industries relying on Fair Use*. Washington, DC: Computer & Communications Industry Association (CCIA).

3D PRINTING, THE INTERNET AND PATENT LAW – A HISTORY REPEATING?

Marc Mimler*
Queen Mary Intellectual Property Research Institute, Centre for Commercial Law Studies (CCLS), Queen Mary University of London

ABSTRACT: 3-D printers are used to print three dimensional objects. Depending on the method applied the created object is constructed of a sort of plastic that the printer produces and shapes in the requested shape. 3-D printers have become more and more affordable in recent times and have therefore reached a wider distribution among the general public. Users can therefore nowadays print 3-D objects from the comfort of their home. Additionally, there are websites available that can be accessed to download files that contain templates which can be read into a computer and used for printing objects. This development may have important, if not dangerous ramifications. There have been reports that 3-D printing has been used to produce parts of handguns which otherwise needed to be registered.

But the development may also have an enormous impact on Intellectual Property (IP) Rights holders. 3-D printing could be used to produce objects that are covered by an IP right. One could for instance print an object which is covered by a design right. But there could also be the possibility to produce an object covered by a patent, trade mark or copyright.

This paper wishes to analyse this issue in relation to the law of patents and will discuss the pertinent laws of the United Kingdom and Germany. Its focus will be on assessing whether the making available of files that contain templates for objects used for printing may constitute an indirect infringement of the patented object. Ultimately, the paper wants to analyse whether the law of patents is adequately equipped to deal with these new developments.

KEYWORDS: 3D Printing, Patent Law, Indirect patent infringement, United Kingdom, Germany, Internet.

1. INTRODUCTION

If one considers the futuristic gadgets that some science fiction tales such as Star Trek depict then one can imagine that the evolving technology of 3D printing may herald the dawn of a new age for mankind. Replicators are one of the fantastic inventions

* My thanks go to Dr Manfred Mimler for his useful comments on the draft of this paper. Additionally, I would like to thank Dr Gaetano Dimita, Dr Phillip Johnson and Ms Priscilla Robledo for their useful comments, ideas and suggestions in relation to this paper.

that are displayed within the Star Trek universe. They are able to produce something as trivial like a cup of Earl Grey tea drunk by Captain Picard on the star ship Enterprise to much more complex apparatuses and objects. The use of replicators facilitates the lives of people living at the *final frontier* of the known and inhabited galaxy. Moreover, they exemplify a fundamentally important aspect of a utopian world in which mankind is self-sufficient and where poverty is banished: Due to the fact that almost everything needed could be reproduced, mankind is able to shift its focus from the pursuit of amassing riches to provide for its livelihood to «exploring strange new worlds and seeking out new life forms and civilisations». A brave new world!

The inception of 3D printing may have brought us a step closer to the utopia that Star Trek provides.[1] However, only the future can reveal whether this eventually may occur.

Today's 3D printing technology does however raise more contemporary issues that might have real implications for our societies and economies. A technology that allows reproducing 3-dimensional objects raises great expectations as 3D printing could fundamentally change the way that today's economies of scale operate. One example that is mentioned in this regard is that it may have ramifications on the way manufacture is conducted nowadays. Economies of scale tend to shift production to countries where labour costs are comparatively lower. 3D printing may reverse this development. It has been said that it could bring back manufacture to countries of the developed world as the advantage of low cost countries vanishes.[2] The positive effects on the environment have also been mentioned as the need for worldwide transportation of goods decreases.[3]

It was also mentioned that 3D printing could rupture the distribution chain between manufacturer and consumer by circumventing distributors, wholesalers and retailers. Consumers could obtain a template directly from the designer of this object via the internet and print the product at home or a «3D printing shop» nearby. Additionally, attention has been drawn to the fact that the designs obtained can be individually changed and adapted to the customers' needs.[4] Rather than having to use a ready-made

1 There are reports that the National Aeronautics and Space Agency (NASA) and the European Space Agency (ESA) are developing plans for building a lunar station on the surface of the moon by using 3D printers, http://arstechnica.com/science/2013/03/giant-nasa-spider-robots-could-3d-print-lunar-base/ <last accessed 05.03.2013>

2 («Print me a Stradivarius-How a new manufacturing technology will change the world,» 2011) («Three-dimensional printing from digital designs,» 2011)

3 Indeed the logistic company DHL has held a congress relating to this issue. 3D printing could seriously jeopardise the company's business model when goods do not need to be shipped anymore but could instead be printed in the vicinity of where there are needed; («Three-dimensional printing from digital designs,» 2011)

4 («Three-dimensional printing from digital designs,» 2011)

product consumers could individualise the products.[5] Eventually, the dichotomy between producer and consumer could whittle away and would mark the inception of a *prosumer* society.[6]

Initially, 3D printers were used by manufacturing companies. The price to acquire a 3D printer was out of the reach for the general public. But recently the prices have decreased which made 3D printers more widely available for the general public. However, wider availability gives also rise to concerns. There have been reports that 3D printing can be used to produce parts for «home-made» hand guns.[7]

3D printing is a field of technology that is rapidly developing and may give an innovative boost as it may propel the pace in which ideas materialise into final products.[8] Yet the possible ramifications for IP remain to be analysed more thoroughly. This paper wishes to discuss the issues surrounding the distribution of 3D printing templates over the internet as they relate to the law of patents. It is structured into 4 parts including this introduction: Part 2 will provide a short overview of how 3D printing has developed over the years and how it is conducted in practice. Part 3 will highlight how indirect patent infringement is assessed *de lege lata*. The analysis is provided with reference to the laws of Germany and the United Kingdom as two major patent jurisdictions in Europe. It will focus in particular on how indirect infringement of patent rights is structured and against which acts this liability rule provides protection. Part 4 will discuss which implications 3D printing may have on all parties concerned and whether there is a gap in protection which might need to be addressed by the legislator. The article then concludes.

2. 3D PRINTING

2.1. Development

3D printing has initially been used for «rapid prototyping»[9] rather than for end products. Especially, the automobile and aerospace industry applied this technology

5 This YouTube video demonstrates how a pair of shoes provided by a 3D printing file can be individualised by the consumer and printed using a 3D printer; http://www.youtube.com/watch?v=CP1oBwccARY&list=UUgKadKkzK-Ea_YnogNKtOlA&index=8 <last accessed 02.03.2013>

6 (Ratto & Ree, 2012)

7 http://www.forbes.com/sites/andygreenberg/2012/08/23/wiki-weapon-project-aims-to-create-a-gun-anyone-can-3d-print-at-home/ < last accessed 22.01.2013>; BBC video: http://www.bbc.co.uk/news/world-us-canada-21639015 <last accessed 03.03.2013>

8 («Three-dimensional printing from digital designs,» 2011)

9 (Ratto & Ree, 2012); («Print me a Stradivarius-How a new manufacturing technology will change the world,» 2011)

to construct prototypes.[10] This was beneficial as a prototype of the end product could swiftly and cheaply be produced and tested for its aptitude before putting resources into manufacturing the end product.[11] Nowadays however more than 20% of items printed from a 3 D printer are end products and it has been said that this number may increase to 50 % by the year 2020.[12]

Many 3D printers work by using an additive method.[13] This method can be undertaken in two ways: Either plastic is burned and then put into position by a printer head or powder is burnt together with a laser.[14] The materials now suitable for 3D printing are plastic, metal and resin.[15] This range already allows many objects to be produced by using 3D printing technology.[16] However, the application of 3D printing and the range of material which can be used are expanding. This may lead to more complex and functional objects suited to be reproduced by 3D printers.[17]

The implications of this new development are not totally visible yet. It has been said that the inception of 3D printing may change the way of how economies of scale operate. The traditional way of manufacture that is based on cutting shapes out of a material left a lot of waste. This could be dramatically decreased through 3D printing. Additionally, the pace of ideas being materialised into a tangible product could be decreased. It has for example been said that the time from concept to final product could drop «by as much as 50-80%.»[18]

But 3D printing may be become more interesting for average consumers as the prices for 3D printers have decreased over the last years. The RepRap project[19] brought a 3D printer to life that was affordable to the wider public and had the advantage that it could reproduce large amounts of its parts itself. Based on the RepRap technology, MakerBot Industries have started their business in 3D printers and is currently selling 3D printers for $2,199.[20] Models such as the «Cube» are available from $ 1,399

10 («Print me a Stradivarius-How a new manufacturing technology will change the world,» 2011)

11 («Three-dimensional printing from digital designs,» 2011)

12 («Three-dimensional printing from digital designs,» 2011)

13 (Ratto & Ree, 2012)

14 («Three-dimensional printing from digital designs,» 2011)

15 («Print me a Stradivarius-How a new manufacturing technology will change the world,» 2011)

16 The Economist lists that medical implants, jewellery, football boots designed for individual feet, lampshades, racing-car parts, solid-state batteries, customised mobile phones and even making mechanical devices are already being produced by 3D printers, («Three-dimensional printing from digital designs,» 2011)

17 On Bio-Printers and other applications in the field of medicine see: (Jewell, 2013, pp. 4-5)

18 («Three-dimensional printing from digital designs,» 2011)

19 http://reprap.org <last accessed 03.03.2013>

20 http://store.makerbot.com/replicator2.html <last accessed 03.02.2013>

onwards.[21] But even the big players in the field have shown interest in producing affordable 3D printers: HP, for example, have also started to engage into 3D printing.[22]

2.2. From product to replica

As mentioned before 3D printing was initially used to generate prototypes of products. The product designer would use a computer to digitally produce the shape on a computer with the help of Computer Animated Design (CAD) software.[23]

However products that are already available can be scanned with the help of a 3D scanner.[24] This scan file is able to instruct the programme of a 3D printer to print an identical replica of the scanned object in plastic, metal or resin. Such a file in digital format could be uploaded and made available on a website and distributed.[25] From this website other internet users may download this template, blueprint[26] or 3DPDF[27] which he or she may use to instruct a 3D printer to print, and therefore replicate an object.

The question therefore is whether the person who distributes such a 3DPDF that covers an object protected by a patent could be liable of patent infringement. This is a relevant issue as there are websites that allow internet users to upload and download such 3DPDF like www.thingiverse.com, www.kraftwurx.com or www.shapeways.com.

3. 3D PRINTING AND PATENT LAW

3.1. Introduction

Intuitively, one would imagine that the IP issues raised by 3D printing would concern areas such as copyright or designs. These rights could be impaired by the fact that the copy produced by the printer may constitute an IP infringement. Such an effect on patents is not that obvious as one tends to relate these rights to the functional aspects of an object.

---

21 http://cubify.com/ <last accessed 07.02.2013>

22 http://www8.hp.com/uk/en/hp-news/press-release.html?id=462891&jumpid=reg_r1002_uken_c-001_title_r0002 <last accessed 03.03.2013>

23 (Weinberg, 2010, p. 3)

24 (Weinberg, 2010, p. 3)

25 (Jewell, 2013, p. 6)

26 (Weinberg, 2010, p. 2)

27 Bradshaw et al are using this term for the file that contains the 3D scan of the original template. (Bradshaw, S., Bowyer, A., Haufe, 2010, p. 24). This term will be used henceforth.

However, the functional aspect of a patented object could also be replicated by a copy made by a 3D printer. In this respect *Bradshaw et al*[28] refer to the *Haberman* patent[29] that covered a feeder cup for infants and stipulate that the invention could be replicated by a 3D printer. Similarly, the *Croc* shoe has been awarded patent protection in the United States.[30] Such an object and its function could be replicated by a 3D printer, especially if one has in mind the current pace of how 3D printing technology is developing. Therefore, 3D printing does have the potential to affect patent rights and will become more and more relevant for this field of IP law.

A direct infringement of the patent could not be committed by just making a scan of the patented object and making that file available on the internet. A product patent is directly infringed where someone «makes, disposes of, offers to dispose of, uses or imports the product or keeps it whether for disposal or otherwise».[31] This could mean that the person printing a patented product with a 3D printer could possibly be liable for direct patent infringement as he or she thereby «makes» a replica.[32] The recent developments of 3D printers being available for home use may often have the effect that direct patent infringement may not be actionable[33] as the use may fall under a private and non-commercial use exception.[34] This paper however focusses on the aspect where a patented product is scanned and this 3DPDF is made available on a website where internet user can download it and eventually print that product. The question therefore lies on whether the person making the 3DPDF available on the internet would commit an indirect infringement of a patented product.

3.2. Patent law in Europe

In comparison to other fields of intellectual property a unitary patent law does not exist as such in the European Union. The European Parliament however has recently adopted the so-called unitary patent package which includes regulations and an agreement on a common court system.[35]

---

28 (Bradshaw, S., Bowyer, A., Haufe, P., 2010, p. 26)

29 The «Anyway-Up Cup» was granted patent protection in the United Kingdom. This patent was subject of a patent case before the High Court of England and Wales and was held to be valid by the late Justice Laddie; (Haberman v Jackel [1999] FSR 683)

30 US Patent 6.993.858

31 See: Section 60 (1) (a) UK Patents Act 1977. A similar wording can be found in § 9 Nr. 1 of the German Patent Act.

32 (Bradshaw, S., Bowyer, A., Haufe, P., 2010, p. 27)

33 (Bradshaw, S., Bowyer, A., Haufe, P., 2010, p. 27)

34 Section 60 (5)(a) UK Patents Act 1977, § 11 Nr. 1 German Patent Act

35 http://www.europarl.europa.eu/news/en/pressroom/content/20121210IPR04506/html/Parliament-approves-EU-unitary-patent-rules <last accessed 02.03.2013>

Some harmonisation of substantial patent law provisions has already been achieved within the European Union. The European Patent Convention (EPC) provided a template for the Member States of the European Patent Organisation for national legislators, apart from setting out a substantive law for the European Patent Office to process and administer patent applications.

The EPC however just provided for substantive provisions in relation to search, examination and grant of patent applications. Post-grant provisions relating to infringement and exceptions to patent infringement were not included in the EPC-tasking. Some significant approximation of national laws in relation to such post-grant matters was provided by the Community Patent Convention (CPC) which was conceived at the Luxembourg Conference in 1975. The Convention aimed at providing a unitary patent right throughout the then European Communities (EC).[36] The Convention was never enacted due to failure of some EC member states to ratify it.

The CPC's provisions relating to infringement and exceptions provided a template which member states transposed into their national patent legislation.[37] The provisions of infringement in the United Kingdom and Germany therefore resemble each other to a great extent.[38] Even though there is resemblance in wording and application national courts have interpreted and applied the rules relating to patent infringement differently over the years despite their common origin.[39]

3.3. Rationale of indirect patent infringement

Legislators have provided for provisions against indirect infringement in order to facilitate the enforcement of patents by right holders.[40] Whereas it is often difficult and expensive to track every individual direct infringer, having a remedy against the supplier

36 Article 2 (2) CPC 1975

37 See: Resolution on the Adjustment of National Patent Law, (Records of the Luxembourg Conference on the Community patent, 1975, p. 332)

38 Furthermore, the provisions were deemed to have the same effect to their «sister provisions» in other member states. The British legislator manifested that provisions relating to infringement and exceptions thereof «*are so framed as to have, as nearly as practicable, the same effect in the United Kingdom as the corresponding provisions of the European Patent Convention, The Community Patent Convention and the Patent Co-operation Treaty have in territories to which those conventions apply*», Section 130 (7) UK Patents Act 1977

39 The well-known Epilady cases highlight this problem. National Courts of 5 EPC Member States held the patent as being infringed, whereas the courts of 4 EPC Member States came to the opposite conclusion

40 (Benkard, 2006, §10 [2]), (Kraßer, 2009, pp. 807-808)

for the direct infringer as the «spider in the web» can become an advantage.[41] Provisions against indirect infringement are meant to prevent direct patent infringement before it can occur.[42] It is linked to direct patent infringement in the sense that it aims at restricting uses of the patented invention that would constitute a direct infringement.[43]

3.4. The law of indirect patent infringement in the United Kingdom and Germany

In comparison to the law of direct patent infringement the Agreement on Trade-Related Aspects of Intellectual Property (TRIPS) has not provided for provisions for indirect infringement. The laws of the United Kingdom and Germany have modelled their provisions on indirect infringement on Article 30 of the CPC 1975.[44]

Article 30 CPC 1975: *Prohibition of indirect use of the invention*

1. A Community patent shall also confer on its proprietor the right to prevent all third parties not having his consent from supplying or offering to supply within the territories of the Contracting States a person, other than a party entitled to exploit the patented invention, with means, relating to an essential element of that invention, for putting it into effect therein, when the third party knows, or it is obvious in the circumstances, that these means are suitable and intended for putting that invention into effect.
2. Paragraph 1 shall not apply when the means are staple commercial products, except when the third party induces the person supplied to commit acts prohibited by Article 25.
3. Persons performing the acts referred to in Article 27 (a) to (c) shall not be considered to be parties entitled to exploit the invention within the meaning of paragraph 1.

This provision has been incorporated into the UK Patents Act 1977 in Section 60 (2), (3) and (6). The German legislator has transposed Article 30 CPC 1975 within § 10 of the German Patent Act. It is noted that the wording in both provisions in the United Kingdom and Germany are not identical but very similar to the provision in the CPC.

Importantly, an indirect infringement can be committed even where there has been no direct infringement resulting from the offering and supply of means relating to an

41 (Kraßer, 2009, pp. 807, 808). This is in contrast to the old law before the implementation of the CPC rules where indirect infringement required a direct infringement to have occurred.

42 BGH GRUR 2004, 758 – *Flügelradzähler*

43 (Benkard, 2006, § 10 [2])

44 This provision corresponds to Article 26 of the Community Patent Convention 1989.

essential element of the invention.[45] This is also the case in the United Kingdom.[46] Under the former German law contributory infringement was seen as a participation in an infringement which therefore required for a direct infringement to have occurred.[47]

3.4.1. Supply or offering to supply

The alleged infringer must supply or offer to supply the means relating to an essential element of the invention. The wording supply stipulates a transfer of the means to a third party.[48] The wording of the provisions of indirect infringement could actually «cover the supply of a product which is not itself the subject of a patent but which is so designed as to be used in a patented method».[49]

3.4.2. Means relating to an essential element of that invention

Second, the infringer's supply or the offer to supply must relate to means relating to an essential element of the invention. It has been said that the term would stipulate that the legislator meant to imply that means are of tangible and physical nature and applied to put the function of the invention into effect.[50] Hence, simple and abstract instructions would normally not be considered to be means in the context of Section 60 (2) UK Patents Act 1977.[51]

In *Menashe Business Mercantile Ltd v William Hill Organization Ltd*[52] however, the Court of Appeal found that software provided on a CD or downloaded from the internet within the United Kingdom could be such means. The invention in question related to a casino game consisting of a host computer, terminal computers, communication means and a computer programme to operate the terminal computers. The users were provided with CDs containing the software or could download it from the internet which enabled them to play the game.[53] Eventually, whether the element which is being supplied or offered to supply is indeed essential will depend on the facts of the case.[54]

---

45 BGH GRUR 2001, 228 – *Luftheizgerät*; (Benkard, 2006, § 10 [3]); (Kraßer, 2009, p. 805)

46 (Chartered Institute of Patent Attorneys (CIPA), 2011, [60.09])

47 (Harguth & Carlson, 2011, p. 190)

48 (Miller et al., 2010, [14-55])

49 (Cook, 2011, p. 265)

50 (Chartered Institute of Patent Attorneys (CIPA), 2011, [60.09])

51 (Roughton et al, 2010, [6.56])

52 *Menashe Business Mercantile Ltd v William Hill Organization Ltd* [2003] R.P.C. 31

53 *Menashe Business Mercantile Ltd v William Hill Organization Ltd* [2002] R.P.C. 47, [2] (EWHC)

54 (Miller et al., 2010, [14-56])

Looking at Germany, the German Federal High Court has held that means are objects of physical nature which are applied to conduct a direct infringement according to § 9 of the German Patent Act.[55] Instructions on how to produce the patented product are not such means.[56] *Benkard* however refers to a decision by the Regional Court of Düsseldorf that stipulates that even digitally processed data may be regarded as the object of an indirect infringement.[57] Whether the means are essential is based on whether such elements assist in putting the protected invention in effect.[58]

3.4.3. To put the invention into effect

The means must enable a third party to put the invention into effect. The Court of Appeal of England and Wales gave some guidance of what was meant thereby: It held that putting the invention into effect equated to putting it into an infringing state in the meaning of Section 60 (1) UK Patents Act 1977.[59]

The German term with this regard relates to the fact that the means provided or offered enable the use of the invention («*zur Benutzung der Erfindung*»). This stipulates that such use of the patented invention would constitute a direct infringement under § 9 Nr.1 – Nr. 3 of the German Patent Act[60] and falls within its scope of protection as provided by the patent claims.[61] This assessment resembles very much the position in the United Kingdom.

Importantly, it has to be noted that the means only have to *enable* the recipient of the means to put the invention into effect, i.e. in an infringing state. It is not necessary that the recipient actually does so. As mentioned above, indirect infringement does not require a direct infringement to take place.

3.4.4. The territoriality aspect

Only actions committed within the jurisdictions in question will be sanctionable as indirect patent infringement. By this, the offer to supply or the supply of means for putting the invention into effect must emanate from within Germany[62] or the United Kingdom.[63]

---

55 BGH GRUR 2001, 228, 231 – *Luftheizgerät*

56 (Benkard, 2006) § 10 [4]; (Kraßer, 2009, p. 808). *Mes* however considers «instructions, written techincal preparations, modells and drawings« as being able to be means, (Mes, 2011, § 10 [11])

57 (Benkard, 2006, § 10 [4])

58 (Kraßer, 2009, p. 809)

59 *Menashe Business Mercantile Ltd v William Hill Organization Ltd* [2003] R.P.C. 31, [24], [27]

60 (Benkard, 2006, § 10 [2])

61 (Kraßer, 2009, p. 809)

62 (Benkard, 2006, § 10 [14])

63 The Court of Appeal held that the invention must be suitable and intended to put into effect in the United Kingdom and by this, in an infringing state. Some other form of effect did not

An offer to supply or a supply made from abroad and addressed to customers in Germany however does fulfil this criterion.[64] Patents are territorial rights and therefore the provisions against indirect infringement wish to prevent that an invention that is protected within its territory can be infringed directly.

3.4.5. Knowledge

Finally, the alleged infringer must have actual or constructive knowledge of the fact that the means are suitable and intended to put the invention into effect.[65] Therefore, sheer knowledge that means are suitable for this purpose does not suffice. He or she must know that they are intended to be used in the mentioned way. Importantly, the alleged infringer must not have actual knowledge that the means he or she is offering or is offering to supply are actually protected by a patent. The knowledge can however be derived from the given circumstances and is closely related to the facts of the case. Such knowledge, for instance, can be given where the means supplied can only be used in an infringing way by the third party.[66]

Apart from proving positive knowledge, an indirect infringement can also be found where it is obvious to a reasonable person that the means would be used in an infringing way in the given circumstances. This means that there should not be reasonable doubts as to the suitability and purpose of the means to be used to put the invention into effect.[67] This provision facilitates filing for indirect infringement as it is otherwise difficult to prove that the alleged infringer had actual knowledge.[68]

3.4.6. Parties not entitled to exploit the patent

There is no indirect infringement of a patent according to § 10 of the German Patent Act where the offer or the supply is being made to authorised persons («berechtigte Personen»). This corresponds to a «licensee or other person entitled to work the invention» within Section 60 (2) UK Patents Act 1977.

Both pieces of legislation[69] provide that such authorised persons are not those persons to which an exception (§ 11 Nr 1 – Nr 3 of the German Patent or Section 60 (5)

---

suffice that the effects were just felt in the United Kingdom. See: *Menashe Business Mercantile Ltd v William Hill Organization Ltd* [2003] R.P.C. 31, [29].

64 (Kraßer, 2009, p. 810)

65 (Roughton et al, 2010, [6.49])

66 (Benkard, 2006, § 10 [19])

67 (Benkard, 2006, § 10 [20])

68 BGH GRUR 2001, 228, 231 – *Luftheizgerät;* (Harguth & Carlson, 2011, p. 191)

69 § 10 (3) German Patent Act, Section 60 (6) UK Patents Act 1977

(a), (b) and (c) UK Patents Act 1977) applies to. This means that an indirect infringement cannot be avoided by the fact that the use of the person who the means have been offered or supplied to is excused from otherwise having committed a direct infringement due to private and non-commercial use or experimental use of the patented invention.

3.4.7. Staple goods

An indirect infringement is not given where the means offered or supplied are staple goods.[70] These are considered to be products which are for every days needs and are generally obtainable.[71]

4. IMPLICATIONS FOR 3D PRINTING

Having outlined how indirect infringement is structured the question then arises under what conditions the person making a 3DPDF available on a website could be found liable. Importantly, this question needs to be separated into two different scenarios depending on the way the patentee intended the patented object to be manufactured:

- Where the patented object is produced by a different means than with 3D printing i.e. by traditional ways of manufacture then the issue arises whether a 3DPDF developed by a 3D scanner of the patented object, made available on the internet and applied to reproduce that object by a 3D printer would be considered as indirect infringement.
- In the other scenario, the patented object was originally designed by applying CAD software and intended to be manufactured by 3D printers.

The differentiation is important as a 3DPDF is an essential ingredient when the manufacture is done with the help of 3D printers. This is however not the case where manufacture is done by conventional manufacture and the 3D printing is just an alternative way of producing the patented object. In this scenario the 3DPDF serves as a sort of template.

4.1. Supply or offering to supply

Based on the wording it appears that providing a 3DPDF on a website from which internet user could download it would be considered as an «offering for supply». An interpretation of the wording does not seem to be limited to an offer of tangible objects.[72]

---

70 Section 60 (3) UK Patents Act 1977, § 10 (2) German Patent Act

71 (Chartered Institute of Patent Attorneys (CIPA), 2011, [60.01])

72 (Keukenschrijver, 2013, § 10 [15])

Additionally, in *Menashe Business Mercantile Ltd v William Hill Organization Ltd,* the Court of Appeal based its positive finding of indirect infringement on the fact that the defendant had provided the software which was used in the patented invention on a CD.[73] The court however indirectly implied that indirect infringement could also be found when users are able to download the software.[74]

Additionally, a teleological interpretation seems to be in favour of such an interpretation. With broadband internet connections being widely available the economic reality nowadays is such that digital contents can be obtained and downloaded swiftly over the internet. It appears that the legislator would have intended the provision to cover internet commerce and distribution. It therefore can be said that making a 3DPDF available on the internet could be found as an «offer to supply».

4.2. Means relating to an essential element to put the invention into effect

This provision seems to be quite straightforward in relation to patented objects originally manufactured with a 3D printer. Then, the 3DPDF containing the printing template or a 3DPDF that derived from a 3D scan which creates a printing template is essential for creating the patented object and are arguably a «means relating to an essential element». Additionally, they serve to put the invention into effect. This is its primary purpose and was the way the original inventor intended to manufacture the object. This would normally also fall within the scope of protection as outlined by the patent claims.[75] Therefore, a 3DPDF, even one derived from a 3D scan, is used to «put the invention into effect».

Whether a 3DPFP derived from a 3D scan of the patented object is a means relating to an essential element to put the invention into effect where the patented product is manufactured traditionally is however not as straightforward. Here a 3DPDF is not necessarily part of the manufacturing process.

The case law which is discussed above additionally still seems to require the means to be tangible.[76] The Court of Appeal however generally seems to allow means to be of

---

73 *Menashe Business Mercantile Ltd v William Hill Organization Ltd* [2003] R.P.C. 31, [6]

74 The Court of Appeal mentioned that the users of the software would have «usually» been provided on a CD, (ibid [6]). The first instance decision specifically mentions that the users were able to download the software, *Menashe Business Mercantile Ltd v William Hill Organization Ltd* [2002] R.P.C. 47, [2] (EWHC). The wording of the Court of Appeal decision therefore stipulates that the court held that downloading the software and the defendant then making this software available to download would constitute an indirect infringement.

75 Article 69 (1) EPC

76 See above 3.4.2

intangible nature.[77] Additionally, regarding a literal interpretation, neither the German term *«Mittel»* nor the English term «means» necessarily indicate that the means need to be of tangible nature which could make 3DPDF to be considered as means.

It is however difficult to assess whether the 3DPDF created from a 3D scan could also be considered to be an essential element of the invention. It provides a digital representation of a physical part.[78] So it could be argued that it just provides an instruction on how to make the product.[79] A similar argument has been made in relation to the equivalent provision in the Patent Act of the United States which speaks of components.[80] If one follows this line of argument instructions cannot constitute «means to put the invention into effect.»[81]

It could however be said that a 3DPDF would enable the user of a 3D printer to put the invention into effect. Lord Aldous has stated that «to put, the invention into effect» must require the means to be intended to put the apparatus claimed into effect: thereby requiring the claimed apparatus to become effective.[82] It therefore seems to depend on what the invention claims and whether this can be replicated by a 3D printer. Then a 3DPDF would suffice for the user to «make» the invention. This would constitute a direct infringement in accordance with Sec 60 (1) (a) UK Patents Act 1977. The replica produced could therefore fall within the scope of protection of the patent as the law of indirect infringement requires *de lege lata*.

Eventually, it remains doubtful whether an indirect infringement could currently be committed in this scenario. It could however be argued that making a 3DPDF available on the internet after the digitisation of the original object by a 3D scanner should not fall outside the scope of indirect infringement where the replica printed constitutes a direct infringement. This, in particular, when one considers the *ratio legis* of provisions against indirect infringement as serving to prevent direct infringement. 3DPDFs are essential for putting the invention into effect when using a 3D printer. However, this issue could potentially constitute a loophole in patent protection and requires to be clarified by the courts.

---

77 See above 3.4.2

78 (Thornewell II, 2004, p. 2834)

79 (Thornewell II, 2004, pp. 2834, 2835)

80 (Thornewell II, 2004, pp. 2836-2837). The argument that software as such is patentable according to the Supreme Court (Diamond v. Diehr, 450 U.S. 175(1981)) and should therefore should be treated as a component (William R. Thornewell II, 2004, p. 2838), cannot be transposed into European patent law as software «as such» is excluded from patent protection, Article 52 (2) (c), (3) EPC.

81 See above 3.4.2

82 *Menashe Business Mercantile Ltd v William Hill Organization Ltd* [2003] R.P.C. 31, [24]

4.3. The territoriality aspect

Based on the current law there will probably not constitute a significant problem with applying the territoriality rules of indirect infringement to the scenarios analysed. If the file, that has been accessed, downloaded and used in Germany or the UK as a 3D printing template to print the object then the patented invention has been supplied for use in the territories of the jurisdictions in question. Through this, the invention would have been put into effect.

The fact that the 3DPDF may be emanating from a server which is not based within the United Kingdom or Germany does not set a hurdle for finding that its offer over the internet could have been made to users situated in these jurisdictions.[83] As the file would be available on the internet which can practically be accessed from everywhere in the world the offer to supply or the supply for using them in computer terminals as printing templates could still be regarded as an offer or a supply to users in the United Kingdom[84] or Germany.[85]

4.4. Knowledge

Finally, finding that the alleged infringer had knowledge relating to whether the means were suitable and intended could present an obstacle. Where the patented object is manufactured by using 3D technology and is manufactured by using a 3DPDF it could be argued that the alleged infringer had constructive knowledge when he makes such a file available on the internet. Alternatively, right holders may argue that it would have been obvious to a reasonable person that the 3DPDF would be suitable and intended to put the invention into effect.

The issue could be different where 3D printing is not part of the manufacture of the patented object. Finding that the alleged infringer had constructive knowledge could be difficult for the patentee to prove. It would also be difficult to bring forward that it would be obvious to a reasonable person that the 3DPDF would be suitable and intended to be used in an infringing way by the person downloading that file. The template could be altered in shape and therefore also be put to function by the user of

83 See above 3.4.4

84 In relation to the fact that the host computer has been based abroad the Court of Appeal held in its *Menashe* decision that: «[it] is of no relevance to him, the user, nor the patentee as to whether or not it is situated in the United Kingdom.»: *Menashe Business Mercantile Ltd v William Hill Organization Ltd* [2003] R.P.C. 31, [32].

85 *Keukenschrijver* stipulates that the reasoning of the Court of Appeal in *Menashe* can be applied to the scenario in Germany, (Haupt, 2007, p. 190)

the 3D printer.[86] This could render the reproduced product to fall out of the scope of protection. The question therefore is whether this fact may alter the knowledge of the alleged indirect infringer. This is already difficult to prove in ordinary indirect infringement cases and relies heavily on the facts of the case. Therefore, clarification by courts is imperative to provide a clearer picture.

4.5. Staple Goods

Finally, a 3DPDF would most probably not be considered a staple good. This may be the case for the computer and the 3D printer used or may also apply to the compound the replica is made of.[87] A 3DPDF does not appear to be a widely obtainable product for every days use as stipulated by the relevant provisions.

5. CONCLUSIONS

3D printing is a developing technology and its impact on our societies has yet to be seen. Bearing all the possibilities in mind that 3D printing may entail it is not surprising that this would constitute «the next industrial revolution.»[88]

The cover of *The Economist* from 10th of February 2011 showed a violin which was made by a 3D printer as a sample of what is already possible.[89] The lead article on the topic of 3D printing has questions whether mass 3D printing requires for intellectual property laws to adapt to it.

IP right holders could fear that this technology may lead to mass appropriating of their IP rights. This may possibly lead to a decrease in providing incentives to businesses engaged in research and development.[90] The law of indirect infringement however has the potential to address the concerns that patent holders may have with this regards. Courts however need to clarify the arising issues and ambiguities that are still left with regards to this technology.

Therefore, it may be useful to draw analogies from copyright law. 3D printing finally places digitisation and the distribution over the internet fully into the realm of patent law. Copyright law has had to address issues relating to the digitisation of protected works and mass copying thereof for quite some time now.[91] It would be useful to display

86 («Print me a Stradivarius-How a new manufacturing technology will change the world,» 2011)

87 (Weinberg, 2010, p. 14)

88 («Three-dimensional printing from digital designs,» 2011)

89 («Print me a Stradivarius-How a new manufacturing technology will change the world,» 2011)

90 (Sissons & Thompson, 2012, p. 23)

91 (Graznak, 1998, p. 58), http://www.smh.com.au/technology/technology-news/3d-printing-could-herald-new-industrial-revolution-20130429-2ingp.html <last accessed 30.04.2013>

how copyright law responded to these issues which may serve as a template for the issues 3D printing may bring in relation to patent law.

There is however a common fear that intellectual property rights could interfere with this development and stifle innovation in the field of 3D printing. The *Economist* article stipulates that tightening legal norms would stifle innovation whereas conversely a more lenient application of IP rules would lead to more piracy.[92] What is imperative is that policy makers respond diligently and with foresight to this new development.[93] Lessons learned from copyright law in relation to digitisation must be taken into account.

6. BIBLIOGRAPHY

Benkard, G. (Ed.). (2006). *Patentgesetz, (10th ed.).* Munich: C.H. Beck Verlag.

Bradshaw, S., Bowyer, A., Haufe, P. (2010). The Intellectual Property implications of low-cost 3D printing. *ScriptEd*, *7*, 5–31. doi:10.2966/scrip.

Chartered Institute of Patent Attorneys (CIPA). (2011). *CIPA Guide to the Patents Acts (ed.).* London: Sweet & Maxwell.

Cook, T. (2011). *A User's Guide to Patents, (3rd ed.).* Haywards Heath: Bloomsbury Professional.

Graznak, P. (1998). From Atoms to Bits and Back: DVD Technology and Copyrighted Content. *Entertainment Law Review*, *77*(1), 76–85.

Harguth, A., & Carlson, S. (2011). *Patents in Germany and Europe. Procurement, Enforcement and Defense. An International Handbook.* Alphen aan den Rijn :Wolter Kluwer.

Haupt, I. (2007). Territorialitätsprinzip im Patent- und Gebrauchsmusterrecht bei grenzüberschreitenden Fallgestaltungen. *GRUR*, *109*(3), 187–195.

Jewell, C. (2013). 3-D Printing and the future of stuff. *WIPO Magazine*, (2), 2-6.

Keukenschrijver, A. (Ed.). (2013). *Busse: Patentgesetz, (7th ed.)*. Berlin, Boston: De Gruyter

Kraßer, R. (2009). *Patentrecht (6th ed.).* Munich: C.H. Beck.

Mes, P. (2011). *Patentgesetz Gebrauchsmustergesetz - Kommentar (3rd ed.).* Munich: C.H. Beck.

Miller, R., Burkill, G., Birss, C., & Campbell, D. (2010). *Terrell on Patents (17th ed.)* London: Sweet & Maxwell.

92 («Print me a Stradivarius-How a new manufacturing technology will change the world,» 2011)

93 (Jewell, 2013, p. 6)

Office for Official Publications of the European Communities (1982). *Records of the Luxembourg Conference on the Community patent 1975*. Luxembourg

Print me a Stradivarius-How a new manufacturing technology will change the world. (2011, February 11). *The Economist*.

Ratto, M., & Ree, R. (2012). Materializing information : 3D printing and social change. *First Monday [Online]*. Volume 17 Number 7 (27). Retrieved 07.02.2013 from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3968/3273

Roughton, A., Johnson, P., & Cook, T. (eds.) (2010). *The Modern Law of Patents (2nd ed.).* London: Lexis Nexis.

Sissons, A. & Thompson, S. (2012). Three Dimensional Policy: Why Britain needs a policy framework for 3D printing. *The Big Innovation Centre*

Three-dimensional printing from digital designs. (2011, February 11). *The Economist*.

Thornewell II. W. (2004-2005). Patent Infringement Prevention and the Advancement of Technology: Application of 35 U.S.C. § 271(f) to Software and «Virtual Components». *Fordham Law Review*, *73*(5), 2815–2856.

Weinberg, M. (2010). It will be awesome if they don't screw it up: 3D printing, intellectual property, and the fight over the next great disruptive technology. *Public Knowledge*. Retrieved from http://www.publicknowledge.org/files/docs/3DPrintingPaperPublicKnowledge.pdf

COMUNICACIONES SOBRE REGULACIÓN

REGULATION AS A MECHANISM TO ENCOURAGE COMPETITION IN THE AREA OF TELECOMMUNICATIONS: TOWARDS THE CONCEPT OF EMULATED COMPETITION

Humberto Carrasco Blanc
School of Law,
University of Edinburgh, Doctoral Research Student

ABSTRACT: Regulation has been used in the telecommunications sector at different points in time to fulfill a various market needs. Before liberalisation of telecommunications, regulation established the parameters of the state-owned telecommunications company. Later, it specified the rights and duties of the incumbent. Hypothetically speaking, a higher degree of regulation is necessary to create new competitive markets, and once progress has been made, a lesser degree of regulation is required in order to advance to ex-post regulation.

Competition law has become an indispensable component of the regulatory framework, which can act through two pathways: 1. Ex-post regulation utilizing traditional principles of competition law; 2. Ex-ante regulation that seeks to introduce competition to a market.

The second kind of regulation has been called 'regulation for competition' or 'synthetic competition'. The concept of 'emulated competition' is proposed because it explains in a more appropriate way its legal nature and its intended and unintended effects. In order to develop this concept, the mutual influence between sectoral regulation and competition law will be analysed. Furthermore, the possibility of applying competition law in situations where there is a regulated market will be studied.

The US stumbled into the liberalization of telecommunications in the 1960s - 1970s. The UK and Chile began the processes during the 1980s. The comparison, inter alia, will allow to evaluate the effectiveness of differing regulatory strategies for the telecommunications sectors after 30 years.

KEYWORDS: Regulation, Telecommunications, Competition, Synthetic Competition, Emulated Competition.

1. OVERVIEW

Regulation can have different reasons.[1] Before liberalization of telecommunications, regulation established the parameters of the state-owned telecommunications company. Later, it specified the rights and duties of the incumbent. Hypothetically speaking, a higher degree of regulation is necessary to create new competitive markets and once progress has been made, a lesser degree of regulation is required in order to advance to ex-post regulation.[2]

1 Baldwin & Cave, 1999, p. 9.

2 InfoDev-ITU & ICT regulation toolkit, 2012a.

Deregulation is closely tied to this process. Although it is related to the idea of undoing or reversing something, there is no clear understanding of deregulation[3] and its outcome has been questioned.[4] The idea of re-regulation seems to be a better proposition since there is a reformulation of old rules and the creation of new ones.[5] Nevertheless, the concept of «regulatory capitalism» is preferred because it more adequately captures the explosion of regulation in the Neo-Liberalism era.[6]

Competition law has become an indispensable component of the regulatory framework, which can act through two pathways: 1. Ex-post regulation utilizing traditional principles of competition law; 2. Ex-ante regulation that seeks to introduce competition to a market.[7]

The second kind of regulation has been called 'regulation for competition'[8] or 'synthetic competition'.[9] I would like to propose the concept of 'emulated competition' because it explains in a more appropriate way its legal nature and its intended and unintended effects. In order to develop this concept, the mutual influence between sectoral regulation and competition law will be analysed. Furthermore, related to the previous topic, the possibility of applying competition law to a case where there is a regulated market will be analysed. The case law study will be the treatment of some abuse of dominance cases, particularly margin squeeze. There is no uniform response to this issue and some accept the joint applicability of sectoral regulation and competition law (the EU and Chile) and others reject it (the U.S.).

Following this analysis, it can be concluded that Chile appears to have its own unique model. There is a strong and mutual influence between sector-specific regulation and competition law and no tension arises between these concepts. The Chilean model is influenced by the US with its consumer welfare goal and by the EU's approach, which is focused on a blend of sectoral regulation and competition law.

The US, the EU and Chile have been chosen for comparative study in this context. The US, the EU and Chile started the process of liberalisation of the telecommunications markets early. The US essentially stumbled into the liberalization of telecommunications in the 1960s and 1970s.[10] The UK was the first country in Europe that began

3 Farris, 1981, pp. 44–50.

4 D. Levi-Faur, Jordana, & Gilardi, 2005, p. 33.

5 Vogel, 1996, p. 3.

6 D. Levi-Faur et al., 2005, p. 33.

7 Walden & Angel, 2005, p. 18.

8 David Levi-Faur, 1998, p. 667.

9 Ginsburg, 2009, p. 5.

10 Crandall, 2000, p. 417.

the liberalisation and privatisation processes during the 1980s.[11] At the same time, Chile started the same process.[12] The comparison, inter alia, will allow to evaluate the effectiveness of differing regulatory strategies for the telecommunications sectors after 30 years.

2. NEO-LIBERALISM AND COMPETITION

Neo-Liberalism is based on a deep belief in the effects of competition arising from market players. It argues that efficient markets produce three benefits: lower prices, better quality of goods and services, and a dynamic technological progress[13].

The reform process was undertaken as part of a strategy to liberalise the public services under the belief that competition would bring benefits to consumers[14]. However, the outcome of the liberalisation process has been a far-cry from its aim of drawing multiple actors into the telecommunications markets and instead large transnational service suppliers have arisen.[15] It seems to be that in the telecommunications area there has been a transition from monopoly to oligopoly rather than to real competition.[16]

3. REGULATION, SECTOR-SPECIFIC REGULATION AND COMPETITION LAW

Regulation has been defined as 'the employment of legal instruments for the implementation of social-economic policy objectives'.[17] Competition law and sector-specific regulation are parts of the general concept of regulation. These two areas have diverse goals. Whereas the objectives of competition law could be: consumer welfare, consumer protection, redistribution and protecting competitors[18]; sectoral regulation serves to foster competitive markets, prevent abuse of market power and provide a universal service.[19] However, sector-specific regulation is very closely related to com-

11 Pitt, 2005, p. 294.

12 Moguillansky, 1998, p. 7.

13 Simpson, 2008, p. 5.

14 Hall, 2002, p. 204.

15 Hermann, 2007, p. 14.

16 Collins, 2004, p. 25.

17 den Hertog, 2000, p. 223.

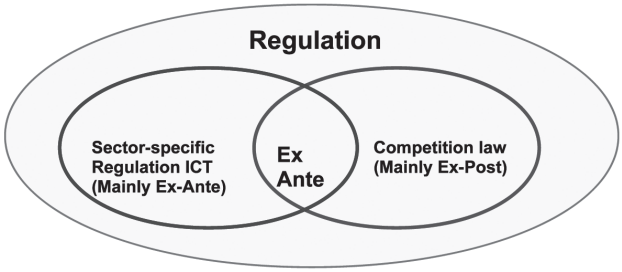
18 Whish, 2009, pp. 19–22.

19 Landgrebe, 2002, p. 5.

petition law[20] and this relationship has provoked confusion because there are no clear limits.[21]

It is important to distinguish between ex-ante and ex-post regulation at this point. Whereas ex-ante regulation involves the application of specific rules and restrictions to prevent anti-competitive activities before it occurs; ex-post regulation, calls for applying corrective measures and punishments when transgressions do occur.[22]

The following venn diagram summarizes the relationship between regulation, sector-specific regulation and competition law:



4. TELECOMMUNICATIONS MARKETS: A NATURAL MONOPOLY?

Telecommunications markets have not developed naturally from the beginning.[23] The old wisdom considered this market as a typical case of natural monopoly,[24] but this vision has been criticised.[25] Although the reasons to conceive of it as a natural monopoly are still present, the benefits gained after introducing competition appear to have undermined them.[26] After eliminating or relaxing the barriers to develop new markets, the landscape for competition in telecommunications markets was not encouraging.

5. MANIPULATION OF THE NEW TELECOMMUNICATIONS MARKETS

After opening and creating new markets, a question arises: How to develop competition in markets where there is none or almost none?

20 Landgrebe, 2002, p. 10.

21 Landgrebe, 2002, p. 11.

22 ITU-infoDev ICT Regulation Toolkit, 2012, p. 5.

23 Pitt, 2005, p. 294.

24 Fransman, 2000, p. 8.

25 Thierer, 1994, p. 267.

26 InfoDev-ITU & ICT regulation toolkit, 2012b.

It was necessary to develop competition through to public policy.[27] Among others regulatory tools, it was possible to find:

a. Interconnection.

b. Local Loop Unbundling

c. Indirect access

d Number portability

This is not the opportunity to analyse all of these tools as this task would require a separate research.

6. SYNTHETIC COMPETITION

The design and manipulation of telecommunications markets via regulation has been named «synthetic competition»[28]. The goal is to assure the participation of multiple players in the market.[29]

In synthetic competition the preferences of the regulators could be to create a multi-player market based on different reasons than competition law goals. A regulator could prefer **productive efficiency**[30] instead of **allocative efficiency** or even **dynamic efficiency**.[31]

In **allocative efficiency** 'it is usually assumed that products are being produced in the most efficient (least-cost) way.'[32] When this happens, the consumer surplus, the measure of evaluating consumer welfare,[33] is at its largest.[34] In other words, the higher the allocative efficiency, the greater the consumer welfare.

Productive efficiency refers to the production of an output 'at the lowest possible cost given the current technology.'[35]

---

27 Green & Teece, 1998, p. 624.

28 Ginsburg, 2009, p. 5.

29 Ginsburg, 2009, p. 5.

30 Ginsburg, 2009, p. 6.

31 Monti, 2008, p. 131.

32 Khemani, Shapiro, & Centre for Co-operation with European Economies in Transition, 1993, p. 65.

33 Khemani et al., 1993, p. 29.

34 Whish, 2009, p. 4.

35 Nazzini, 2011, p. 35.

Dynamic efficiency is related to the introduction of new production technology that increases productive efficiency[36].

These three efficiencies help to evaluate the social welfare in an industry.[37]

In the US antitrust law, the goal is consumer welfare or **allocative efficiency**.[38] In the EU competition law, there are diverse goals, such as economic freedom and consumer welfare[39] or, in other words, **one long-term social welfare objective**.[40]

Synthetic competition is combined with other goals, such as universal service or the development of the internal market and the promotion of citizens' interests.[41]

What kind of consequences could be derived from synthetic competition?

One effect is that a regulator's decision after imposing a regulatory measure cannot be evaluated in the same way than a competition law case.

The Supreme Court (SC) case of *Verizon v. FCC* (also called TELRIC) is a good example. The Federal Communications Commission (FCC) is required by the 47 U.S.C. § 251 (c)-(d) 1996 Telecommunication Act to mandate an incumbent local exchange carrier (ILEC) to make its network available to competitive local exchange carriers (CLEC). The FCC is the entity in charge of regulating the price at which a CLEC may lease unbundled network elements (UNEs) from the incumbent. Under 47 U.S.C. § 252 (d)-(1)(A)-(i) the price must be a just and reasonable rate based on the cost of providing the network element. The FCC established that the prices for UNEs would be fixed under the forward-looking (total element long-run incremental cost -TELRIC) rather than historical cost. The incumbents challenged this. The SC declared that 'The job of judges is to ask whether the Commission made choices reasonably within the pale of statutory possibility in deciding what and how items must be leased and the way to set rates for leasing them. The FCC's pricing and additional combination rules survive that scrutiny.'[42] There was a dissenting opinion from Justice Breyer who expressed that 'The majority nonetheless finds the Commission's pricing rules reasonable. As a regulatory theory, that conclusion might be supportable. But under this deregulatory statute,

36 Nazzini, 2011, p. 37.

37 Nazzini, 2011, p. 32.

38 Ginsburg, 2009, p. 6.

39 Lovdahl Gormsen, 2010, p. 185.

40 Nazzini, 2011, p. 391.

41 «Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive),» 2002, sec. 8.

42 Cornell University Law School, 2002, p. 69.

it is not.'[43] However, Justice Breyer's opinion 'seems to be more a ground of competition policy than of administrative law'.[44]

7. REGULATION IN TELECOMMUNICATIONS: TEMPORARY?

It has been pointed out that 'sector-specific regulation has a transitional character and is aimed at addressing and solving temporary market failures'.[45] However, 'ten years after the transitory introduction of regulation, structure-preserving behaviour, e.g., an expansion in regulatory scope and responsibility, a boost in personnel, and higher budgets for the authorities in question, can be observed'.[46]

Why does this happen?

Several reasons have arisen to recognize its permanent character.[47] However, the most relevant argument is that the telecommunications industry is progressively evolving towards an oligopoly structure.[48] Consequently, deregulation of the mandatory interconnection or LLU could play against competition instead of promoting it.[49]

8. INTERACTION BETWEEN THE SECTOR-SPECIFIC REGULATION AND COMPETITION LAW

The state has moved from a welfare state to a competition state[50] and the competition state must face a paradox: 'the greater the commitment of the competition state to the promotion of competition, the deeper its regulation will be'.[51] A complex relationship then arises between competition and regulation and between sector-specific regulation and competition law.

Indeed, if sectoral regulation has been used to open and develop markets, could competition law be used to further help in this task?

---

43 Cornell University Law School, 2002, p. 29.

44 Ginsburg, 2009, p. 9.

45 Koenig, Bartosch, & Braun, 2002, p. 64.

46 Scheld, 2007.

47 Berhin, Godart, Jolles, & Nihoul, 2005, pp. 11–18.

48 Gaffard & Krafft, 2000, p. 1.

49 Berhin et al., 2005, p. 16.

50 Cerny, 1997, p. 259.

51 David Levi-Faur, 1998, p. 676.

The answer has not been uniform. On the one hand, the US has denied the possibility of applying anti-trust law in regulated markets after *Trinko*[52] and *LinkLine*[53] cases, but on the other hand, the EU have accepted the application of competition law for regulated markets in *Deutsche Telekom*[54] *and Telefónica.*[55] In Chile, there has not been any discussion about this issue and competition law has been applied to regulated[56] and unregulated markets.[57]

Moreover, the mutual influence between sector-specific regulation and competition law has been uneven as discussed below. This research will focus mainly in the influence of sector-specific regulation on competition law because it will help to develop the concept of emulated competition and its intended and unintended effects.

9. THE INFLUENCE OF COMPETITION LAW ON SECTOR-SPECIFIC REGULATION

9.1. The US case

During the 1980s, it was clear that antitrust law intellectually dominated over industry-specific regulation.[58] The key moment was the *AT&T* case which restructured the U.S. telecommunications sector.[59] In the 1990s, the situation changed because of the strong repercussion of the theories of market failure predicated on network effects over FCC and the antitrust division, which moved the balance to sectoral regulation.[60] The loss of influence of antitrust law on sectoral regulation was confirmed after *Trinko*[61] and *LinkLine*[62] cases during the 2000s.

52 Cornell University Law School, 2004.

53 US Supreme Court, 2009.

54 Infocuria, 2010.

55 Infocuria, 2012.

56 Supreme Court of Chile, 2010.

57 Supreme Court of Chile, 2007.

58 Geradin & Sidak, 2005, p. 8.

59 Alden, 2002, p. 5.

60 Geradin & Sidak, 2005, p. 8.

61 Cornell University Law School, 2004.

62 US Supreme Court, 2009.

9.2. The EU case

It has been highlighted that 'The success of competition policy in the liberalisation of the telecom sector was mainly due to a carefully designed inter-institutional process...'[63] Furthermore, the 'long-term plan is to have a legal framework using only competition law ex post regulation.'[64]

There are many examples of the influence of competition law on European sector-specific regulation, such as markets definitions[65] and recommendations and commission guidelines.[66] However, the main focus of this research will be on the concept of 'Significant Market Power' (SMP) because its importance is reflected in the fact that the 2002 regulatory reform has been called the SMP regime.[67] Special ex-ante obligations may be imposed on telecommunication companies considered by national regulatory authorities to have SMP. Article 14 paragraph 2 of the Framework Directive regulates this situation. It says 'An undertaking shall be deemed to have significant market power if, either individually or jointly with others, it enjoys ***a position equivalent to dominance***,..'.

This phrase might suggest that SMP and dominance are the same. However, although it is true that the concept of SMP is applied by reference to the European Court of Justice's definition of dominance,[68] the resemblance is not absolute because:

a. The way of evaluating SMP is different from the way of evaluating dominance. SMP evaluation is an ex-ante analysis whereas dominance is an ex-post appraisal.[69]

b. The application of competition law principles in sector-specific regulation could have different outcomes between the regulator and the competition authority. This was illustrated in the margin squeeze Telefónica case[70] where it was declared by the Commission that regulators can apply ex ante analysis, but cannot entirely eliminate the risk of anti-competitive behaviour.[71]

---

63 Ungerer, 2001, p. 18.

64 Temple Lang, 2009, p. 34.

65 De Muyter & Verheyden, 2010, p. 2.

66 «Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive),» 2002, sec. 27; Geradin & Sidak, 2005, p. 19.

67 de Streel, 2003, p. 489.

68 Hausman & Sidak, 2007, p. 388; Temple Lang, 2009, p. 44.

69 European Commission, 2002, para. 70.

70 Commission of the European Communities, 2007.

71 European Commission, 2007.

10. THE INFLUENCE OF SECTOR-SPECIFIC REGULATION ON COMPETITION LAW

10.1. The case of the US

In relation to network industries dominated by an ***unregulated monopolist***, it has been said that 'In short, the Verizon case concerning TELRIC pricing will likely influence the shape of antitrust remedies in product integration cases.'[72] Nevertheless, there is no obligation in a competition law case to follow this method because a court analyses historical data and the method to be applied may be different after the assessment.

In a ***regulated market***, the situation is different. The SC held in *Trinko* that in the existence of a regulatory structure, 'the additional benefit to competition provided by antitrust enforcement will tend to be small…'[73] Nevertheless, the Court did not categorically deny the possibility of applying competition law in addition to sector-specific regulation.[74]

10.2. The case of the EU

10.2.1. The principle of equality of opportunities

This principle developed under ex-ante regulation case law[75] has been applied in ex-post competition law cases. In these ex-ante cases 'a system of undistorted competition, as laid down in the Treaty, can be guaranteed only if ***equality of opportunity*** is secured as between the various economic operators'.[76] The principle was used for the first time in a pure ex-post/competition law case [77] in *Deutsche Telekom*.[78]

The Court of First Instance declared that equality of opportunity 'means that prices for access services must be set at a level which places competitors on an equal footing with the incumbent operator as regards the provision of call services...'[79]

72 Geradin & Sidak, 2005, p. 11.

73 Cornell University Law School, 2004, p. 15.

74 Cornell University Law School, 2004, p. 15.

75 Infocuria, 1991a, 1991b, 2003, 2005.

76 Infocuria, 1991a, 1991b, 2003, 2005.

77 De Muyter & Verheyden, 2010, p. 3.

78 Infocuria, 2008, 2010.

79 Infocuria, 2008, para. 199.

The Court repeated this argument in the price squeeze *Telefónica* case.[80]

10.2.2. The extent to which sector-specific regulation impacts on the substantive assessment of the materiality of an abuse of dominant position

This **example** is in the Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, also called 'the Guidance Paper'. This case has to do with the '**extent to which sector specific regulation impacts the substantive assessment of the materiality of an abuse**'.[81] The guidance states 'In applying the general enforcement principles set out in this Communication, the Commission will take into account the specific facts and circumstances of each case. For example, in cases ***involving regulated markets***, the Commission will take into account the specific regulatory environment in conducting its assessment.'[82]

10.2.3. From Equally Efficient Competitor (EEC) test to Reasonably Efficient Competitor (REC) test?

There are diverse kind of tests utilized to detect a margin squeeze issue, of which the principal tests are the Equally Efficient Competitor (EEC) test and Reasonably Efficient Competitor (REC) test[83]. Whereas the EEC test analyses the costs of the incumbent (historical evaluation – ex post), the REC test asseses the costs of a hypothetical reasonably efficient rival (sets of assumptions and expectations - ex ante). The regulatory authorities prefer to use the REC test to evaluate newly liberalised markets[84] and the EEC test is considered the general rule to assess a case of abuse of dominant position[85] and margin squeeze.[86]

The influence of sector-specific regulation on competition law appears because the Notice on the application of the competition rules to access agreements in the telecommunications sector-framework, relevant markets and principles, called 'Access Notice', recognizes the possibility of using the REC test as an alternative to EEC test in an ex-post/price squeeze case.[87]

---

80 Infocuria, 2012, para. 204.

81 De Muyter & Verheyden, 2010, p. 3.

82 European Commission, 2009, para. 8.

83 Auf'mkolk, 2012, p. 150.

84 Auf'mkolk, 2012, p. 151.

85 European Commission, 2009, para. 80; Gravengaard & Kjaersgaard, 2010, p. 289.

86 Auf'mkolk, 2012, p. 159.

87 European Commission, 1998, para. 118.

11. COMPETITION LAW AND SECTORAL REGULATION: COMPLEMENTS?

11.1. The US case

Before *Trinko*, the regulated industries were subject to competition law[88] Comparing the *AT&T*,[89] *Trinko* and other contemporaneous decisions, a 'radical change in the relationship between competition law and regulation law'[90] can be seen. Before *Trinko* antitrust law operated alongside regulation, including rate and access regulation.[91] Later, the SC pointed out that in the presence of a regulatory structure, designed to deter and remedy anti-competitive harm, the additional benefit provided by antitrust law would be small.[92] A case about the securities market, called *Credit Suisse*[93] reinforced the Trinko's view. The SC declared that 'the securities laws are «clearly incompatible» with the application of the antitrust laws in this context.[94]

In *Linkline,* the SC rejected the application of antitrust law in a regulated market.[95]

11.2. The EU case

The Commission has expressed that regulation and competition law constitute a 'coherent regulatory framework.'[96] The Access Notice declares that they 'are both important and mutually reinforcing for the proper functioning of the sector.'[97]

In turn, the ECJ has expressed that competition rules laid down by the EC Treaty supplement the legislative framework.[98] In Telefónica, the General Court expressed a similar conclusion.[99]

88 Klovers, 2011, p. 490.

89 Leagle, 1983.

90 Brennan, 2008, p. 135.

91 Klovers, 2011, p. 494.

92 Cornell University Law School, 2004, p. 12.

93 Cornell University Law School, LII, 2007.

94 Cornell University Law School, LII, 2007, p. 1.

95 US Supreme Court, 2009, p. 9.

96 European Commission, 1991, para. 15, 1998, para. 57–149.

97 European Commission, 1998, para. 58.

98 Infocuria, 2010, para. 92.

99 Infocuria, 2012, para. 293.

12. THE CHILEAN SITUATION

12.1. The influence of competition law on sector-specific regulation

There is a strong influence of competition law on sectoral regulation. The first example is price regulation[100]. Article 29 of the General Telecommunications Act 18.168 (GTA) states that the Competition Tribunal (CT) has to evaluate the conditions in the market. If they are not sufficient to guarantee system of free pricing, then tariff regulation must be applied by the regulator (Subsecretaría de Telecomunicaciones -SUBTEL). Also, the CT determines which companies have dominance in the market. The last report (2009)[101] held that mobile telephony is a substitute for fixed telephony, but did not take the same view regarding VoIP. It also stated that there is not indispensable pricing regulations related to local telephony. Additionally, it issued several recommendations to the regulator in order to promote competition, such as number portability which became law in 2010.[102]

A last example can be found in the article 18 of Decree Law 211 (Free Competition Act), which declares that the CT can dictate instructions of general character in accordance with the law that must be fulfilled by the private parties in actions or contracts that the latter executed or enter into and that are related to competition or could hinder it. In accordance with this rule, the 18th of December 2012 the CT issued the General Instructions No. 2/2012 about the effects on free competition of price differentiation in the public telephone services «on-net/off-net tariffs» and bundling of telecommunications services. In general terms, this regulation addresses the anti-competitive effects of differential tariff for off-net and on-net calls.

12.2. The influence of sector-specific regulation on competition law

12.2.1. The Value of Regulators' reports

This issue can be illustrated via some competition law cases. In the *Celulink* case, Telefónica was accused of margin squeeze and refusal to supply in the termination of fixed-to-on net mobile calls markets.[103] Telefónica argued that the activity of the plaintiffs was illegal because it avoided the regulated access charges and provided a public telephone service without authorization. The regulator filed charges against some of the plaintiffs and informed the CT that the plaintiff's activity was unlawful under the

100 OECD Competition Committee, 2012, p. 203.

101 Competition Tribunal, 2009a, pp. 60–62.

102 Number Portability Act 20.471, 2010.

103 Supreme Court of Chile, 2010, p. 1.

Telecommunications regulation. The CT[104] and the Supreme Court of Chile[105] (SCC) dismissed this argument. This was because, at the time of the SCC decision, there was not any final judicial judgment regarding the alleged illegality of the services. Also, the SCC added that regulator reports have to be deemed expert opinion if there is a technical issue and enlightened thought if there is a legal question[106].

In the *Voissnet* case about IP Telephony, the SCC expressed the CT 'has no jurisdiction to rule about the legal nature of IP telephony services for the purpose of implementation of the General Telecommunications Act'[107] because the regulator has exclusive competence to technical interpretation of the regulations governing telecommunications according the article 6 of the GTA.

12.2.2. Article 8 of the GTA

Paragraph 7 of article 8 of the GTA lays down a sectoral rule that has been applied to competition law cases. The article provides that the concessionaires of telecommunications public services 'shall not execute any action that implies discrimination or alteration to a healthy and due competition between all those that provide these complementary services'. A common type of complementary service is internet provision. This rule was applied by the CT in the *Voissnet* case where the CT pointed out that this rule is 'a reflection of the general rules of competition law'.[108] This rule seems to be close to the principle of equality of opportunities in Europe.

12.3. The Chilean Model

According the previous paragraphs there is a strong and mutual influence between sector-specific regulation and competition law. There is no issue about the compatibility of sectoral regulation and competition law. Consequently, competition law has been applied in cases related to regulated and unregulated markets.

In the *Celulink* case, there was an express recognition of the diverse goals of sectoral regulation and competition law.[109] Consumer welfare seems to be accepted as the main goal of competition law,[110] but there is a minority opinion which suggests that non-

104 Competition Tribunal, 2009b, para. 109.

105 Supreme Court of Chile, 2010, para. 11.

106 Supreme Court of Chile, 2010, para. 11.

107 Supreme Court of Chile, 2007, para. 34.

108 Competition Tribunal, 2006, para. 44.

109 Competition Tribunal, 2009b, p. 85.

110 OECD Competition Committee, 2011, p. 11.

economic goals must be considered.[111]

13. EMULATED COMPETITION

Evidence shows that competition law alone is not the best way to introduce competition into telecommunications market.[112] Therefore, attempts have been made to promote competition by various other means. For example, sector-specific regulation has been one choice. This method uses only sector-specific regulation without applying competition law. In contrast, sector-specific regulation has been coupled with competition law offering another approach to increase competition. Chile on the other hand, appears to have developed its own model. This, therefore, introduces a third possible method to increase competition. This Chilean model is influenced by the US with its consumer welfare goal and by the EU's approach which is focused on a blend of sectoral regulation and competition law.

I would like to propose a new approach and a new concept: 'emulated competition'. By this, I mean a set of regulatory tools used to foster competition in sector-specific regulation. This concept is to be preferred to synthetic competition because:

1. The word synthetic[113] evokes the idea of something made with artificial or unnatural substances. That is not the situation in the relationship between sector-specific regulation and competition law. Both are used as forms of 'regulation'.
2. The regulatory tools are used to mimic a perfect market. The expression emulate relates to the idea of matching or surpassing an achievement, typically by imitation.[114] The achievement in this type of competition is, of course, the imitation of a perfect market.

The features of emulated competition are:

a. Its main goal is to promote competition. However, it should be noted that it could be combined with non-economic goals, such as, media pluralism or universal service.

This can be confirmed in the following cases. The 1996 Telecommunication Act in the US primarily sought «to promote competition».[115] The Act expressly stated this ob-

111 Competition Tribunal, 2007.

112 ICT Regulation Toolkit & InfoDev-ITU, 2012.

113 Oxford University Press, 2012a.

114 Oxford University Press, 2012b.

115 Ginsburg, 2009, p. 10.

jective in some rules, for instance 47 U.S.C. § 276 (b)-(1) related the provision of payphone services. In Europe, the Framework Directive declares in article 8 N°2 that 'The national regulatory authorities shall promote competition'. Finally, in Chile the regulation that establishes the requirements to obtain, install, produce and exploit authorizations of intermediate services of telecommunications to provide physical infrastructure for telecommunications, expresses in the second recital, that this regulation creates «the infrastructure operator», among other reasons, to introduce «more competition» in the mobile phone industry.

However, the main goal of competition can be watered down due to other objectives found in the regulations. For example, article 18 N°2 of the Framework Directive imposes a bundle of duties on the Member State 'in order to promote the free flow of information, media pluralism and cultural diversity' of digital interactive television services. It is possible, therefore, for a regulator to decide to promote competition by using diverse regulatory tools with the objective of promoting a multi-player market that allows media pluralism and cultural diversity. Turning to universal service, some regulators use the licensing process in order to impose universal service duties. In Chile, there was a tender procedure regarding the licensing of 4G in 2.6 GHz during the 2012.[116] Among the requirements to participate in this process, it was needed to provide services to 543 isolated locations.[117] It is possible to see the regulator imposing a universal service obligation through this tender process. In sum, the regulator looks for the benefits of competition, but at the same time it tries to achieve other non-economic goals.

b. Its rules cannot be interpreted in the same way as competition law rules, particularly in an administrative law case.

This aspect was analysed in the Supreme Court case of Verizon v. FCC. The central point here was that TELRIC methodology chosen by FCC 'was neither inconsistent with the text of the statute nor contrary to its underlying objective of «promoting and reduce[ing] regulation», the Court upheld the Commission´s pricing scheme'[118] That was because it was not an antitrust case, but an administrative law case. In other words, there was an evaluation of ex-ante regulation but not an ex-post antitrust law assessment.

116 Subtel, 2011.

117 Subtel, 2012.

118 Ginsburg, 2009, p. 9.

c. Although it could be aligned with competition law methodologies, it does not operate in the same way.

This can be concluded by looking at the concept of Significant Market Power (SMP). This concept is interpreted and applied by reference to the European Court of Justice's definition of dominance in Article 102 (ex-82) of the EC Treaty. The SMP evaluation is an ex-ante analysis whereas the dominance position is an ex-post appraisal. However the application of competition law principles in sector-specific regulation could have different outcomes depending on their application by either National Regulatory Authority or Competition Authority.

d. It could have influence on competition law.

This feature could be called the 'irradiative effect' of emulated competition.

In regards to the US, after the decision in Verizon case concerning TELRIC pricing may well be influential but it will be limited to unregulated markets taking into consideration the decisions in *Trinko* and *LinkLine* cases.

In the case of Europe, the influence seems to be bigger. This was expressed through of the principle of equality of opportunities; the extent to which sector-specific regulation impacts the substantive assessment of the materiality of an abuse; and the possibility of applying the Reasonably Efficient Competitor (REC) test to a competition law case as a valid alternative to Equally Efficient Competitor (EEC) test.

Finally, in the case of Chile the influence can be seen on the value of regulators' reports and article 8 of GTA. This rule prohibits any discrimination or alteration of a healthy competition in complementary services.

e. It is permanent, in order to keep competition in concentrated markets.

In order to support the permanent nature of emulated competition, there is an economic paradigm for telecommunication deregulation[119] which explains why the telecommunications market is concentrated. This paradigm was developed based on similar historical experiments in other industries, such as, aviation, trucking, banking, etc., during the late 1970s and early 1980s. This paradigm has three economic stages. The first stage (in the initial five years) is characterized by an increase in mergers, acquisitions and new entrants. There are new products and markets. In the second stage (between five and ten years), the wave of mergers and acquisitions declines with the emergence of new entrants. The objective is on securing market share. Finally, the third stage (after ten years) is marked by the systematic formation of an oligopolistic environment with

119 Shaw, 2001, p. 6.

harmful effects over the consumers. Unfortunately, this economic paradigm seems to be a reality. Indeed, evidence shows that after approximately 30 years since liberalisation started, markets in telecommunications are highly concentrated in Europe,[120] the US[121] and Chile.[122]

Finally, it has been expressed that 'The electronic communications sector is characterised by high costs in constructing networks and infrastructure and, therefore, of high and non – transitory structural barriers to entry.'[123] If the entry barriers are not transitory, the regulatory instruments such as interconnection and LLU will not be either.

14. CONCLUSION

The relationship between sectoral regulation and competition law in the telecommunications markets is not a simple subject. More research is necessary to establish the points of agreement and disagreement between the two sectors. The proposed concept of emulated competition aims to clarify some complex issues which affect the interaction between sectoral regulation and competition law. Emulated competition can help us to understand the nature of rules that seek to promote competition in the telecommunications markets and their intended and unintended effects in the field of competition law. Finally, measures that promote competition have not been successful in promoting a market with a diversity of providers because the markets remain highly concentrated. The reasons for this are beyond the scope of this work and require a separate study.

15. BIBLIOGRAPHY

Alden, J. (2002). *Competition Policy in Telecommunications: The case of the United States of America* (pp. 1–68). Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFAQFjAA&url=http%3A%2F%2Fwww.itu.int%2Fosg%2Fspu%2Fni%2Fcompetition%2Fcasestudies%2Fus%2Fus%2520case%2520study.pdf&ei=3139T6zGEObA0QWk7OiiBw&usg=AFQjCNEIR9RNnPej_-cDDE7b2ullYDjsRQ&sig2=0Qvm3XTeDL9_-9fdQb5wbw

120 Berhin et al., 2005, p. 17.

121 Alegria, Kaczanowska, & Setar, 2012, pp. 1–2.

122 Briones, Bosselin, & Briones, 2012, pp. 10–12.

123 Broumas, 2009, p. 182.

Alegria, A., Kaczanowska, A., & Setar, L. (2012). *Highly Concentrated: Companies That Dominate Their Industries* (Special Report) (pp. 1–5). Ibis World. Retrieved from http://www.ibisworld.com/Common/MediaCenter/Highly%20Concentrated%20Industries.pdf

Auf'mkolk, H. (2012). The «Feedback Effect» of Applying EU Competition Law to Regulated Industries: Doctrinal Contamination in the Case of Margin Squeeze. *Journal of European Competition Law & Practice*, *3*(2), 149. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eda&AN=73911026&site=eds-live

Baldwin, R., & Cave, M. (1999). *Understanding regulation theory, strategy, and practice*. Oxford University Press,.

Berhin, D., Godart, F., Jolles, M., & Nihoul, P. (2005). Sector-Specific Regulation in European Electronic Communications--Meant to Disappear? *Info*, *7*(1), 4–19. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ecn&AN=0783160&site=eds-live

Brennan, T. J. (2008). Essential Facilities and Trinko: Should Antitrust and Regulation Be Combined? *Federal Communications Law Journal*, *61*, 133. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edslex&AN=edslexD7399F8E&site=eds-live

Briones, R., Bosselin, H., & Briones, C. (2012, January 6). Modelo economico-social y competencia en los mercados Chile: Un caso de oligopolio y asistencialismo. Retrieved from http://www.elmostrador.cl/media/2012/01/Chile-un-caso-de-oligopolio-y-asistencialismo.pdf

Broumas, A. G. (2009). The Necessity of Sector Specific Regulation in Electronic Communications Law. *Journal of International Commercial Law & Technology*, *4*(3), 176–184. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eda&AN=51893490&site=eds-live

Cerny, P. G. (1997). Paradoxes of the competition state: The dynamics of political globalization. *Government & Opposition*, *32*(2), 251.

Collins, R. (2004). From monopolies, virtual monopolies and oligopolies to ... what??: media policy and convergence in South Africa and the United Kingdom. *Southern African journal of information and communication*, (5), 23–39. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsoai&AN=edsoai.757379239&site=eds-live

Commission of the European Communities. Wanadoo España vs. Telefónica. , No. COMP/38.784. Retrieved from http://ec.europa.eu/competition/antitrust/cases/dec_docs/38784/38784_311_10.pdf

Competition Tribunal. Demanda de Voissnet S.A. y requerimiento de la FNE en contra de CTC. , No. C-60-05 (Competition Tribunal October 26, 2006). Retrieved from http://www.tdlc.cl/DocumentosMultiples/Sentencia_45_2006.pdf

Competition Tribunal. GLR Chile Limitada. , No. NC Nº 173-06 (Competition Tribunal July 27, 2007). Retrieved from http://www.tdlc.cl/DocumentosMultiples/Resoluci%C3%B3n-20-2007.pdf

Competition Tribunal. (2009a). *Informe emitido en ejercicio de la facultad conferida al tribunal en el artículo 29° de la ley 18168 de 1982 / Report issued in exercise of the power conferred on the court in Article 29 Act 18168 of 1982* (No. 2/2009). Santiago, Chile: Competition Tribunal. Retrieved from http://www.tdlc.cl/DocumentosMultiples/Informe_02_2009.pdf

Competition Tribunal. Demanda de OPS Ingeniería Ltda. y Otros contra Telefónica Móviles de Chile S.A. , No. C 126-07 (Competition Tribunal October 15, 2009). Retrieved from http://www.tdlc.cl/DocumentosMultiples/Sentencia%20_88_2009.pdf

Cornell University Law School, L. Verizon Communications Inc. et al. v. Federal Communications Commission et al. Certiorari to the United States Court of Appeals for the Eighth Circuit. , No. (00-511) 535 U.S. 467 (2002) (Supreme Court May 13, 2002). Retrieved from http://www.law.cornell.edu/supct/search/display.html?terms=fcc&url=/supct/html/00-511.ZS.html

Cornell University Law School, L. Verizon Communications Inc. v. Law Offices of Curtis v. Trinko. , No. 02-682 540 U.S. 398 (US Supreme Court January 13, 2004). Retrieved from http://www.law.cornell.edu/supct/html/02-682.ZO.html

Cornell University Law School, LII. Credit Suisse Securities (USA) LLC, fka Credit Suisse First Boston LLC, et al. v. Billing et al. , No. 05–1157. , 426 F. 3d 130 (US Supreme Court June 18, 2007). Retrieved from http://www.law.cornell.edu/supct/html/05-1157.ZS.html

Crandall, R. W. (2000). Telecommunications Liberalization: The U.S. Model. In T. It? & A. O. Krueger (Eds.), *Deregulation and interdependence in the Asia-Pacific region / edited by Takatoshi Ito and Anne O. Krueger.* (pp. 415–436). Chicago, Ill.?: University of Chicago Press, c2000. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edshlc&AN=edshlc.008385158-5&site=eds-live

De Muyter, L., & Verheyden, A. (2010). Interplay: ex post and ex ante regulation: Converging on substance, diverging on process? *Intermedia (0309118X)*, *38*(4), 26. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eda&AN=54862208&site=eds-live

De Streel, A. (2003). The Integration of Competition Law Principles in the New European Regulatory Framework for Electronic Communications. *World Competition: Law & Economics Review*, *26*(3), 489–514.

Den Hertog, J. (2000). General Theories of Regulation. In *Encyclopedia of law and economics. Volume 3. The regulation of contracts* (pp. 223–270). Elgar; distributed by American International Distribution Corporation, Williston, Vt. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ecn&AN=0664836&site=eds-live

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). (2002). *OFFICIAL JOURNAL- EUROPEAN COMMUNITIES LEGISLATION L*, *45*, 33–50. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbl&AN=RN112182550&site=eds-live

European Commission. Guidelines on the application of EEC competition rules in the telecommunications sector (1991/C 233/02). , 08.10.00.00 2–26 (1991). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:51991XC0906%2802%European Commission. Notice on the application of the competition rules to access agreements in the telecommunications sector - framework, relevant markets and principles. , 08.10.00.00 2–28 (1998). Retrieved from http://eur-lex.europa.eu/Notice.do?val=229833:cs&lang=en&list=229833:cs,&pos=1&page=1&nbl=1&pgs=10&hwords=Notice%20%20on%20%20the%20%20application%20%20of%20%20the%20%20competition%20%20rules%20%20to%20%20access%20%20agreements%20%20in%20%20the%20telecommunications%20%20sector~&checktexte=checkbox&visu=#texte

European Commission. Commission guidelines on market analysis and the assessment of significant market power under the Community regulatory framework for electronic communications networks and services. , Pub. L. No. 2002/C 165/03 (2002). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52002XC0711%2802%29:EN:NOT

European Commission. (2007, July 4). MEMO/07/274 - Antitrust: Commission decision against Telefónica - frequently asked questions. Retrieved July 12, 2012, from http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/274

European Commission. Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings. , 08.30.00.00 (2009). Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009XC0224%2801%29:EN:NOT

Farris, M. T. (1981). The Multiple Meanings and Goals of Deregulation: A Commentary. *Transportation Journal (American Society of Transportation & Logistics Inc)*, *21*(2), 44–50.

Fransman, M. (2000). Evolution of the telecommunications industry into the internet age. *Jets paper- University of Edinburgh Institute for Japanese European Technology Studies*, (19), ALL. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbl&AN=RN094465205&site=eds-live

Gaffard, J.-L., & Krafft, J. (2000). Telecommunications: understanding the dynamics of the organization of the industry. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsoai&AN=edsoai.711197184&site=eds-live

Geradin, D., & Sidak, J. G. (2005). European and American Approaches to Antitrust Remedies and the Institutional Design of Regulation in Telecommunications. In *Handbook of Telecommunications Economics. Volume 2. Technology Evolution and the Internet* (pp. 517–553). North-Holland, Elsevier. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ecn&AN=0951455&site=eds-live

Ginsburg, D. H. (2009). Synthetic Competition. In F. Leveque & H. Shelanski (Eds.), *Antitrust and Regulation in the EU and US: Legal and Economic Perspectives* (pp. 1–19). Elgar. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ecn&AN=1104115&site=eds-live

Gravengaard, M. A., & Kjaersgaard, N. (2010). The EU Commission guidance on exclusionary abuse of dominance-and its consequences in practice. *EUROPEAN COMPETITION LAW REVIEW*, *31*(7), 285–305. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbl&AN=RN272403604&site=eds-live

Green, J. R., & Teece, D. J. (1998). Four Approaches to Telecommunications Deregulation and Competition: The USA, the UK, Australia and New Zealand. *Industrial and Corporate Change*, *7*(4), 623–635. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ecn&AN=0493342&site=eds-live

Hall, D. (2002). EU competition policies and public services. *Transfer?: European review of labour and research?; quarterly of the ETUI-REHS Research Department*, *8*(2), 198–213. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edszbw&AN=EDSZBW364521473&site=eds-live

Hausman, J. A., & Sidak, J. G. (2007). Evaluating market power using competitive benchmark prices instead of the Herfindahl-Hirschman index. *Antitrust Law Journal*, *74*(2), 387–407.

Hermann, C. (2007). Neoliberalism in the European Union. *Studies in Political Economy: A Socialist Review*, (79), 61. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eda&AN=25415524&site=eds-live

ICT Regulation Toolkit, & InfoDev-ITU. (2012). New Zealand: Using Competition Law to Regulate Interconnection | ICT Regulation Toolkit. Retrieved March 14, 2012, from http://www.ictregulationtoolkit.org/en/PracticeNote.2597.html

Infocuria. France v Commission. , No. C-202/88 (Court of Justice March 19, 1991). Retrieved from http://curia.europa.eu/juris/showPdf.jsf?text=&docid=96210&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=19984

Infocuria. RTT v GB-Inno-BM. , No. C-18/88 (Court of Justice (Fifth Chamber) December 13, 1991). Retrieved from http://curia.europa.eu/juris/showPdf.jsf?text=&docid=95900&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=19984

Infocuria. Connect Austria. , No. C-462/99 (Court of Justice (Fifth Chamber) May 22, 2003). Retrieved from http://curia.europa.eu/juris/showPdf.jsf?docid=48315&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=19984

Infocuria. ISIS Multimedia and Firma 02. , No. C-327/03 and C-328/03 (Court of Justice (Third Chamber) October 20, 2005). Retrieved from http://curia.europa.eu/juris/showPdf.jsf?docid=60649&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=19984

Infocuria. Deutsche Telekom v Commission. , No. T-271/03 (General Court April 10, 2008). Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=71055&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=1461555

Infocuria. Deutsche Telekom v Commission (appeal). , No. C-280/08 P (Court of Justice (Second Chamber) October 14, 2010). Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=82938&pageIndex=0&doclang=EN&mode=doc&dir=&occ=first&part=1&cid=1461555

Infocuria. Telefónica and Telefónica de España v Commission (Appeal). , No. T-336/07 (General Court (Eighth Chamber) March 29, 2012). Retrieved from http://curia.europa.eu/juris/document/document.jsf?text=&docid=121143&pageIndex=0&doclang=ES&mode=doc&dir=&occ=first&part=1&cid=1461125

InfoDev-ITU, & ICT regulation toolkit. (2012a). 2.2 Regulation in Transition to Competitive Market | ICT Regulation Toolkit. *Regulation in Transition to Compe-*

titive Market. Retrieved April 12, 2012, from http://www.ictregulationtoolkit.org/en/Section.1686.html

InfoDev-ITU, & ICT regulation toolkit. (2012b). 3.1.2 The natural monopoly thesis | ICT Regulation Toolkit. Retrieved April 18, 2012, from http://www.ictregulationtoolkit.org/en/Section.2478.html

ITU-infoDev ICT Regulation Toolkit. (2012). Glossary of Terms. Retrieved from https://docs.google.com/viewer?a=v&q=cache:T4OMWlwD4_UJ:www.ictregulationtoolkit.org/Glossary+&hl=es&pid=bl&srcid=ADGEESgQ0Vva77Jnp0BaItjV8G4R1GKi4rMl-z9_MACQev32GXHsykWD8nilHIUQTPvQYbnd7JNEByizMw97ZOEwFG9ftAUfasfxcp9zWIxAIOEzDiWFLHyyOKAwqzB69Ve8Bs6_jyzE&sig=AHIEtbRhaVeGObV5XpysEtMU8TJx3R9m-w

Khemani, R. S., Shapiro, D. M. (Gefeierte P., & Centre for Co-operation with European Economies in Transition. (1993). *Glossary of industrial organisation economics and competition law*. Paris. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edszbw&AN=EDSZBW256951993&site=eds-live

Klovers, K. (2011). Unfit for Prime Time: Why Cable Television Regulations Cannot Perform Trinko's «Antitrust Function.» *Michigan Law Review*, *110*(3), 489–519.

Koenig, C., Bartosch, A., & Braun, J. D. (2002). *Ec Competition and Telecommunications Law*. Kluwer Law International. Retrieved from http://books.google.co.uk/books?id=FdJLSHV7qz8C

Landgrebe, J. (2002). The mobile telecommunications market in Germany and Europe: analysis of the regulatory environment. Ludwig-Maximilians-University of Munich. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsref&AN=MTCAMVIO.LANDGREBE.LUDWIGMAXIMILIANSUNIVERSI.BJJB&site=eds-live

Leagle. United States v. American Tel. and Tel. Co. , No. 552 F.Supp. 131 (Supreme Court February 28, 1983). Retrieved from http://www.leagle.com/xmlResult.aspx?xmldoc=1982683552FSupp131_1659.xml&docbase=CSLWAR1-1950-1985

Levi-Faur, D., Jordana, J., & Gilardi, F. (2005). *Regulatory Revolution by Surprise: on the Citadels of Regulatory Capitalism and the Rise of Regulocracy*.

Levi-Faur, David. (1998). The competition state as a neomercantilist state: Understanding the restructuring of national and global telecommunications. *Journal of Socio-Economics*, *27*(6), 665–685. doi:10.1016/S1053-5357(99)80002-X

Lovdahl Gormsen, L. (2010). *A Principled Approach to Abuse of Dominance in European Competition Law [electronic resource]. / Liza Lovdahl Gormsen.* Cambridge?: Cambridge University Press, 2010. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cat00234a&AN=edinb.1941861&site=eds-live

Moguillansky, G. (1998). *Las reformas del sector de telecomunicaciones en Chile y el comportamiento de la inversión*. Santiago de Chile. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edszbw&AN=EDSZBW304395234&site=eds-live

Monti, G. (2008). Managing the intersection of utilities regulation and EC competition law. Department of Law, London School of Economics and Political Science. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsoai&AN=edsoai.692471025&site=eds-live

Nazzini, R. (2011). *The foundations of European Union competition law?: the objective and principles of Article 102 / Renato Nazzini.* Oxford?; New York?: Oxford University Press, 2011. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edshlc&AN=edshlc.012578665-4&site=eds-live

Number Portability Act 20.471. , Pub. L. No. 20.471 (2010). Retrieved from http://www.leychile.cl/Navegar?idNorma=1020620&buscar=20.471

OECD Competition Committee. (2011). *Chile – Accession Report on Competition Law and Policy 2010* (p. 66). Retrieved from http://www.oecd.org/chile/47950954.pdf

OECD Competition Committee. (2012). *Excessive Prices* (pp. 1–468). Retrieved from http://www.oecd.org/competition/abuseofdominanceandmonopolisation/49604207.pdf

Oxford University Press. (2012a). Synthetic. *Oxford Dictionaries*. Retrieved from http://oxforddictionaries.com/definition/emulate?q=emulation#emulate__4

Oxford University Press. (2012b). Emulate. *Oxford Dictionaries*. Retrieved from http://oxforddictionaries.com/definition/emulate?q=emulation#emulate__4

Pitt, E. (2005). Competition Law in Telecommunications. In *Telecommunications Law and Regulation* (pp. 293–240). Great Britain: Oxford University Press.

Scheld, H. (2007). Sector-specific Regulation: Transitory or ad Infinitum? An International Status Report on Regulatory Institutions. Retrieved April 21, 2012, from http://econpapers.repec.org/article/cesifodic/v_3a5_3ay_3a2007_3ai_3a4_3ap_3a35-40.htm

Shaw, J. (2001). *Telecommunications deregulation and the information economy / James K. Shaw.* 2nd ed. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cat00234a&AN=edinb.1219084&site=eds-live

Simpson, S. (2008, June 5). Pervasiveness and efficacy in regulatory governance - neo-liberalism as ideology and practice in European telecommunications reorganisation. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsoai&AN=edsoai.730227527&site=eds-live

Subtel. (2011, December 1). Concurso público para otorgar concesiones de Servicio Público de Transmisión de Datos Fijo y/o Móvil en las bandas de frecuencias 2.505 – 2.565 MHz y 2.625 – 2.685 MHz. Retrieved February 10, 2013, from http://www.subtel.gob.cl/index.php?option=com_content&view=article&id=3043%3Aconcurso-26&catid=65%3Aautorizaciones-tramites&Itemid=315&lang=es

Subtel. (2012, March 16). Bases del concurso público para otorgar concesiones de servicio público de transmisión de datos fijo y/o móvil en las bandas de frecuencias 2.505 – 2.565 mhz y 2.625 – 2.685 mhz. Retrieved from http://www.subtel.gob.cl/images/stories/apoyo_articulos/concurso_4g/bases_2600_refundido.pdf

Supreme Court of Chile. Voisnett S.A. y requerimiento de la fne contra CTC. , No. 6236/2006 (Supreme Court July 4, 2007). Retrieved from http://www.poderjudicial.cl/modulos/TribunalesPais/TRI_esta402.php?rowdetalle=AAANoPAANAABG9NAAF&consulta=100&glosa=&causa=6236/2006&numcua=16535&secre=UNICA

Supreme Court of Chile. Ops y otros contra Telefonica Moviles de Chile S.A. , No. 8077/2009 (Supreme Court July 7, 2010). Retrieved from http://www.poderjudicial.cl/modulos/TribunalesPais/TRI_esta402.php?rowdetalle=AAANoPAAkAABUH6AAB&consulta=100&glosa=&causa=8077/2009&numcua=23671&secre=UNICA

Temple Lang, J. (2009). European competition policy and regulation: differences, overlaps, and constraints. In F. Leveque & H. Shelanski (Eds.), *Antitrust and Regulation in the EU and US: Legal and Economic Perspectives* (pp. 21–75). Elgar. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ecn&AN=1104115&site=eds-live

Thierer, A. (1994). Unnatural monopoly: Critical moments in the development of the Bell system monopoly. *CATO Journal*, *14*(2), 267.

Ungerer, H. (2001). *Use of EC Competition Rules in the Liberalisation of the European Union's Telecommunications Sector* (pp. 1–22). Brussels: European Commission. Retrieved from http://ec.europa.eu/competition/speeches/text/sp2001_009_en.pdf

US Supreme Court. Pacific Bell Telephone Co. v. Linkline Communications, Inc. , No. 07-512 503 F. 3d 876 (US Supreme Court February 27, 2009). Retrieved from http://www.supremecourt.gov/opinions/08pdf/07-512.pdf

Vogel, S. K. (1996). *Freer markets, more rules?: regulatory reform in advanced industrial countries / Steven K. Vogel*. Ithaca, N.Y.?; London?: Cornell University Press, 1996.

Walden, I., & Angel, J. (2005). *Telecommunications law and regulation* (2nd ed.). Oxford?; New York: Oxford University Press.

Whish, R. (2009). *Competition law*. Oxford [u.a.]. Retrieved from http://ezproxy.lib.ed.ac.uk/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edszbw&AN=EDSZBW581006690&site=eds-live

5

REGULATING CODE: TOWARDS PROSUMER LAW?

Professor Chris Marsden
Professor of Law, Law School, University of Sussex

Dr Ian Brown
Senior Research Fellow at the Oxford Internet Institute, Oxford University

ABSTRACT: In this interdisciplinary paper written by a socio-legal scholar and a computer scientist, we explain a novel holistic approach to Internet regulation in the broader public interest. We argue for 'prosumer law' and give an example of our proposed solution to the problems of dominant social networking sites. What should prosumer law consist of? We examine the international governance of information, especially the apparent incompatibility of human rights and trade-related concerns exposed in such multi-stakeholder fora as the OECD. We examine the 'hard cases' of Google search dominance and Facebook social networking site dominance, and their challenges to competition and to fundamental rights of prosumers. Finally, we argue for holistic regulation of the Internet, taking a trans-disciplinary perspective to solve 'hard cases' we examine. Prosumer law suggests a more directed intervention, to prevent Facebook or Google+ or any other network from erecting a fence around its piece of the information commons: to ensure interoperability with open standards. It is not sufficient for it to permit data deletion as that only covers the user's tracks. It requires some combination of interconnection and interoperability, more than transparency and the theoretical possibility to switch. It needs the ability for exiting prosumers to interoperate to permit exit.

KEYWORDS: Prosumer; law; competition; human rights; regulation.

1. INTRODUCTION: PROSUMER LAW AND INTERNET REGULATION

We are all becoming 'prosumers,' sharing intimate details of our personal lives online. But this 'prosumer environment' is currently either grossly unregulated, leaving personal information at the mercy of the multinationals who host it, sell adverts based on it, and sometimes claim to own it, or subject to knee-jerk over-regulation. This paper examines how a prosumer law interoperability framework can be applied to Internet law and policy. First, we assess the standard analyses of Internet regulation. We explain how regulation of this virtual environment is best approached by examining the protocol stack rather than geographical approaches and assessing regulatory intervention according to the code solution or solutions used. However, following Shannon (1948, 1949), we reject a technologically determinist view of code as an efficient stand-alone solution and examine the predominant justifications for various regulatory systems, classified as broadly supported by economic or rights-based regulation (Lessig 1999; Balleisen

and Moss 2010). We analyse the regulatory shaping of «code» –the technological environment of the Internet comprising hardware, software and their interactions, notably in the protocols and standards used to achieve interoperability– to achieve more economically efficient and socially just regulation. In the following section, we explore a particularly promising recent approach, multistakeholder governance (Drake and Wilson 2008; DeNardis 2009).We go on to explore code-based solutions that involve both competition analysis and interoperability requirements in strategic communications sectors, before examining the case studies of search engines and social networking sites. We conclude that prosumer law is urgently needed to enable European citizens to make most effective use of the opportunities offered by broadband technologies, Web2.0 and the overall Digital Agenda.

The Internet is not a novelty in regulatory discussion (and was not at the time of much initial surveying in this field; Kahin and Nesson 1997). But it's relatively fast and technologically dynamic development means that there is likely to remain a governance gap between what the technologists and advanced users know of the medium and political responses, as with many other advanced technologies (Brownsword 2005). Internet regulatory history is partial or incomplete, as the issue areas were either neglected by regulators for Internet-specific reasons as technically forbidding (as with many Internet security problems) or because of forbearance based on the desire to avoid harming self-regulatory mechanisms (Price and Verhulst 2004; Priest 1997) and to ensure the continued competitiveness advantages of rapid Internet deployment and development. Regulation has lagged Internet development.

There is an extensive history of competition policy in favour of open technology standards that long predates the Internet (Kahin and Abbate 1995), but the evidence of extensive network effects and innovation that can rapidly tip markets has helped focus policymakers' attention on the potential for using interoperability as a solution to the online competition and innovation problems that have emerged. As competition policy provides for interoperable remedies, governments have set great store by the success of open standards as solutions for the well-known entrenchment of dominant Internet commercial actors using network effects (Pitofsky 1998; Lemley and McGowan 1998). The market and information failures of the network effects pervading the Internet were noted by the chair of the FTC as early as 1996 and have been in evidence throughout its development (Bar, Borrus, and Steinberg 1995, Pitofsky 1998). As the technology stabilizes and matures, it may be that less radical innovation lies ahead, but we see no reason for policymakers to surrender entirely to a cable television model (Lemley and Lessig 1999) for the Internet in copyright or carriage or convergence on social networking. Therefore, solutions that maintain interoperability and open standards, which drove Internet, World Wide Web, mobile, and computer innovation, should be maintained against the Janus-faced comfort of a largely walled-garden, passive Internet future. We consider US arguments (Wu 2010, Zittrain 2008, Lessig 1999, 2006) for self-regulation

to have demonstrably failed, and focus on European policy to explore prosumerism as both a market-based and citizen-oriented regulatory tool. We base our argument on the empirical case studies presented in 'Regulating Code' (Brown and Marsden 2013), but we extend our argument from that monograph to assess the environmental preconditions for prosumer law.

2. CONFLICTING THEORETICAL APPROACHES TO INTERNET REGULATION

There are three existing conflicting theoretical approaches to Internet regulation from a technical and legal policy perspective: continued technological and market-led self-regulation, reintroduction of state-led regulation, and multi-stakeholder co-regulation.

The first, self-regulation, holds that from technical and economic perspectives, self-regulation and minimal state involvement are most efficient in dynamic innovative industries such as the Internet. This explanation is challenged by three factors: technological, competition, and democratic. Technology is never neutral in its social impact (Reed 2007; Dommering 2006). Network and scale effects are driving massive concentration in information industries (Zittrain 2008; Wu 2010). And voters will not allow governments to ignore the social impact of this ubiquitous medium.

The second explanation holds that from the legal policy perspective, governments need to reassert their sovereignty. It states that code and other types of self-regulation critically lack constitutional checks and balances for private citizens, including appeal against corporate action to prevent access or remove materials (Frydman and Rorive 2002; Goldsmith and Wu 2006). According to this explanation, government should at least reserve statutory powers to oversee self-regulation to ensure the effective application of due process and attention to fundamental rights in the measures taken by private actors. However, government regulation has serious legitimacy deficits, with as much government as market failure in Internet regulation to date, with overregulation evident in public and private censorship (MacKinnon 2012). There has been widespread industry capture of regulators and legislators in, for instance, copyright law (Horten 2011). Incumbents lobby to protect and introduce new barriers to entry with regulatory or legislative approval, as in a perceived failure to enforce or approve network neutrality legislation (Marsden 2010). There has been continued exclusion of wider civil society from the formal policy discussion, where official views do not permit easy representation of new non-corporate technical or user rights lobbies (Mueller 2010).

The civil society argument leads to the third multistakeholder co-regulatory explanation: that formally inclusive multistakeholder co-regulation –reintroducing both state and citizen– is the approach that has the best chance to reconcile market failures

and constitutional legitimacy failures in self-regulation (Collins 2010; Marsden 2011). Though intended to increase inclusiveness by representation beyond the government-business dialogue, there are significant questions as to the effectiveness, accountability, and legitimacy of civil society groups in representing the public interest. There is a body of work on Internet governance specifically addressing legitimacy gaps and development challenges in global institutions from an international political economy perspective (Mueller 2010; Drake and Wilson 2008). Given the legitimacy gap in multistakeholder interaction, it is unsurprising that the approach so far has been to conduct conversations rather than make law in such fora, reflecting the «unconference» approach of Internet innovators (in which agendas are collaboratively determined by participants at the beginning of a meeting). Cynicism is at least partly justified (Morozov 2011).

Co-regulation has been extensively discussed in European law (Senden 2005; Hüpkes 2009, Marsden 2011), including in Internet regulatory debates (Frydman, Hennebel, and Lewkowicz 2008) and in relation to data protection governance (Raab 1993). Co-regulation is even more familiar to Australian regulatory scholars since the term entered common use in about 1989 (Marsden 2011), with the term applied to codes of conduct for industry sectors (Palmera 1989; McKay 1994; Grabowsky 1995; Sinclair 1997) including the Internet (Chen 2002). Adoption of the term in the United States has been slow, with co-regulatory in legal terms referring to state-federal division of competencies (Noam 1983). However, both Balleisen (Balleisen and Eisner 2009; Balleisen 2010) and Weiser (2009, 2010) have made extensive claims for co-regulation to be adopted more frequently.

2.1. Empirical 'Hard' Case Studies Exploring Prosumer Law

Our approach takes a multidisciplinary perspective from both computer science and law, following Kahin and Abbate (1995), Berman and Weitzner (1995), and Lessig and Resnick (1998). We cover European as well as U.S. regulation and policy, and explain why a geographically specific attempt to regulate will largely fail to achieve optimal code and regulatory solutions. Previous legal work has tended to examine the Internet from a position reflecting the technology's unregulated origins (Post 2009), even in debunking the borderless «Wild West» mythology of early libertarian paradigm (Lessig 2006; Goldsmith and Wu 2006; Zittrain 2008). They equally have tended to be U.S.-centric. This debate has been effectively ended in favour of realistic pragmatic viewpoints (Reidenberg 1993, 2005). Regulatory and political economy work has concentrated on single issues or themes, such as the domain name system or privacy issues. There has been significant analysis in individual issue areas, notably the Internet Corporation for Assigned Names and Numbers, or ICANN (Mueller 2002) and Internet standard setting (Camp and Vincent 2004). Holistic examinations have tended to be compendia, such as Marsden (2000), Thierer and Crews (2003), and Brown (2013), or examine the Internet from development or other political economy perspectives (Cowhey, Aronson, and Abelson, 2009).

We examined empirically grounded, multidisciplinary case studies of five difficult areas –what we refer to as hard cases: data protection; copyrights; censors; social networking; and smart pipes (Brown and Marsden 2013: Chapters 3-7). The first three are case studies in fundamental rights with economic implications. The final two are studies of the most innovative platforms to develop new markets and protect those fundamental rights. We deliberately omitted search, whose development was critically dependent on 2012-13 antitrust activity in Brussels and Washington. Hence the final substantive part of this article considers recent developments in the regulation of search (Zittrain 2008; Deibert et al. 2010). The mass take-up of social networking tools has heightened concerns over privacy, copyright, and child protection and created a generic centre for regulatory activity that raises new questions about the scope and focus of Internet regulation. With nearly one billion Facebook users, regulators' concerns over ordinary citizens' use of the Internet have led to specific regulatory instruments that address the risks of such use (Facebook 2012; Office of the Data Protection Commissioner Ireland 2011). The case study which concludes this article builds on the literature and regulatory proceedings to assess the extent to which the more conventional issues-based regulatory instruments are being supplemented by generic social networking regulation.

We address these key questions in each of the substantive case studies:

- Who were the key stakeholders (traditional and multistakeholder), and how far were they involved in policy debates, organizational design, and operational issues associated with the regulatory processes or institutions adopted? What was the institutional political economy (Mueller 2010)?
- How far did solutions have source, process, or outcome legitimacy (Weber and Grosz 2009), including human rights compliance, in the outcome? This exploration is based on both documents relating to design and later judgments of human rights bodies (e.g., national parliamentary scrutiny committees, Council of Europe).
- How effective is the current and developing code solution? How might it have developed differently under different regulatory conditions?

In each case study, we examined whether governments have moved from sledgehammer prohibition-based, enforcement-oriented regulation, to smarter regulation that works technically, with some degree of outcome legitimacy in terms of goals. These might, for instance, support the creation of public goods and disruptive innovation in markets. A smart solution in terms of code and regulation would provide effectiveness in enforcement (whether by law or code), technical efficiency (in an engineering sense) and legitimacy, transparency, and accountability (to allay rights-based concerns). Unsurprisingly, the outcomes are likely to be trade-offs among these goals.

There are regulatory opportunities to shape the market in favour of interoperability if regulators choose such options. The open Internet policy coordination challenge is acknowledged by the G8 nations (2011: 14): «As we adopt more innovative Internet-

based services, we face challenges in promoting interoperability and convergence among our public policies on issues such as the protection of personal data, net neutrality, transborder data flow, ICT security, and intellectual property». This policy field displays both a plurality of market actors (content and carriage disguises the various interests within and between those sectors, such as mobile networks and vertically integrated actors) and a profusion of formal (state and supranational) and informal (standard-setting) regulators. It exhibits advanced examples of regulatory capture, especially in the more static and matured regulatory environment of telecoms.

2.2. Regulating Through Code

A more technical view can provide a different perspective. Engineers designed the Internet, and its content, services, and applications sit on the infrastructure. Therefore the logic of the infrastructure's design can provide a basis to assess what is different about the Internet for regulatory purposes: its code (Reidenberg 1998; Lessig 1999; Werbach 1997). This suggests that we explore the Internet from the perspective of those who designed its standards, whether the basic standards of the Internet Protocol (IP) itself and its end-to-end design (Clark and Blumenthal 2011), the motives and (limited) policy purposes behind the refinement of that design, or the particular applications that interact directly with the content layer (Berners-Lee and Fischetti 2000). Internet self-regulation emerges from that technical perspective. Early analysts viewed technical and geographical challenges to existing regulatory functions (Johnson and Post 1996) as insurmountable obstacles to regulation. Later analysis demonstrated that there was much greater interdependence between the allegedly global and un-regulable Internet and national rules. The ability of the state to seize physical assets and interrogate evidence (such as data on servers) is at the centre of national enforcement (Brown, Edwards, and Marsden 2009), as well as traditional state censorship.

Clark et al. (2005: 10) recognize that struggle or «tussle» between different interests is as important in technology evolution as in economic and political systems, suggesting that «we, as technical designers, should not try to deny the reality of the tussle, but instead recognize our power to shape it». As Greenstein (2011) advises standards bodies, «doing the tussle» can create more robust and widely adopted industry standards. Although this is a mandate for the technical community, it can be extended to the legal regulatory communities that directly shape the various aspects of Internet development, many of which already recognize that their shaping decisions are moves in a game rather than acts of sovereign design. Design choices in code can be as normative as law –decisions have to be made on the values that code embeds (Brown, Clark, and Trossen 2011). Code has continued to morph rapidly even as legislation has tried to adapt. Investor certainty and democratic participation in legislative processes are arguably enhanced by the leisurely speed of legislation, contrasted with the rapid –but slowing– progress of Internet standards in which only technical experts can realistically participate. Most

progress has happened with technical protocol development within companies (and, arguably, open source communities), where coordination («tussle») problems are less complex than in legislatures. A more dynamic social network than blogs and e-mail, a better P2P voice over Internet protocol client that could evade ISP control, and a new search algorithm and method of targeting advertising were all eagerly taken up by consumers. The development of Google, Facebook, and Skype is testimony to the ability of emergent code to respond to and keep pace with market demands.

Architecture, law, norms, and markets interplay (Lessig 1999). Regulators have only slowly woken up to regulation using technology. If regulators fail to address regulatory objects at first, then the regulatory object can grow until its technique overwhelms the regulator (Wu 2003). Digitally locked music formats were outpaced by the overwhelming Metcalfe's law effect of MP3 file sharing as a legitimate but untethered technology. Major rights holders were highly successful in coordinating demands for DRM from tech companies, but ultimately they were defeated when their own cartel was attacked by the dominant monster they created: iTunes. Apple used its pricing policy as a bargaining tool to push rights holders to abandon DRM (Williams and Gunn 2007).

Code can be controlled effectively by government in the public interest, to control corporations as well as to censor citizens. Reidenberg (2005) argues that law can use code to overcome code, as Yahoo! filters French users to prevent access to Nazi memorabilia auctions. Another example is China using Cisco routers and code to create its «Golden Shield» filter (Deibert et al. 2010). A combination of points of control (Zittrain 2006) and scale economies (Lemley and McGowan 1998) give levers for law and markets to act on architecture. Traction results from the physical presence of the Internet company on the sovereign territory of the host government. The forces of regulation can be shaped more subtly: forbearance in one dimension enables expansion in others. Where code is slow to evolve, law can assist by removing bottlenecks to innovation. Where law is designed expressly to stymie code innovation, code is likely to spill over any logjam by creating new paths to achieve user goals, as, for instance, in the P2P solution to friends sharing music files. Accusations of illegality did not serve as a veto on user adoption of P2P. Both permissive un-regulation and prohibition create pitfalls in public understanding of the effect of regulation on technologies. In simple terms, these regulatory clichés of the Internet routing around censorship as damage, or the heavy hand of the law falling on all users, do not greatly assist public and policymaker understanding of the wider challenges of Internet regulation any more than death penalty debates assist in understanding the scope of physical world regulation (Reed 2010, 2012).

Regulation that succeeds or fails based on the presence or absence of specific software tools is doomed to eventual failure, while most users own open computing platforms and can download and run the software of their choice. A horizon limit of Zittrain (2008) is a failure to fully incorporate the market structure limits to generativity versus stability and move beyond nudges into regulation (House of Lords 2011).

Despite Zittrain's concerns over the rise of «tethered» devices, the success of the iPhone and Android software platforms (with limited oversight from Apple, and even less from Google) demonstrates that the benefits to innovation of openness will continue to give manufacturers a strong incentive to provide such a capability (Ohm and Grimmelman 2010), though we note that mandated interoperability is neither necessary in all cases nor necessarily desirable (Gasser and Palfrey 2012). Moves to hardwire regulation in all computing devices in an attempt to enforce copyright restrictions have faded away in the face of resistance from manufacturers and consumers, both by lobbying and in the marketplace.

3. COMPETITION LAW AND THE INTERNET

Are there solutions that may be effective ex ante to ensure the development of technologies that do not act against the public interest, without stifling innovation and introducing bureaucratic interventionist regulation to an area that has blossomed without it? Such a solution would avoid the economic determinism of belief in the invisible hand of the market, and the technological determinism of some (typically super-profitable multinational) technology companies that claim that progress all but inevitably results in wider choice and more desirable features, despite public policy concerns.

Two examples present themselves: one a remedy of necessity in competition law, the second a deliberate design feature increasingly being deployed by OECD governments. The first is the use of competition law to engage in predicting and designing prospective markets, and the second is the widespread adoption of interoperability policies across the European Union and like-minded territories. The recent literature on competition policy has tended toward substituting economic judgments of consumer harm for political judgments and the apparent triumph of the Chicago school of microeconomics and associated economic doctrines regarding the perfectability of competition (Lessig 1998). The notion of creative destruction, whereby a lazy monopolist is overwhelmed by an innovative flexible competitor, has gained much ground, following the work of Joseph Schumpeter and the Austrian school (Mehra 2011). The Internet had appeared secure ground for Schumpeter's hypothesis, and social networks even more so, given News Corporation–owned MySpace's dominance that was replaced rapidly by that of start-up Facebook between 2007 and 2009. Against this must be placed two rival readings of this case study. The first is that social networks were an immature medium, and the growth of the market floated all ships in enabling all rivals to grow while consumers experimented. Consumer preference led to a maturing of the market, which itself tipped toward the eventual winner, Facebook, whose monopoly is now arguably durable. The second reading is more structural: that social networking had relatively low entry barriers in the past, as did, for instance, search engines, but that the advertising-dominated mass market model that currently applies is inimical to the

successful overturning of Facebook's dominance. Internet markets are not in continuous «Schumpeterian emergency» (Bresnahan 2011).

The fertile testing ground of social networks can be once more employed as Google+ challenges Facebook, just as Microsoft's Bing search engine challenges Google's main search engine business. Net neutrality deals with a century-old monopoly over copper telephone wiring into the home that has been leveraged by state-sanctioned monopolies as it became possible to attach modems and other appliances to the copper telephone network. Schumpeterian creative destruction theory in such a durable and high-entry-cost environment is arguably a misapplication. One could date concern over closed walled garden social networks –closed areas of moderated content and services intended to encourage users to stay within affiliated Web pages and thus attract advertising– further back to the time of the 1994 MCI investment in News Corporation, leveraging its ISP access business into content (Noam 1994).

3.1. Interoperable Code and Communications Policy

An extensive legislative and regulatory history of public communications occupies a special place in regulatory policy far predating modern competition law. This has always justified an ex ante regulatory policy. The loss of the ability to license particularly multinational Internet enterprises does not of itself entirely negate ex ante regulation –standards define the architecture of code, and standards are heavily government influenced even when not government funded. The government imprimatur on standards enables significant control, which is arguably as true in the twenty-first century as it was for Marconi in the nineteenth (Spar 2002). The notion that communications policy introduces certain rights and duties is as old as electrical and electronic communications media, with the 1844 Railways Act in the United Kingdom introducing the right for government to take control of the telegraph for the national interest –this only seven years after electric telegraph technology was standardized (Marsden 2012). Cannon (2003) suggests that the fundamental regulatory constraint imposed on U.S. telecoms firms in the 1980s was open network architecture (ONA) under the 1985 Computer III inquiry by the U.S. Federal Communications Commission (FCC). (The Computer II and III inquiries refer to investigations by the FCC into the regulation of data transfer and the conditions necessary to achieve an increasingly competitive market for that data.) This constraint had its European equivalent (ONP) and amounted to interoperability plus physical interconnection between networks (Coates 2011).

Understanding code and legal regulation leads to a better understanding of how regulation can work toward better code rather than simply avoiding the worst of code. That conjunction of code and regulation will lead to better outcomes than a Chinese wall designed to keep out code. We explain how innovative regulatory and policy responses to the increasingly controlled Internet user experience can harness the power of code to create opportunities for innovation rather than erect entry barriers to new

applications. We consider the code remedies imposed on Microsoft in the European Commission (EC) final settlement of its antitrust case in 2009 and Intel in its Federal Trade Commission (FTC) antitrust settlement of 2010 (Coates 2011). We argue that interoperability is the key to regulating dominant actors' uses of code. Such checks to encourage competition do not ensure fundamental rights that must be respected in communications industries, and we argue that improved competition law enforcement to shape more interoperable code must be accompanied by human rights audits to create greater commercial and state respect for fundamental rights (Murray and Klang 2005).

The outcome of the two decades of Microsoft competition litigation, beginning with U.S. antitrust investigation in 1991 prior to the dawn of mass Internet adoption, was to enforce interoperability and application programming interface disclosure (EC 2010b), with Intel settling a similar long-standing investigation into interoperability and anticompetitive practices. The interoperable code solution was extended and adapted by the complainants in both Google and Facebook investigations by the EC opened in 2010 (IP/10/1624). Apple's iTunes faced similar calls in its price discrimination settlement by the EC in 2007–2008 (IP/08/22) and its preliminary antitrust investigation into Apple's App Store policies (IP/10/1175). Most merger decisions throughout the period 1996 to 2011 supported interoperability and open standards, including European media mergers in the mid-1990s, the AOL-TimeWarner and Baby Bell mergers subject to Computer III requirements, and European Commission abuse of dominance decisions against Intel, Microsoft, and Apple. It is our contention that similar remedies should be pursued against the new information monopolists of Google and Facebook, where abuse of dominance is found. Google and Facebook negotiated consent decrees after user privacy breaches, which commits both to agreeing to privacy audits of all products and applications every two years until 2030.

Moreover, the interoperability approach does prevent a further regulatory arm wrestle of the type that Wu so colourfully chronicles and has pervaded the history of pre-Internet communications policy. It does depend on effective enforcement, and in this it suggests a heroic commitment to such policies at national as well as European levels, which critics suggest is beyond the European Commission's appetite for implementation (Moody 2010). Critics may argue that an approach founded largely on the relatively puny market impact of the Microsoft decision is grasping at the shortest of straws. The alternative, trench warfare based on regulatory attempts to re-establish rigid separation of functions (Kroes 2010), is in our view both an excessive intervention given the continuing flow of innovation in the Internet ecosystem and likely to favour the politically skilled incumbents more than scrappy entrants, as we have seen in our case studies.

A comparable example is the attempt to separate retail from investment banking. This has been a far higher political priority in the wake of the vast regulatory failures in

bank regulation since 1980 but shows little real progress since 2007's calamitous revelation of the extent of the larceny in the banking system in the United States and Europe (Davies 2010). We accept that a complex and interlocking EIF will depend on coordination between member states and the European Commission, a coordination shown to be spectacularly lacking in the altogether more important matter of the governance of the single European currency in 2010 through 2012. However, interoperability is technical enough, and its problems and potential hostages lie far enough away from Brussels (mainly in Silicon Valley, San Diego, and Seattle) that a heroic policy signal is possible.

The FTC may have shown the way in its treatment and settlement of the Intel case, with its emphasis on interoperability requirements as a remedy with a six-year period stated and conditions affecting interoperability and patent policy in the case of change of control, a spectacularly invasive example of interoperability being hard-wired (FTC 2010). It is coincidental and fortuitous that interoperability can also mean free software in principle (however expensive its implementation and integration with legacy systems). Politicians who (perhaps mistakenly) assume that interoperability is a free and leisurely European lunch are more likely to support that policy. However, we recognize that interoperability is neither a simple nor a cost-free option (Gasser and Palfrey 2012), nor that it should be imposed without prima facie evidence of dominant actors' refusing to provide interface information that permits interoperability. Kroes (2010a) referred to the arduous attempts made by antitrust authorities on both sides of the Atlantic to ensure interoperability in the Microsoft and Intel cases. The outcome was to deny those actors the tools to exclude innovative competitors from the market. Hard-wired interoperability is the most promising solution to achieve those ends, however tortuous the task.

It has been suggested that open participatory standards are themselves better for the development of fundamental rights in terms of participation and more equal access to information (La Rue 2011). Support for an open environment to stimulate innovation does suggest less corporate control of the value chain and possibilities for state censorship (Zittrain 2003) but does not in itself guarantee fundamental rights. The wider the choice of code available to users, the higher their ability is to choose code that respects their speech freedoms and personal data, but that is by no means a given. Creating conditions for interoperability does not enable governments or corporations (or civil society) to shirk the responsibility to ensure Internet architectures respect fundamental rights. For example, communications equipment that can help repressive states monitor users and ultimately punish dissidents creates an obligation on manufacturers and democratic governments to prevent export of such technology to such states (MacKinnon 2012). While that is not yet a regulatory aim that has been enforced, a fundamental rights argument (Google's mission statement, «Don't Be Evil») argues that such a regulation would need to be placed on top of any innovation or competition arguments in such a specialized sector (Brown and Korff 2012).

The EC's thinking on interoperability and code has developed through the course of the Microsoft, Intel, and Rambus cases (Coates 2011). Neelie Kroes was competition commissioner from 2005 to 2009 and signalled more intervention on interoperability: «I will seriously explore all options to ensure that significant market players cannot just choose to deny interoperability with their product» (Kroes 2010). She argues that the lengthy Microsoft case has lessons for action: «The Commission should not need to run an epic antitrust case every time software lacks interoperability.» Eighteen years of transatlantic competition proceedings against Microsoft resulted only in a choice of browsers, a very large but proportional fine, and some old code being released. Microsoft and Intel's settlements illustrate a general point about smart structural remedies under competition policy: network effects demand very effective transatlantic cooperation plus policy formed from research into global information technology. This applies the Lessig «code is law» analysis but with Braithwaite and Drahos' international coordination regulatory approach applied to the overall information environment (Braithwaite and Drahos 2000; Drahos and Braithwaite 2002). Forerunners of the suggested policy direction are 1980s data protection and 1990s cryptography cooperation.

Institutional examination needs to account for alternative histories, as previous Internet policy studies have concluded following North (1990; Benkler 2006). Our framework and conclusions can be applied to two recent developments, based on our continued examination of the issues in 2012-13. These are the continued competition investigations into Google's dominance of search advertising, and the privacy law reforms specifically applied to social networks, notably Facebook. We note as background that net neutrality, state censorship and copyright reform all remain mired in exactly the public goods failures that we have extensively documented.

4. CASE STUDY I - SEARCH MARKETS

Google has faced competition investigations on both sides of the Atlantic since 2010. It settled with the US authorities on 3 January 2013 (FTC 2013), and sent a settlement proposal to the European Commission on 1 February 2013 (Brunsden and White 2013). Experts have severely criticized both the timing and content of the Obama Administration's settlement, which they portray as extremely favourable to Google due to the composition of the outgoing Federal Trade Commission (FTC) board, and the decision not to proceed against the company on the main issues raised. Grimmelman (2013) argued: «If the final FTC statement had been any more favourable to Google, I'd be checking the file metadata to see whether Google wrote it.» The European Commission investigation continues as we write, with the same four principal complaints raised against Google as in the US:

1. Search bias – that Google favours its own products in search results over competitors;

2. Vertical Search Opt-Out – Google protocols don't let websites opt out of particular uses that Google might make of the pages it indexes. A complete opt-out means giving up all Google traffic, a significant driver of traffic – especially in Europe where Google has almost 90% of the search market in the UK, and over 90% in Netherlands, France and Germany;
3. Restrictions on third party use of AdWords in one crucial respect: «The AdWords API Client may not offer a functionality that copies data between Google and a Third Party.» Companies can advertise on Google and Bing, but cannot use a program to copy Google AdWords campaigns over to Bing. This was dropped by Google as their token interoperability sop to the FTC's investigation;
4. Injunctions against standards-essential patents, including those by Google-acquired Motorola Mobility (and see the Posner (2012) now–famous judgment). The FTC concluded (4-1) that the practice is unfair competition, and Google agreed not to engage in it in the future. This fires a shot not just at Google, but also at all its rivals –a clever concession by Google.

While it would be dangerous to speculate whether the European Commission can wring any concessions on the first two points, it is worth noting that on points 3 and 4, it is Google that had claimed the right to regulate others' use of code, to use the AdWords API or to use Motorola Mobility's patents. Google and its competitors routinely privately regulate each other's code.

What we suggest is a «prosumer law» approach where interoperability and content neutrality are taken more seriously by European regulators, as the former Commissioner has continually threatened ever since the brutally extended Microsoft European competition litigation ground to a conclusion. The first objection can be resolved through forcing Google to reinforce its search neutrality rather than bias results using its search algorithms (Bracha and Pasquale 2008), and the second by a relatively trivial (by Google standards) amendment to its code to allow other websites more flexibility in future listing, rather than the 'nuclear option' of a complete opt-out via the existing robots.txt convention.

We do not adopt a strong normative claim that Google should adopt an entirely neutral perspective (nor do we adopt such an approach to network neutrality), but we do advocate enforcement of truth-in-advertising, that any search engine (or ISP using search) claiming verifiably neutral results produce the same, or else be made to prominently advertise its product as a commercially driven, affiliate-biased selective search engine. Search neutrality would require that any Internet search engine provide search results that correspond to its mission to search the Internet for relevant products, with any 'promoted' products advertised as such and separated from the search results requested by the user. Note that this is exactly the solution that leading search engines claim to provide, with 'sponsored links' boxes separated from the overall results in either a sidebar or more intrusive text box above the main results. That would not prevent linking

to an affiliated maps provider, or shopping engine, as long as these links are not in the main results. Such a requirement does not impose a significant regulatory burden on a search provider, rather it reinforces the brands of search providers of integrity. It would not apply to selective search providers if labelled as such: 'a search engine which selectively provides you with search results according in part to its commercial affiliations' (or equivalent wording) would need to be prominently displayed above search results if that were the case. In the book, we suggest a similar approach to network neutrality violators, who could not advertise their services as allowing end-users' choice in accessing the 'Internet' when in fact it is a commercial Intranet to which full access is provided (Marsden 2010).

These code-based solutions are lighter touch than multi-billion Euro fines or structural separation of businesses (Wu 2010). This is an illustration of what we mean by a smarter 'prosumer law' approach. Prosumers enjoy using Google products, and would like to trust Google more by seeing transparency rather than bias. Google is not evil, but it is a stockholder company, and its directors' duties since it was floated publicly in 2003 are to maximise returns. Regulated capitalism demands a response that works with markets and prosumers.

5. CASE STUDY II: SOCIAL NETWORK REGULATION

We give an example of our proposed solution to the problems of dominant social networking services. Descriptions of personal data as the metaphorical oil in the digital economy are wide of the mark, even for data of the deceased (Edwards 2013), unless they have seeped into the sediment. Personal data accumulate with the individual's treks into cyberspace, and therefore a better metaphor is silk, woven into the tapestry of the user's online personality. Moreover, user is a poor description of the potential creativity of the individual user (Von Hippel 1976; Morrison, Roberts, and von Hippel 2000) in cyberspace. The hideous ugliness of the term prosumer (the online creator, after Toffler 1980) should not hide the potential for the individual to move far beyond a caterpillar-like role as a producer of raw silk and encompass their ability to regenerate into a butterfly or moth. The verb to surf indicates the user-generated agenda of the prosumer, as does the weaving of a web by billions of prosumer-created sites. The silk has created tapestries as rich as Wikipedia, as well as Facebook and MySpace (Benkler 2011). It is arguably the loss of the sense of ownership of «your space» that led to the latter's decline. The silkworms that turned created a death spiral (Mehra 2011), even though it was at first only a prosumer boycott (led by those who preferred to control their data cocooned in their own personal form: chrysalis or pupae). The problem is that such boycotts rapidly create a landscape of zombie users: many readers will have a ncient Hotmail and MySpace accounts that are undead, unchecked, unmourned, useless to advertisers, and antithetical to positive network effects that alone can feed a successful business. We por-

tray an information landscape with a billion captured moths creating silk for ever fewer merchants, notably Google, Facebook, Amazon, and Apple. Allowing those moths to evolve and choose whether to exit, control their own prosumption, or continue their silken personal data capture is a key question for prosumer law. As with silk moths, so for prosumers leaving the iron bonds of the dominant social network may only result in vainglorious (social) suicide).

If Google's flotation took some time to wipe away an idealistic founders' myth of anti-evil cartoon-book coding, Facebook's 2012 flotation required no such adjustment. Facebook's buccaneering attitude to 'monetizing' your personal intimate data, and those of your children and grandchildren, was recognised long ago as requiring greater regulatory action. The European home of half of its users has 27 state regulators of personal data, and Facebook chose one that relocated in 2006 from Dublin to Portarlington, Co. Laois (Department of Justice and Equality 2006), resulting in wholesale removal or resignation of its expert staff. Google is also regulated from Portarlington. While German state and federal regulators and others may rattle sabres at Facebook, it is the Irish regulator that took action in auditing Facebook in spring 2012 and insisting on remedial action on at least nine counts (Office of the Data Protection Regulator 2011).

5.1. Prosumer Solution to Social Networking

What should prosumer law consist of? It is not sufficient for it to permit data deletion because that only covers users' tracks; it does not entitle them to pursue new adventures, particularly where all their friends (real and imagined) are cocooned inside the Schumpeterian victor's web. It requires some combination of interconnection and interoperability more than transparency and the theoretical possibility to switch (Werbach 2010; Weiser 2009). It needs the ability for exiting prosumers to spread their wings, take their silk away from the former exploiter, cover their traces, and interoperate their old chrysalis with their new moth life. That suggests interoperability to permit exit (Burk 1999).

Consider the problem with two hard examples: network neutrality and social networking systems (SNS). In the former case, users can exit an ISP that is breaching network neutrality, subject to two as-yet-unfulfilled conditions: that full, meaningful consumer transparency is offered and that switching is trivial, in particular that consumers can leave their minimum-term contract (typically two years) because the ISP has breached its side of the bargain by introducing non-neutral practices. Because consumers keep control of their data (except for law enforcement data retention purposes) and can delete cookies, extract files hosted, and so on, then absent behavioural advertising of the deeply invasive Phorm type (using Deep Packet Inspection to track the prosumer's Web browsing, they are free to leave. Moreover, they can take their telephone number with them to their new ISP. That does presuppose there remains a neutral ISP in the environ-

ment, which is not by any means certain for the Skype-active mobile user (Sahel 2011). Regulatory action in transparency, switching, and contract exit is needed.

In the case of SNS, such a relatively easy transition is not assured. First, there is the extraction of the user's proprietary data. While the Irish regulator decision ensures that data can be returned, it does not cover all the data cocooned in one piece. First, Facebook removed data to the United States without valid consent, as, for instance, in the Like button dispute in Schleswig-Holstein in 2011. Second, data were leaked promiscuously to third-party application providers, as the Federal Trade Commission (FTC) discovered. Third, the formatting of the data and the need to access friends' data (e.g., wedding and baby photos), which are indiscoverable using a search engine, mean that the user is in the position of: «You can leave Facebook, but Facebook never leaves you.»

Prosumer law suggests a more directed intervention to prevent Facebook or Google+ or any other network from erecting a fence around its piece of the information commons: to ensure interoperability with open standards (Lemley 1999). We argue that it is untrue to state that there is so much convergence between platforms that there is no clear distinction between open commons and closed proprietary environments (Barnett 2011), though voluntary forfeiture of intellectual property rights to permit greater innovation has always been commonplace (Bresnahan et al 2011; Barton 1997). It also suggests that Google's attempts to adjust search in favour of its products, if proven to extend beyond preferential puffery for Google+, are inimical to prosumer law. Prosumerism should be a declared policy of the European Commission alongside the European interoperability framework (EIF). European electronic commerce consumer law is a marked departure from freedom of contract in European law. It is therefore not difficult to extend the EIF and the legal protection for prosumers in this direction in law, though implementation requires all member states to commit to such a step in practice as well as theory.

One promising solution to the otherwise patchy nature of regulation is that of SNS interoperability. In earlier work we have identified high sunk costs and network effects as barriers to entry protecting dominant SNS: «The behemoth SNS can influence negotiation with ISPs absent net neutrality regulation, leading to a vertical value chain of dominance» (Brown and Marsden 2008). We proposed that «competition authorities should impose ex ante interoperability requirements upon dominant social utilities … to minimise network barriers» and identified three models of information regulation from case law:

- Must-carry obligations, which are imposed on broadcasters and electronic program guides
- Application programming interfaces (API) disclosure requirements, which were placed on Microsoft by the European Commission ruling upheld by the European Court of Justice

- Interconnection requirements on telecommunications providers, especially those with dominance –already echoed in the AOL/Time Warner merger requirement for instant messaging interoperability.

The success of both Facebook and the AppStore gives pause to those who champion an entirely open model, as consumers appear to prefer low-walled gardens, a debate endlessly reiterated since the AOL walled-garden service. Nevertheless, SNS are another example of some user preference for a relatively closed-walled-garden model.

Facebook in January 2013 enforced its ban on exporting data for use in social networks, by blocking Russian search engine Yandex's new social search mobile app API calls within three hours of launch. It also cut off two apps from 'Find Friends' (Facebook's API): Twitter's photo app Vine and messaging app Voxer. This sounds remarkably like many recent reports of blocking of APIs and content by telecoms companies in breach of net neutrality law. Facebook –like Microsoft, Apple and Intel before it– may be under threat of being in abuse of a dominant position. It should be required to remedy its failure to follow our prosumer law principles, to permit interoperability rather than harming smaller competitors.

United States lobbyists constantly complain that the proposed new EU Data Protection Regulation will raise their costs of doing business. But US federal and state have far more vigorously pursued Facebook, Google and others for their failures to guarantee users' privacy. In November 2012, Google settled for $22.5million in the case of Safari browser tracking cookies (US v. Google Inc. 2012, Devine 2012), on top of a 2011 $8.5million settlement for privacy breaches involving Google Buzz. In January 2013, Facebook settled a class action with a $20million payment into a compensation fund (Fraley v. Facebook 2013, Marsden 2013). In 2012, both companies agreed to settle privacy complaints by agreeing to FTC privacy audit of their products for a twenty-year period (Brown and Marsden 2013: 188). Sector-specific regulation of social networking already exists de facto in the United States, while proposed new European Regulation is unlikely to be implemented before 2016-17.

The final outcome of such an approach continues to be uncertain even as Facebook announced its intention to become an «entertainment hub» with news, video, and music embedded in the site from 2012. This is a similar approach to that adopted by AOL, the mobile Vodafone 360, and MySpace and has previously failed. MySpace, for instance, rewrote its code to prevent the embedding of YouTube videos in 2008, causing significant user unrest. The experience of Facebook as a destination site will prove an excellent case study as its strategy develops. The profound implications of extensions of broadcast or other regulation onto SNS would create a very different regulatory space within which SNS operate. If one views innovation as perpetual and endemic to such networks, one may oppose such regulation on those grounds. If, however, the view is that social networking growth has plateaued with the constrained environment of Facebook now dominating, then the use of competition law on the Microsoft precedent,

and its extension in EIF 2.0, may suggest that interoperability is forced on that dominant network. It is important to note that the drive by government, most pronounced in the European Commission's approach, toward more SNS regulation to conform to European legal norms as well as concerns for child protection and privacy, is conducted in an informal soft law manner (Senden 2005; Marsden 2011). Civic responsibility and the Internet is the leitmotif, from the graduated-response legislation that places enforcement in the hands of ISPs and co-regulation models for harmful but legal content that affects search, e-commerce, SNS, cloud services (Cowen 2013) and other intermediary providers.

6. CONCLUSION: TOWARDS PROSUMER LAW?

Governments, users, and better functioning markets need a smarter «prosumer law» approach to Internet regulation. Prosumer law would be designed to enhance the competitive production of public goods, including innovation, public safety, and fundamental democratic rights. Prosumer law suggests a more directed intervention to prevent Facebook or Google or any other network from erecting a fence around its piece of the information commons: to ensure interoperability with open standards.

The European prosumer has already dealt significant creative destruction to many pre-Internet industries through such services as Linux, Skype, BitTorrent, and the VLC Media Player. It would be fitting for Europe to lead the United States in adapting Von Hippel's ideas to the case studies that we have presented here. We do not have great confidence that the United States will match rhetoric with reality in enforcing such an agenda, preferring talk of «Internet freedoms» and «bills of privacy rights» without actual regulations to achieve those outcomes.

We are convinced that fudging with nudges (Yeung 2012) needs to be reinforced with the reality of regulation and co-regulation, in order to enable prosumers to maximize their potential on the broadband Internet. Prosumerism should be a declared policy of the European Commission alongside the European interoperability framework (EIF). In fact, the Commission on 17 December 2012 launched its Code of European Union Online Rights for European citizens using the Internet (EC 2012). European electronic commerce consumer law is a marked departure from consumer protection in European contract law. It would therefore not be difficult to extend the European interoperability framework and legal protection for prosumers in this direction in law, though implementation requires all member states to commit to such a step in practice as well as theory.

Strengthened data protection rules are an important step towards prosumer law. But interoperability is needed as well as data portability, to permit exit to more prosumer-friendly products than Google and Facebook, should prosumers wish to switch. It

requires a combination of interconnection and interoperability more than transparency and the theoretical possibility to move data. Only then will information markets become more competitive, and prosumers have the luxury of real choice between very different standards offered by their hosts.

7. BIBLIOGRAPHY

Balleisen, Edward J., and Marc Eisner. 2009. The promise and pitfalls of coregulation: How governments can draw on private governance for public purpose. In New perspectives on regulation, ed. David A. Moss and John A. Cisternino, 127–150. New York: The Tobin Project.

Balleisen, Edward, J. 2010. The prospects for effective co-regulation in the United States: A historian's view from the twenty-first century. In Government and markets: Toward a new theory of regulation, ed. Edward J. Balleisen and David A. Moss, 443–481. Cambridge: Cambridge University Press.

Bar, F., M. Borrus, and R. Steinberg. 1995. Islands in the bit-stream: mapping the NII interoperability debate. Working Paper 79, Berkeley Roundtable on the International Economy. http://brie.berkeley.edu/publications/WP%2079.pdf.

Barnett, Jonathan M. 2011. The host's dilemma: Strategic forfeiture in platform markets for informational goods. Harvard Law Review 124:1861.

Benkler, Y. 2006. The wealth of networks: How social production transforms markets and freedom. New Haven, CT: Yale University Press.

Benkler, Y. 2011. Network theory: Networks of power, degrees of freedom. International Journal of Communication 5. http://ijoc.org/ojs/index.php/ijoc/article/view/1093.

Berners-Lee, Tim, and Mark Fischetti. 2000. Weaving the Web: The original design and ultimate destiny of the World Wide Web. New York: HarperCollins.

Bracha, O. and Pasquale, F. (2008) Federal Search Commission? Access, Fairness, and Accountability in the Law of Search, 93 Cornell L. Rev. 1149.

Brown, I. and C. Marsden, Regulating Code, Cambridge: MIT Press, 2013.

Brown, Ian, and Christopher T. Marsden. 2008. Social utilities, dominance and interoperability: A modest proposal. Presentation to GikIII [Geek Law], Oxford. http://www.slideshare.net/blogzilla/social-networks-dominance-and-interoperability-presentation.

Brown, Ian, and Douwe Korff. 2012. Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online. Washington, D.C.: Global Network Initiative. http://globalnetworkinitiative.org/news/new-report-outlines-recommendations-governments-companies-and-others-how-protect-free.

Brown, Ian, David Clark, and Dirk Trossen. 2011. Should specific values be embedded in the Internet architecture? In Proceedings of the Re-Architecting the Internet workshop. New York: ACM Press.

Brown, Ian, Lilian Edwards, and Christopher T. Marsden. 2009. Information security and cybercrime. In Law and the Internet, 3rd ed., ed. L. Edwards and C. Waelde. Oxford: Hart.

Brown, Ian. Ed. 2013. Research handbook on governance of the Internet. London: Edward Elgar

Brownsword, R. 2005. Code, control and choice: Why East is East and West is West. Legal Studies 25:1–21

Brunsden, J. & A. White, 'Google Submits Settlement Offer, EU Antitrust Chief Says', Bloomberg News, 1 Feb. 2013.

Burk, Dan L. 1999. Virtual exit in the global information economy. Chicago-Kent Law Review 73:943–995

Camp, L., and C. Vincent. 2004. Setting standards: Looking to the Internet for models of governance. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=615201.

Cannon, Robert. 2003. The legacy of the FCC's computer inquiries. Federal Communications Law Journal 55:167–205

Chen, Peter. 2002. Lust, greed, sloth: The performance and potential of Internet coregulation in Australia. Griffith Law Review 11:465–496

Clark, David D., and Marjory S. Blumenthal. 2011. The end-to-end argument and application design: The role of trust. Federal Communications Law Journal 63:357–390.

Clark, David D., John Wroclawski, Karen R. Sollins, and Robert Braden. 2005. Tussle in cyberspace: Defining tomorrow's Internet. IEEE/ACM Transactions on Networking 13 (3): 462–475

Coates, Kevin. 2011. Competition law and regulation of technology markets. New York: Oxford University Press.

Constine, J., 'Facebook Is Done Giving Its Precious Social Graph To Competitors', TechCrunch, 24 Jan. 2013.

Cowen, Tim (2013) Competition Law Issues in Cloud Computing, Computers and Law, 10 February

Cowhey, P., J. Aronson, and D. Abelson. 2009. Transforming global information and communication markets: The political economy of innovation. Cambridge, MA: MIT Press.

Cowie, C., and C. Marsden. 1999. Convergence: Navigating bottlenecks in digital pay-TV. Info 3 (1): 53–67

Davies, Howard. 2010. The financial crisis—Who is to blame? Cambridge: Polity Press

Deibert, R. J., J. G. Palfrey, R. Rohozinski, and J. Zittrain, eds. 2008. Access denied: The shaping of power, rights, and rule in cyberspace. Cambridge, MA: MIT Press.

Deibert, R. J., J. G. Palfrey, R. Rohozinski, and J. Zittrain, eds. 2010. Access controlled: The shaping of power, rights, and rule in cyberspace. Cambridge, MA: MIT Press.

DeNardis Laura, E. 2009. Protocol politics: The globalization of Internet governance. Cambridge, MA: MIT Press

Department of Justice and Equality, Address by the Tanaiste at the official opening of the newly decentralised Office of the Data Protection Commissioner, 11 Dec. 2006.

Devine, Lauren-Kelly, 'Court Approves Google's Privacy Settlement', RegBlog, 27 Nov. 2012.

Dolmans, Maurits. 2010. A tale of two tragedies: A plea for open standards. International Free and Open Source Software Law Review 2 (2):115–136. http://www.ifosslr.org/ifosslr/article/view/46/72.

Dommering, E. J. 2006. Regulating technology: Code is not law. In Coding regulation: Essays on the normative role of information technology, ed. E. J. Dommering and L. F. Asscher, 1–17. The Hague: T.M.C. Asser Press

Drahos, Peter, and John Braithwaite. 2002. Information feudalism: Who owns the knowledge economy? New York: Free Press.

Drake, William J., and Ernest J. Wilson III, eds. 2008. Governing global electronic networks: International perspectives on policy and power. Cambridge, MA: MIT Press

Edwards, Lilian. 2013. Privacy, Law, Code and Social Networking Sites. In Research handbook on governance of the Internet, ed. Ian Brown. Cheltenham: Edward Elgar

European Commission, 'Code of EU online rights published', Digital Agenda for Europe Blog, 17 Dec. 2012.

European Commission. 2010a. Communication: Towards interoperability for European public services. December. http://ec.europa.eu/isa/documents/isa_iop_communication_en.pdf.

European Commission. 2010b. Web browser choice for European consumers. http://ec.europa.eu/competition/consumers/web_browsers_choice_en.html

Facebook. 2012. Form S-1 Registration Statement under the Securities Act of 1933, Facebook, Inc. Washington DC: Securities and Exchange Commission. http://sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm

Faulhaber, Gerald R. 2002. Network effects and merger analysis: Instant messaging and the AOL–Time Warner case. Telecommunications Policy 26 (5–6): 311–333

Federal Trade Commission, Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns In the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search, 1 Mar. 2013.

Fraley v. Facebook, Case No. CV-11-01726 RS.

Ganslandt, Mattias. 2010. Completing the internal market. December. http://www.talkstandards.com/completing-the-internal-market/.

Gasser, Urs, and John Palfrey. 2012. Interop: The promise and perils of highly interconnected systems. New York: Basic Books

Goldsmith, Jack, and Tim Wu. 2006. Who controls the Internet? Illusions of a borderless world. New York: Oxford University Press

Grabowsky, P. 1995. Using non-governmental resources to foster regulatory compliance. Governance: An International Journal of Policy, Administration and Institutions 8:527–550

Greenstein, Shane. 2010. Standardisation and coordination. IEEE Micro 30 (3): 6–7

Grimmelman, J. 'Not with a Bang', Laboratorium, 3 Jan 2013.

Group of 8. 2011. G8 Declaration: Renewed Commitment for Freedom and Democracy. G8 Summit of Deauville, May 26–27. http://www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html

Horten, Monica. 2011. The copyright enforcement enigma: Internet politics and the telecoms package. Basingstoke: Palgrave Macmillan.

House of Lords. 2011. Behaviour change. HL Paper, Science and Technology Committee Report. http://www.publications.parliament.uk/pa/ld201012/ldselect/ldsctech/179/17902.htm

IP/08/22 Brussels, 9th January 2008 Antitrust: European Commission welcomes Apple's announcement to equalise prices for music downloads from iTunes in Europe

IP/09/232. 2009b. Social networking: Commission brokers agreement among major Web companies.

IP/10/1175 Brussels, 25 September 2010 Antitrust: Statement on Apple's iPhone policy changes

IP/10/1624 Brussels, 30 November 2010 Antitrust: Commission probes allegations of antitrust violations by Google

Johnson D., and D. Post. 1996. Law and borders: The rise of law in cyberspace. Stanford Law Review. 48:1367–1402.

Kahin, B., and J. Abbate, eds, Standards policy for information infrastructure, Cambridge, MA: MIT Press, 1995.

Kahin, B., and C. Nesson, eds. 1997. Borders in cyberspace: Information policy and the global information infrastructure. Cambridge, MA: MIT Press

Kroes, N. 2010. Address at Open Forum Europe 2010 Summit: Openness at the heart of the EU digital agenda. Brussels. Speech 10/300.

Kroes, N. 2010a. Towards more confidence and more value for European digital citizens European Roundtable on the Benefits of Online Advertising for Consumers Brussels. SPEECH/10/452.

La Rue, Frank. 2011. Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression. Human Rights Council Seventeenth session agenda item 3, A/HRC/17/27, May 2011 17. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Lemley, Mark A., and L. Lessig,. 1999. Ex parte declaration of Professor Mark A. Lemley and Professor Lawrence Lessig in the Matter of: Application for Consent to the Transfer of Control of Licenses of MediaOne Group, Inc. to AT&T Corp CS. Federal Communications Commission. Docket No. 99–251

Lemley, Mark A., and David McGowan. 1998. Legal implications of network economic effects. California Law Review 86:479–611

Lessig, L. 1998. The new Chicago school. Journal of Legal Studies 2: 661–690.

Lessig, L. 1999. Code and other laws of cyberspace. New York: Basic Books.

Lessig, L. 2006. Code version 2.0. New York: Basic Books.

Lessig, L., and P. Resnick. 1998. The architectures of mandated access controls. In Proceedings of the 1998 Telecommunications Policy Research Conference. http://groups.csail.mit.edu/mac/classes/6.805/articles/cda/lessig-resnick-access-controls.pdf

MacKinnon, Rebecca. 2012. Consent of the networked: The worldwide struggle for Internet freedom. New York: Basic Books

Manne, Geoffrey A., and Joshua D. Wright. 2011. Google and the limits of antitrust: The case against the antitrust case against Google. Harvard Journal of Law and Public Policy 34 (1). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1577556

Marsden, C., ed. 2000. Regulating the global information society. New York: Routledge.

Marsden, C. 2010. Net neutrality: Towards a co-regulatory solution. London: Bloomsbury Academic.

Marsden, C. 2011. Internet co-regulation: European law and regulatory legitimacy in cyberspace. Cambridge: Cambridge University Press

Marsden, C., 'Fraley v. Facebook, Inc. - $20m settlement for private education/research of social media users', Regulating Code Blog, 26 Jan. 2013.

McKay, Jennifer M. 1994. Classification of Australian corporate and industry based codes of conduct. International Business Law 22:507–514

Mehra, Salil K. 2011. Paradise is a walled garden? Trust, antitrust and user dynamism. George Mason Law Review 18:889–952.

Moglen, Eben. 2003. The dotCommunist Manifesto. http://emoglen.law.columbia.edu/publications/dcm.html

Moody, Glyn. 2010. European interoperability framework v2–: The great defeat. Computerworld 17. http://blogs.computerworlduk.com/open-enterprise/2010/12/european-interoperability-framework-v2---the-great-defeat/index.htm

Moody, G., 'UK Government Fails Its First Big Procurement Test', ComputerWorld, 1 Feb. 2013.

Morozov, Evgeny. 2011. The Net delusion: The dark side of Internet freedom. New York: Public Affairs Press.

Morrison, P. D., J. H. Roberts, and E. von Hippel. 2000. Determinants of user innovation and innovation sharing in a local market. Management Science 46 (12): 1513–1527

Mueller, Milton. 2002. Ruling the root: Internet governance and the taming of cyberspace. Cambridge, Mass: MIT Press.

Mueller, Milton. 2010. Networks and states: The global politics of Internet governance. Cambridge, MA: MIT Press

Murray, A., and Matthias Klang, eds. 2005. Human rights in the digital age. London:Glasshouse Press.

Noam, E. M. 1994. Beyond liberalization II: The impending doom of common carriage. Telecommunications Policy 18 (6):435–452

Noam, Eli M. 1983. Federal and state roles in telecommunications: The effects of deregulation. Vanderbilt Law Review 36:949–955.

Office of the Data Protection Commissioner. Ireland. 2011. Data protection audit of Facebook Ireland. December 21. http://dataprotection.ie/viewdoc.asp?m=f&fn=/documents/Facebook%20Report/report.pdf/report.pdf

Ohm, Paul, and James Grimmelmann. 2010. Dr. Generative or: How I learned to stop worrying and love the iPhone. Maryland Law Review 69:910–953

Oxman, Jason. 1999. The FCC and the Unregulation of the Internet. Office of Plans and Policy, Federal Communications Commission. http://www.fcc.gov/Bureaus/OPP/working_papers/oppwp31.pdf.

Palmera, Ian. 1989. Images of regulation: Travel agent legislation and the deregulation debate. Politics 24 (2): 13–22

Pitofsky, Robert. 1998. Self regulation and antitrust. Prepared remarks of the chairman, Federal Trade Commission, D.C. Bar Association Symposium, February. http://www.ftc.gov/speeches/pitofsky/self4.shtm.

Posner, R., Apple, Inc. & Next Software Inc. V. Motorola, Inc. & Motorola Mobility, Inc., Opinion And Order of 22 June 2012, Illinois Dist. Ct. No. 1:11-cv-08540.

Post, David. 2009. In Search of Jefferson's moose: Notes on the state of cyberspace. New York: Oxford University Press

Price, M., and S. Verhulst. 2004. Self-regulation and the Internet. Amsterdam: Kluwer.

Priest, Margot. 1997. The privatisation of regulation: Five models of self-regulation. Ottawa Law Review 29:233–301

Reed, C. 2007. Taking sides on technology neutrality. SCRIPTed 4: 263–284

Reed, C. 2012. Making Laws for Cyberspace.Oxford University Press (Oxford),

Reed, C. 2010 How to Make Bad Law: Lessons from Cyberspace. Modern Law Review vol. 73: 6, 903-932 at 10.1111/j.1468-2230.2010.00824.x

Reidenberg, J. 1993. Rules of the road for global electronic highways: Merging the trade and technical paradigms. Harvard Journal of Law and Technology 6:287, 301–304.

Reidenberg, J. 1998. Lex informatica: The formulation of information policy rules through technology. Texas Law Review 76:553–593.

Reidenberg, J. 2004. States and law enforcement. University of Ottawa Law and Technology Journal. 213:225–229.

Reidenberg, J. 2005. Technology and Internet jurisdiction. University of Pennsylvania Law Review 153:1951-1959

Saltzer, J., D. Reed, and D. Clark. 1984. End-to-end arguments in system design. ACM Transactions on Computer Systems 2:277–288

Senden, L. 2005. Soft law, self-regulation and co-regulation in European law: Where do they meet? Electronic Journal of Comparative Law 9 (1) 1–27

Shannon, Claude E. 1948. A mathematical theory of communication. Bell System Technology Journal 27:379–423, 623–656.

Shannon, Claude E. 1949. Communication in the presence of noise. Proceedings of IRE 37(1):10–21

Sinclair, Darren. 1997. Self-regulation versus command and control? Beyond false dichotomies. Law and Policy 19:529–559

Spar, Debora. 2001. Pirates, prophets and pioneers: Business and politics along the technological frontier. London: Random House

Thaler, Richard H., and Cass R. Sunstein. 2009. Nudge: Improving decisions about health, wealth, and happiness. New Haven, CT: Yale University Press.

Thierer, A., and Clyde W. Crews, eds. 2003. Who rules the Net? Internet governance and jurisdiction. Washington, DC: Cato Institute

Toffler, Alvin. 1980. The third wave. New York: Bantam

U.S. v. Google, 3:12-cv-04177, U.S. District Court, Northern District of California (San Francisco).

Von Hippel, E. 1976. The dominant role of users in the scientific instrument innovation process. Research Policy 5 (3): 212–239

Weber, R., and M. Grosz. 2009. Legitimate governing of the Internet. International Journal of Private Law 2:316–330

Weiser, P. 2009. The future of Internet regulation. University of California Davis Law Review 43:529–590.

Weiser, Phil. 2010. Towards an international dialogue on the institutional side of antitrust. NYU Annual Survey of American Law, 66 (1): 101–113.

Werbach, Kevin. 1997. Digital tornado: The Internet and telecommunications policy, Office of Plans and Policy. Federal Communications Commission. http://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp29pdf.html.

Werbach, Kevin. 2002. A layers model for Internet policy. Journal on Telecommunications and High Technology Law 1:37–67.

Williams, Martyn, and Angela Gunn. 2007. EMI to ditch DRM, offer improved sound on iTunes. Computerworld, April 2.

Wu, T. 2003. When code isn't law. Virginia Law Review 89:679

Wu, T., The master switch: The rise and fall of digital empires, New York: Knopf, 2010.

Yeung, Karen. 2012. Nudge as fudge. Modern Law Review 75:122–148

Zittrain, J. 2003. Be careful what you ask for: Reconciling a global Internet and local law. In Who Rules the Net? ed. A. Thierer and C. Crews. Washington, DC: Cato Institute.

Zittrain, J. 2008. The future of the Internet and how to stop it. New Haven, CT: Yale University Press

Zittrain, Jonathan. 2006. The generative Internet. Harvard Law Review 119:1974–2040.

6

EL *BIG DATA* EN LAS ADMINISTRACIONES PÚBLICAS: EL DIFÍCIL EQUILIBRIO ENTRE EFICACIA DE LA ACTIVIDAD ADMINISTRATIVA Y GARANTÍA DE LOS DERECHOS DE LOS CIUDADANOS[1]

Julián Valero Torrijos
Profesor de Derecho Administrativo. Universidad de Murcia
Coordinador del grupo de investigación iDerTec (Innovación, Derecho y Tecnología)

RESUMEN: El uso avanzado de la información administrativa constituye un relevante desafío para el Derecho por cuanto conlleva una tensión latente para las bases conceptuales y las garantías jurídicas en las que se basa la regulación vigente. En el caso del *big data* las posibilidades de tratamiento de información de los ciudadanos plantean un escenario ciertamente apetecible –incluso podríamos decir que tentador– desde la perspectiva de la eficiencia y eficacia de la actividad de las Administraciones Públicas, en particular por lo que respecta a las que suponen una restricción o limitación en la posición jurídica de los particulares. En la presente comunicación se analizan algunas de las principales implicaciones jurídico-administrativas que conlleva dicha modalidad de uso de la información, ofreciéndose elementos de juicio que faciliten el debate dogmático imprescindible para lograr un equilibrio adecuado entre las posibilidades de innovación tecnológica y las garantías que ha de asegurar el Derecho.

PALABRAS CLAVE: *big data*, derechos del ciudadano, protección de datos personales, Administración Pública.

1. INTRODUCCIÓN

El proceso de modernización tecnológica que se ha vivido en los últimos años con la implantación de la Administración electrónica se ha basado en un modelo de gestión y regulación que, en gran medida, no tiene en cuenta el potencial innovador de la tecnología como instrumento para incrementar sustancialmente la eficacia y la eficiencia[2]. A este respecto, las tendencias más recientes (Batini, 21) nos sitúan ante un modelo de gestión de la información basado en el aprovechamiento de la utilidad de los datos a la hora de ofrecer servicios de valor añadido. Desde este planteamiento, tanto el *big data*

1 Este trabajo se ha realizado en el marco del proyecto «Los desafíos jurídicos de Internet para la protección de los datos personales: hacia un marco normativo de tercera generación (DER2009-09157)», financiado por el Ministerio de Economía y Competitividad.

2 Con carácter general, en relación con este planteamiento, cfr. Valero, capítulos 1 y 4.

como el *open data* se han presentado como alternativas dotadas un destacado potencial[3], si bien su virtualidad en el ámbito de las Administraciones Públicas se enfrenta a una serie de problemas y dificultades que, desde el punto de vista jurídico, pasan necesariamente por la adaptación de las garantías formales en que tradicionalmente se ha basado el marco normativo regulador de la actividad administrativa.

Dos notas distintivas especialmente destacadas pueden apuntarse inicialmente en relación con el *big data*: de una parte, la mayor exigencia de transparencia que requiere y/o supone a pesar de las limitaciones del marco normativo vigente y las reticencias que inspiran la práctica administrativa; y, de otra, la necesidad de proceder a una redefinición de las relaciones con los ciudadanos, las empresas y otros prestadores de servicios. Más allá de esta premisa, resulta imprescindible analizar las singularidades que concurren en esta peculiar modalidad de procesamiento de la información para determinar hasta qué punto resulta necesario proceder a la reformulación de las garantías jurídicas a partir de las cuales se ha ordenado tradicionalmente la actividad de inspección de las Administraciones Públicas.

2. CARACTERIZACIÓN GENERAL DEL *BIG DATA* Y DE SUS FUNCIONALIDADES EN EL CONTEXTO DE LA ACTIVIDAD DE LAS ADMINISTRACIONES PÚBLICAS

Se ha mantenido en relación con el *big data* que es la próxima frontera para la innovación, la competitividad y la productividad. Esta afirmación se basa en la evidencia de que los medios tecnológicos actualmente disponibles permiten llevar a cabo tratamientos de la información que exceden la capacidad de procesamiento de las herramientas de

3 Por lo que respecta al *big data*, se ha estimado que la transparencia y el uso avanzado de la información puede suponer incrementar la productividad y conseguir mayores niveles de eficacia y eficiencia, hasta el punto de que el sector público europeo podría reducir el coste de las actividades administrativas entre el 15 y el 20 % (Manyika, 54). En relación con el *open data*, el potencial económico de la actividad vinculada se estima en 32 billones de euros anuales en el ámbito europeo, cantidad que se eleva hasta los 140 si se tiene también en cuenta el impacto económico indirecto (Vickery, 3 y 4). La relevancia de la actividad económica asociada a la información del sector público en el mercado español también es muy relevante, habiéndose estimado en torno a los 330 y 550 millones de euros el volumen de negocio del sector infomediario (AGE, 10).

Ahora bien, el gran problema radica en que, si bien casi el 90 % de la información administrativa se genera en soporte electrónico gracias al proceso de modernización tecnológica que se ha emprendido en las Administraciones Públicas europeas durante los últimos quince años, sin embargo al mismo tiempo son frecuentes las inconsistencias en los formatos y los protocolos de entrada de la información (Manyika, 56); dificultad que supone un importante obstáculo para la utilización avanzada de los datos conforme a las más elementales exigencias jurídicas.

software de bases de datos convencionales en relación con la captura, almacenamiento, gestión y análisis (Manyika y otros, 1), de manera que la obtención de un valor añadido de los datos requiere la utilización de formas alternativas para su tratamiento (Dumbill, 3). Esta exigencia se basa en el incremento sustancial tanto del volumen de información que se maneja, la velocidad con que se hace y, asimismo, la variedad de los datos y la fuentes de información (Dumbill, 4 a 8). No se trata simplemente de una simple agregación cuantitativa de tales variables sino, sobre todo, cualitativa, ya que el incremento en el número de datos que se procesan conlleva igualmente una mayor exactitud en el tratamiento de la información; y, del mismo modo, el aumento exponencial de las fuentes de donde se obtienen los datos permite identificar las que ofrecen información de interés, descartando los datos irrelevantes. Y todo ello de manera prácticamente instantánea en muchos casos, lo que facilita la adopción automatizada de decisiones.

Quizás el aspecto más destacado de la revolución que supone el *big data* consiste en la unificación de grandes conjuntos de datos con un análisis avanzado que permite resolver problemas y buscar alternativas basándose en el uso de potentes algoritmos y aprovechando las posibilidades de aprendizaje de las máquinas. Así, facilita llevar a cabo predicciones en las que basar posteriores decisiones, realizar análisis a partir de los cuales implementar nuevos servicios o prestarlos de manera distinta a como se han venido ofreciendo a partir de las conclusiones obtenidas, incrementar la eficacia y la eficiencia sin tener que reducir los niveles de servicio, realizar comprobaciones de fraudes o incumplimientos de manera automatizada o, entre otras posibilidades, reducir drásticamente los tiempos empleados en la búsqueda de información y segmentar los destinatarios de servicios a los efectos de incrementar su personalización; todo ello a partir de modelos avanzados de gestión de la información basados en la anterior caracterización (Yiu, 16 a 21, Dumbill, 3). En el caso de las Administraciones Públicas son numerosos los proyectos que ya se han puesto en marcha y que, por ejemplo, han permitido incrementar notablemente la eficacia y eficiencia de sistemas de gestión de recursos naturales y bienes de dominio público, plantear políticas públicas mejor enfocadas en ciertos sectores clave como la sanidad o, más recientemente, dar soporte avanzado a las denominadas *ciudades inteligentes*[4].

Por lo que respecta específicamente al objeto de esta comunicación, los tratamientos de información propios del *big data* ofrecen posibilidades innovadoras, hasta ahora desconocidas, en relación con las actuaciones de comprobación propias de la actividad

4 http://www.smartcities.es/ (último acceso: 17/01/2013). En concreto, a modo de ejemplo, el *big data* puede aplicarse a actividades de gran relevancia práctica en grandes ciudades como la gestión del tráfico, la gestión de aparcamientos públicos o la ordenación del transporte colectivo a partir de múltiples sensores ubicados estratégicamente y de los dispositivos móviles de los ciudadanos.

inspectora[5] que realizan las Administraciones Públicas en diversos sectores, en particular aquellas que se basan en el procesamiento de información[6]. En concreto, la nota distintiva de esta modalidad es que permite realizar comprobaciones masivas de forma automatizada no sólo con las propias bases de datos o, en su caso, de otras Administraciones Públicas o entidades privadas a través de los cauces y protocolos formales que se establezcan sino, incluso, con la información desestructurada a la que pueda accederse libremente en Internet, esto es, que no se encuentre protegida con medidas de seguridad adecuadas. Se trata, por tanto, de una herramienta de un relevante potencial en la realización de actividades de inspección en sectores como la recaudación de impuestos, el control de las bajas médicas y su incidencia sobre el sistema de prestaciones, la gestión de subsidios por desempleo o, en general y sin pretensiones de exhaustividad, la supervisión sobre la realización de actividades vinculadas al otorgamiento de subvenciones.

Más allá de la funcionalidad general de esta modalidad de procesamiento informativo, el *big data* puede convertirse en una herramienta de gran ayuda para la realización de actividades inspectoras dada su capacidad para vincular los datos a un sujeto concreto (Yiu, 15), de manera que a partir del resultado de ese tratamiento pudiera incluso iniciarse un procedimiento formalizado e, incluso, imponerse una sanción, revocarse una autorización previa o requerir la devolución de una ayuda. Así pues, aun cuando inicialmente los datos recogidos pudieran encontrarse desvinculados de la persona o entidad a que se refieran, lo cierto es que los actuales medios tecnológicos permiten con cierta facilidad deshacer el anonimato (Cavoukian y Jonas, 3), en particular si tenemos en cuenta la existencia de números únicos de identificación y si no se han adoptado las más elementales medidas de disociación. Incluso, las posibilidades de identificación se incrementan notablemente en un entorno como el propio de la *web 2.0*, donde diversas herramientas –en particular las redes sociales, pero también blogs, foros…– se nutren de la información proporcionada por los propios usuarios o, en su caso, por terceros; con la peculiaridad de que la identificación es directa o, al menos, relativamente sencilla si los datos de que se disponen se pueden combinar con información adicional en poder de la propia Administración o de otras entidades, tales como los prestadores de servicios de la sociedad de la información que, incluso, pueden encontrarse en diversos lugares del mundo (Tene y Polonetsky, 13).

---

5 En todo caso, se ha destacado (Rivero, 67) que «no toda actividad pública de acopio de datos se incluye dentro de la actividad inspectora, sino únicamente aquella dirigida a velar por el ordenamiento jurídico mediante la colaboración de los sujetos privados en determinadas condiciones». A este respecto, el *big data* supone ir más allá, en la medida que ni siquiera es necesaria la colaboración en sentido estricto por cuanto la información se obtendrá en muchas ocasiones sin el conocimiento ni la colaboración del afectado o de terceros.

6 http://www.fbi.gov/news/pressrel/press-releases/health-care-fraud-prevention-and-enforcement-efforts-result-in-record-breaking-recoveries-totaling-nearly-4.1-billion (último acceso: 17/01/2013).

3. IMPLICACIONES JURÍDICAS DEL *BIG DATA* EN RELACIÓN CON LAS ACTUACIONES ADMINISTRATIVAS RESTRICTIVAS O LIMITADORAS DE LA POSICIÓN JURÍDICA DE LOS CIUDADANOS. ESPECIAL REFERENCIA A LA ACTIVIDAD INSPECTORA

Así, pues, a la vista de la caracterización realizada en el apartado anterior, ¿qué garantías jurídicas deben aplicarse a este tipo de tratamientos en relación con su utilización en el marco de actuaciones de la Administración Pública que limiten o restrinjan la posición jurídica de los ciudadanos?

Se trata de una cuestión de gran trascendencia ya que es precisamente el uso de la información así obtenida la que permitirá adoptar decisiones formalizadas, en particular por lo que respecta a la función inspectora que, en algunos casos, podría determinar el ejercicio de la potestad sancionadora[7] o, con carácter general, la iniciación de un procedimiento en sentido estricto[8].

En el supuesto de que la información se refiera a personas físicas identificadas o identificables[9], el procesamiento de la información conforme a este modelo puede facilitar, por ejemplo, la detección de una baja médica fraudulenta o actividades indiciarias de un cierto nivel de vida superior a las posibilidades que en principio correspondan a unos determinados ingresos. En consecuencia, deberían tenerse en cuenta las garantías que ofrece la normativa sobre protección de datos personales, si bien algunos de los principios en que se basa resultan ciertamente de difícil aplicación en estos casos tal y como se analizará en el siguiente epígrafe. Así, por lo que respecta a las cesiones de datos se exige el consentimiento del afectado[10] en ausencia de habilitación legal –en particular si el uso pretendido resulta incompatible con el previsto inicialmente al proporcionarse los datos–, premisa que

7 En todo caso, como se ha enfatizado (Guillén, 33 y 34), la potestad inspectora ha de ser deslindada de la sancionadora, ya que cumple otras finalidades distintas de la punitiva relacionadas con la detección del incumplimiento de las normas.

8 A este respecto se ha considerado que, salvo que así se conciba en la regulación aplicable –tal y como sucede en el ámbito tributario–, las actuaciones inspectoras suelen constituir la fase preliminar de un procedimiento (Fernández, 108 y 109); si bien hay quien, por el contrario, parte de la exigencia general de que la actividad inspectora ha de realizarse en el seno de un procedimiento administrativo (Rivero, 163 y 164). Sin duda, esta doble concepción plantea consecuencias jurídicas muy relevantes por lo que se refiere a la configuración jurídica de las garantías del ciudadano frente al *big data*.

9 En relación con el alcance de este concepto jurídico indeterminado, aun cuando el *big data* incrementa notablemente las posibilidades de identificar al usuario a pesar de haber utilizados técnicas de disociación, no por ello hay que menospreciar su trascendencia en tanto que instrumento de protección del titular de la información (Cavoukian, 4).

10 Cfr. Tene y Polonetsky (2012, 5), en cuya opinión debería prescindirse de la exigencia del consentimiento cuando los beneficios del uso prospectivo de los datos sean mayores que los riesgos para la privacidad. En todo caso no deja de ser una valoración de *lege ferenda* que, por tanto, no puede admitirse si tenemos en cuenta el marco normativo vigente.

resulta razonable en el caso de las comunicaciones formalizadas. Pero ¿qué sucede cuando la información en que se base la actuación inspectora se encuentre accesible en una red social, a través de un blog o de la participación en un foro? En estos casos nada parece obstar a que se utilice lícitamente (Tene y Polonetsky, 14), al menos en los supuestos en que la política de privacidad del instrumento utilizado no prevea restricciones en el acceso a la información o, de contemplarlas, el usuario no haya utilizado las herramientas que le proporcione el proveedor de servicios y, en consecuencia, no hubiese impedido su conocimiento por quien no estuviese autorizado. Ahora bien, podría darse el caso de que la información se hiciese accesible por un tercero sin consentimiento del afectado, supuesto en el que la difusión sería ilícita y, por tanto, determinaría la invalidez de la actuación administrativa que se basase en ella. Ni siquiera en estos casos cabría argumentar la existencia de una habilitación legal –bastante frecuente por lo que se refiere a la actividad inspectora– ya que la eventual actividad probatoria se encontraría viciada de nulidad al tratarse de una difusión ilícita de la información que vulnera un derecho fundamental.

Por el contrario, cuando la información se refiera a personas jurídicas no resultarían de aplicación las garantías reconocidas legalmente a las personas físicas por la normativa sobre protección de datos personales, ya que aquellas carecen del referido derecho. No obstante, con independencia de la naturaleza jurídica del titular de los datos, la singularidad e intensidad del tratamiento informativo exigen un reforzamiento de la transparencia por lo que se refiere con carácter general a la actividad administrativa restrictiva o limitadora de derechos y, en especial dada la especial ausencia de garantías formales reconocidas legalmente, a la de naturaleza inspectora[11], de manera que el sujeto pasivo de la misma pueda conocer el origen de los datos, los criterios utilizados en su tratamiento y el resultado obtenido con su procesamiento[12]. Todo ello sin perjuicio de que se hubiese iniciado formalmente un procedimiento administrativo y, en consecuencia, fuesen aplicables los derechos reconocidos al afectado como interesado[13], de manera que la atribución de carácter reservado a dichas actuaciones sólo estaría justificada en los casos en que sea necesario para las finalidades de la investigación preliminar (Fernández, 357).

---

11 En consecuencia, pensamos que la posibilidad de limitar el derecho de acceso a que se ha aludido doctrinalmente (Rivero, 188 y 189) ha de ser interpretada restrictivamente en estos casos.

12 Exigencia inexcusable cuando se refieran a personas físicas, ya que en este caso concurriría el derecho de acceso específico en materia de protección de datos personales por lo que, a pesar de las dificultades inherentes a su infrecuente ejercicio, se han planteado soluciones para incentivar su ejercicio dada la relevancia de la transparencia a este respecto (Tene y Polonetsky, 26, 31 y 34).

13 No es admisible, por tanto, que las actuaciones inspectoras queden relegadas a una fase de penumbra donde no existan garantías para el afectado, ya que existe el riesgo de que se desvirtúe su naturaleza y el procedimiento que se tramite a continuación quede convertido en un mero trámite (Fernández, 110 a 113).

Así pues, más allá de la exigencia de una obligación del ciudadano de soportar la intervención administrativa para que pueda hablarse de actividad de inspección (Rivero, 75), los tratamientos informativos en que se basa el *big data* parten de una dinámica distinta: normalmente la información no se proporciona ni por el afectado ni por un tercero sino que, simplemente, se encuentra disponible en principio para otras finalidades diversas del ejercicio de una potestad administrativa. Sin embargo, a partir del procesamiento de los datos pueden iniciarse actividades inspectoras y, asimismo, las comprobaciones basadas en el *big data* pueden tener lugar en el seno de actuaciones de esta naturaleza. En consecuencia, dado que no siempre existirá un procedimiento en sentido estricto, resulta imprescindible adecuar las garantías jurídicas del afectado –que, por tanto, no siempre gozará del estatuto jurídico propio del interesado– frente a esta actividad de limitación dada la singularidad e intensidad características del *big data*. Así pues, resulta imprescindible que cualquier búsqueda informativa basada en esta modalidad sea autorizada formalmente, quede registrada y, en caso de utilizarse efectivamente los resultados obtenidos–ya de manera directa o, simplemente, para realizar ulteriores comprobaciones más precisas–, se incorporen formalmente al expediente relativo a la actuación administrativa principal en relación con la cual hayan de surtir efectos la referencia al origen de la información y la metodología empleada, de manera que se garantice al afectado el pleno ejercicio de sus derechos.

4. EL USO DEL *BIG DATA* EN LAS ADMINISTRACIONES PÚBLICAS DESDE LA PERSPECTIVA DE LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

El uso de sistemas de *big data* por parte de las Administraciones Públicas para el ejercicio de sus competencias y, en particular, para llevar a cabo actuaciones inspectoras plantea como uno de los retos más relevantes su conformidad con las garantías propias del derecho fundamental a la protección de los datos de carácter personal. Con carácter general se han destacado cuatro desafíos principales a este respecto: el anonimato, la especial protección de datos sensibles, la necesidad de garantizar la mayor capacidad de elección del titular de los datos a la hora de controlar el uso de los mismos y, finalmente, la posibilidad de crear de perfiles de usuario que se utilicen para limitar beneficios o derechos (Brill, 2 a 4).

Desde la perspectiva de la legislación española en la materia y teniendo en cuenta las anteriores consideraciones, el principio general de consentimiento como garantía principal del titular de los datos –artículo 6 LOPD– queda ciertamente superado. En efecto, en primer lugar, cabe suponer que en muchos casos la información se difunde precisamente para que sea conocida por terceros, de manera que habitualmente el usuario ni siquiera se plantea la posibilidad de restringir o limitar el uso de sus datos por parte de los destinatarios, ya que si desea establecer este tipo de limitaciones nor-

malmente procederá a activar las herramientas que suelen ofrecer los proveedores de servicios[14].

Más aún, la exigencia general del consentimiento queda excepcionada con gran amplitud en el supuesto de que los datos se recojan por las Administraciones Públicas para el ejercicio de sus competencias o, con carácter general, para aquellos supuestos en que así se prevea a través de una norma con rango legal, supuesto ciertamente frecuente en el ámbito de las potestades administrativas limitativas o restrictivas de derechos de los ciudadanos, en particular por lo que respecta a la actividad inspectora. Incluso, la relativización jurisprudencial del concepto de interés legítimo[15] para proceder al tratamiento de los datos personales sin consentimiento del afectado constituye una amenaza evidente para la integridad del consentimiento como herramienta principal de protección en esta materia.

La posición jurídica del titular de los datos ha recibido un nuevo y reciente varapalo jurisprudencial que tiene una especial incidencia en relación con el objeto de esta comunicación. En efecto, el Tribunal Constitucional[16] ha venido a avalar la irrelevancia del principio de calidad de los datos en su manifestación del uso compatible que garantiza el artículo 4 LOPD y que, en última instancia, ha de considerarse que forma parte del contenido esencial del derecho constitucional garantizado en el artículo 18.4 del Texto Constitucional. En consecuencia, y por lo que se refiere al ámbito específico del *big data*, según dicha interpretación habría que considerar que las Administraciones Públicas podrían utilizar la información de los ciudadanos que se encuentre libremente accesible a través de Internet o, incluso, en otras bases de datos de las Administraciones Públicas siempre que se trate del ejercicio de sus propias competencias.

Se trata de una consecuencia muy discutible por cuanto deja sin efecto el control que podría llevarse a cabo desde la perspectiva del contenido esencial del derecho a la protección de los datos personales, pero más allá de esta consideración no puede dejarse de advertir que la plena vigencia de las garantías informativas inherentes al titular de este derecho. En concreto, según el artículo 5.4 LOPD, más allá de que no fuere necesario el consentimiento en base a la existencia de una habilitación legal al efecto, la utilización de sistemas de tratamiento de información basados en el *big data* determinan que el titular de los datos haya de ser informado de forma precisa, expresa e inequívoca en el plazo de tres meses siguiente al registro de sus datos. Sin embargo, existe una excepción a esta exigencia que se contiene en el artículo 5.5 LOPD, en virtud de la cual no será precisa la información «cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia Española de Protección de Datos

14 Así, por ejemplo, en el caso de twitter el usuario puede restringir el acceso a sus mensajes, de manera que sólo quien decida podrá conocer el contenido de su perfil.

15 A este respecto, véase la STS de 8 de febrero de 2012, sala 3ª, recurso 25/08.

16 STC 17/2013, de 31 de enero, f.j. 9.

o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias»[17]. En consecuencia, la Administración Pública habrá de solicitar autorización expresa a la correspondiente autoridad de control, de modo que si no lo hiciese podría entenderse que la actuación restrictiva o limitadora que se base en la información así obtenida ha vulnerado el contenido esencial del derecho fundamental consagrado en el artículo 18.4 del Texto Constitucional así como, en su caso, el derecho a la defensa consagrado en el artículo 24 de la Norma Fundamental y, por consiguiente, sería nula de pleno derecho al amparo de lo dispuesto en el artículo 62.1.a) LRJAP.

Sin embargo, al margen de esta obligación informativa, el derecho de acceso sí que se encuentra legalmente limitado en algunas condiciones que podrían afectar a algunas de las modalidades de actuación administrativa en las que el *big data* ofrece un mayor potencial. En concreto, por lo que respecta al ámbito policial y tributario, estaría justificado denegar el derecho de acceso cuando su ejercicio pudiera afectar en el primer caso a las necesidades de la investigación que se esté realizando y, en el segundo, cuando el afectado esté siendo objeto de actuaciones inspectoras. Pero, ciertamente, la limitación sólo podría aplicarse en los referidos ámbitos materiales, ya que en la medida que nos encontramos ante un derecho fundamental cualquier limitación ha de interpretarse de manera restrictiva y, en última instancia, la mayor parte de las normas sectoriales que regulan la actividad administrativa ni siquiera se preocupan de regular el estatuto jurídico del titular de los datos personales.

En consecuencia, a la vista de las restricciones sustantivas a las que la interpretación jurisprudencial parece abocar, resulta imprescindible reforzar las garantías informativas del titular de los datos personales como principal medida de protección, ya que de lo contrario existe un riesgo cierto de que su posición jurídica sea puramente testimonial y, en consecuencia, la posibilidad de defensa de los derechos e intereses legítimos quede seriamente dañada.

5. CONCLUSIONES

La innovación basada en el uso de la tecnológica actualmente disponible es uno de los principales desafíos para llevar a cabo una gestión avanzada de la información por parte de las Administraciones Públicas. Sin embargo, ni el marco normativo vigente ni

17 Es importante recordar a estos efectos que la posibilidad de eximir a la Administración Pública de informar al titular de los datos cuando «impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas» a que se refería la versión inicial del artículo 24.1 LOPD fue declarada inconstitucional por la STC 292/2000, de 30 de noviembre, sin que hasta la fecha se haya procedido a darle una nueva redacción.

los sistemas documentales se encuentran preparados para este desafío, salvo destacadas excepciones. A través de las alternativas que ofrecen los modelos de gestión basados en el *big data* la actividad administrativa –en general y, en particular, la de naturaleza restrictiva o limitadora de los derechos de los ciudadanos– puede incrementar de forma notable su eficacia y eficiencia. Sin embargo, resulta imprescindible llevar a cabo una inexcusable adaptación de un régimen jurídico que no puede ya sustentarse en las tradicionales e insuficientes garantías formales que, en ocasiones y como ha tratado de justificarse someramente en esta breve comunicación, resultan claramente insuficientes e inadecuadas. Existe, por tanto, un riesgo cierto de que se conviertan en una barrera que dificulte la innovación tecnológica o, incluso, se perciban como meras previsiones formales cuyo efectivo cumplimiento sea habitualmente ignorado. En consecuencia, la posición jurídica del ciudadano no puede verse perjudicada por la singularidad del tratamiento informativo en que consiste el *big data* y la falta de concreción de las garantías de que adolece el régimen jurídico que, con carácter general, regula la actividad administrativa en esta materia, debiendo adoptarse las medidas normativas o, en su caso, interpretativas que aseguren la efectividad del ejercicio de todos sus derechos sin perjudicar con ello la adecuada defensa de los intereses generales.

6. BIBLIOGRAFÍA

Administración General del Estado (AGE): *Estudio de caracterización del Sector Infomediario en España*, edición 2012 (accesible en: http://datos.gob.es/datos/sites/default/files/files/Estudio_infomediario/Info_sector%20infomediario_2012_vfr.pdf)

Batini, C. (2010). «Data Governance», en G. Viscusi, C. Batini y M. Mecella, *Information Systems for eGovernment*. Heidelber: Springer-Verlag

Brill, J. (2012). «Big Data, Big Issues», conferencia pronunciada el 2 de marzo de 2012 en la Facultad de Derecho de la Universidad de Fordham, accesible online desde http://ftc.gov/speeches/brill/120228fordhamlawschool.pdf)

Cavoukian, A. y Jonas, J. (2012). «*Privacy by Design* in the Age of Big Data», Ontario Information and Privacy Comissioner, junio de 2012, (accessible en http://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf)

Dumbill, E. (2012), «Getting up to Speed with Big Data», *Big Data Now: 2012 Edition*, O'Reilly, Sebastopol, 2012, (accessible en http://oreilly.com/data/radarreports/big-data-now-2012.csp)

Fernández Ramos, S. (2002). *La actividad administrativa de inspección. El régimen jurídico general de la función inspectora*. Granada: Comares

Guillén Caramés, J. (2010), *Régimen Jurídico de la Inspección en Derecho de la Competencia*. Cizur Menor: Thomson-Aranzadi

Manyika, J. y otros (2011). *Big Data: The next frontier for innovation, competition and productivity*, McKinsey Global Institute (http://www.mckinsey.com/insights/mgi/research)

Rivero Ortega, R., *El Estado vigilante*, Tecnos, Madrid, 2000

Tene, O. y Polonetsky, J. (2012). «Privacy in the Age of Big Data: a Time for Big Decisions», *Stanford Law Review (online)*, núm. 63.

(http://www.stanfordlawreview.org/online/privacy-paradox/big-data)

– (de próxima publicación) «Big Data for All: Privacy and User Control in the Age of Analytics», *Northwestern Journal of Technology and Intellectual Property*

(http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364)

Valero Torrijos, J. (2013), *Derecho, Innovación y Administración electrónica*. Sevilla: Global Law Press

Vickery, G. (2011). «Review of recent studies on PSI re-use and related market developments», (http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=1093)

Yiu, C. (2012). «The Big Data Opportunity. Making government faster, smarter and more personal», *Policy Exchange*

(http://policyexchange.org.uk/images/publications/the%20big%20data%20opportunity.pdf)

COMUNICACIONES SOBRE PRIVACIDAD

7

EL DERECHO A LA PROTECCIÓN DE DATOS EN LA ADMINISTRACIÓN DE JUSTICIA

Rosa Cernada Badía
Investigadora de la Universidad de Valencia

RESUMEN: La informatización de la Justicia se presenta como un proceso tardío pero insoslayable, que no puede amparar prácticas que vulneran los derechos fundamentales y las garantías procesales. En particular, el derecho a la protección de los datos personales incorporados a los ficheros dependientes de los órganos judiciales. Al efecto, el Consejo General del Poder Judicial, órgano competente para la creación y determinación del régimen jurídico de tales ficheros, ha adoptado medidas de seguridad de nivel alto, acordes a las exigencias de la normativa sobre protección de datos. Asimismo, el acceso al expediente judicial electrónico y el ejercicio de las comunicaciones judiciales se someten a cautelas específicas para evitar divulgaciones indebidas. El sistema de protección culmina con las potestades de la autoridad de control, cuya determinación ha suscitado controversia, a partir de la reciente doctrina del Tribunal Supremo, que ha declarado la incompetencia de la Agencia Española de Protección de Datos para ejercer potestades de fiscalización y control sobre los órganos judiciales. Una materia cuya resolución deviene fundamental para garantizar el derecho a la protección de datos en la Administración de Justicia.

PALABRAS CLAVE: protección de datos personales, E-Justicia, Autoridad de Control, Publicidad procesal.

INTRODUCCIÓN

Desde la segunda mitad del siglo XX, el desarrollo tecnológico ha acompañado la evolución de las estructuras económico-sociales y, por ende, del Estado. Este proceso, sin embargo, ha desnudado las limitaciones del animal estatal, cuyo inmovilismo burocrático constituye el germen de una ineficacia sentida como endémica. Una circunstancia especialmente sangrante en la Administración de Justicia, debido a la tradicional escasez de medios que ha postergado el proceso. Por ello, la incorporación de las Tecnologías de la Información y Comunicación (en adelante, TIC) a la Administración de Justicia se ha acometido a fines del siglo XX, sobre la base que proporcionó la informatización de la Administración General del Estado. Este proceso, iniciado bajo el impulso europeo con acciones puntuales, se ha afrontado globalmente por la Ley 18/2011, de 5 de julio, reguladora del uso de las Tecnologías de la Información y la Comunicación en la Administración de Justicia (en adelante, LUTICAJ).[1]

1 *BOE* 6 de julio de 2011: http://www.boe.es/boe/dias/2011/07/06/pdfs/BOE-A-2011-11605.pdf

La informatización de la Justicia plantea retos apasionantes al Estado de Derecho, pues el objetivo de agilización de la Justicia no puede utilizarse como pretexto para desmaterializar los derechos y garantías que reconoce la Constitución española de 1978 (en adelante, CE). Especialmente, los derechos fundamentales del proceso que declara el artículo 24 de la CE y el derecho fundamental a la protección de datos consagrado en el artículo 18 de la CE. Este trabajo atiende a la protección de los datos personales generados en el seno de los procesos judiciales. Derecho que se relaciona con dos usos de las TIC en la Administración de Justicia[2]:

a) la gestión y almacenamiento de la información en ficheros judiciales, aspectos que entroncan con el fenómeno del *big data*, por la magnitud de datos incorporados.

b) la difusión de la información judicial. Ante la amplitud de este uso, el presente estudio se limita a examinar la satisfacción del principio de publicidad procesal interna, como acto procesal más estrictamente ligado a la protección de datos por la Administración de Justicia.

1. UNA APROXIMACIÓN A LA PROTECCIÓN DE DATOS COMO DERECHO FUNDAMENTAL

En el proceso de informatización de la Justicia, uno de los derechos especialmente vulnerable es el derecho a la protección de datos. Derecho fundamental de tercera generación[3] que concreta el derecho a la intimidad en el ámbito de la informática[4]. En Europa, sin perjuicio de la normativa internacional en la materia[5], la protección de datos presenta un triple ámbito de tutela, a partir de la acción normativa del Consejo de Europa, la Unión Europea y los Derechos nacionales.

---

2 Cerrillo, Agustí. (2007). Las tecnologías de la información y el conocimiento al servicio de la justicia iberoamericana en el siglo XXI. En: *«E-justicia» [monográfico en línea]. IDP. Revista de Internet, Derecho y Política*. N.º 4. UOC. (p. 5). Consulta 19 de abril de 2013 en: http://www.uoc.edu/idp/4/dt/esp/monografico.pdf.

3 Frente al carácter reaccional de la *privacy* anglosajona, el derecho a la protección de datos en Europa presenta un contenido prestacional. Martínez, Ricard. (2004). *Una aproximación crítica a la autodeterminación informativa*». Madrid: Thomson-Civitas. (p. 258).

4 Ordóñez, David. (2012). La protección de datos personales en la jurisprudencia europea después del Tratado de Lisboa. En Javier Díez-Hochleitner; Carmen Martínez; Irene Blázquez; Javier Frutos. *Últimas tendencias en la jurisprudencia del Tribunal de Justicia de la Unión Europea. (2008-2011)*. Las Rozas (Madrid): La Ley. (p. 141).

5 Entre otras, las directrices para la regulación de los archivos de datos personales informatizados, adoptadas mediante resolución 45/95 de la Asamblea General de Naciones Unidas, de 14 de diciembre de 1990 o las Directrices de la OCDE que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales, efectivas desde el 23 de septiembre de 1980.

La tutela del Consejo de Europa se articula a partir del Convenio 108 del Consejo de Europa sobre protección de Datos Personales de 28 de enero de 1981[6], completado con diversas recomendaciones sectoriales[7] e interpretado por la Jurisprudencia del Tribunal de Estrasburgo a partir de la sentencia *Leander c. Suecia* de 1987. El acervo jurisprudencial de Estrasburgo cristalizó, en el seno de la Unión Europea, en el desarrollo de una normativa específica y la consagración del derecho a la protección de datos en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea [8] (*DOCE* 18 de Diciembre de 2000). El texto de referencia es la 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 (*DOCE* 23 de noviembre de 1995), modificada por el Reglamento (CE) nº 1882/2003 del Parlamento Europeo y del Consejo de 29 de septiembre de 2003 (DOUE 21 octubre de 2003).

A partir del marco que proporciona la directiva, se dictaron diversos actos conexos que completaron la normativa en la materia[9]. La regulación que ofrece la directiva, sin embargo, no resulta homogénea, pues exige su previa trasposición por los Estados miembros. Asimismo favorecía la fragmentación, ya desde su origen, al excluir su aplicación en el ejercicio de actividades en ese momento comprendidas en el segundo y tercer pilar.

Este marco jurídico fue modificado por el Tratado de Lisboa que, al suprimir la tradicional división en tres pilares, permite homogeneizar la normativa sobre protección de datos. Así, el artículo 16 del Tratado de Funcionamiento de la Unión Europea (*DOUE* 30 de marzo de 2010) ha servido de base para la adopción de nuevas normas en la materia y, en particular, para la discusión de una Propuesta sobre Reglamento General de Protección de Datos[10] (en adelante, PRGPD), que sustituiría a la Di-

6 Este convenio está siendo objeto de un proceso revisión que culminará en una nueva redacción, ya muy avanzada. Cfr.: http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

7 Cfr.: http://www.coe.int/t/dghl/standardsetting/dataprotection/legal_instruments_en.asp

8 Sustituida por la Carta de Derechos Fundamentales de la Unión Europea de 12 de diciembre de 2007 *(DOUE* 14 diciembre) que ostenta el mismo carácter vinculante que los Tratados.

9 Entre otros, la 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 electrónicas, modificada en 2009. Cfr,: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm#amendingact (Consulta 22 de abril de 2013)

10 Propuesta COM (2012) 11 final de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, de 25 de enero de 2012. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:ES:PDF (Consulta 22 de abril de 2013).

rectiva[11] y que, al ser directamente aplicable en los Estados miembros, permitiría la aplicación homogénea y coherente del derecho de protección de datos (Considerando 8 de la PRGPD).

Respecto a los Derechos nacionales, es clásica la referencia al Derecho alemán, en cuyo seno se planteaba la existencia de un derecho de autodeterminación informativa. Esta reflexión doctrinal sirvió de base para su reconocimiento expreso por el Tribunal Constitucional Alemán en la Sentencia de la Ley del Censo de Población de 15 de diciembre 1983 (BVerfGE 65, 1 – Volkszählung)[12]. Y asimismo, sirvió de inspiración para su reconocimiento en Derecho español.

En España, el derecho a la protección de datos se ha configurado primero por la doctrina[13] y posteriormente por la jurisprudencia, a partir del artículo 18.4 de la CE, a cuyo tenor: «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». La CE consagra así la libertad informática[14] como derecho fundamental específico[15], cuyo desarrollo se regula por la vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter personal (en adelante, LOPD) y su reglamento aprobado por Real Decreto 1720/2007, de 21 de diciembre (en adelante, RLDPD). Tales normas se revisten de una garantía adicional: la tutela de la Agencia Española de Protección de Datos (en adelante, AEP), como autoridad de control.

La definición del derecho a la protección de datos se ha perfilado por el Tribunal Constitucional, especialmente en sentencias 290/2000 y 292/2000, ambas de 30 de noviembre[16], reconociendo su naturaleza de derecho fundamental autónomo respecto a los demás derechos del artículo 18 de la CE. Su especialidad respecto al derecho a la intimidad radica en la atribución a su titular de diversas facultades de control sobre

---

11 Cfr. Troncoso, Antonio (2012). «Hacia un nuevo marco jurídico europeo de la protección de datos personales». *Civitas. Revista española de derecho europeo*. Nº 43, p. 25-184.

12 Traducción por: Daranas, Manuel. (1984). Sentencia de 15 de diciembre de 1983: Ley del Censo. Derecho de la Personalidad y Dignidad Humana. *Boletín de Jurisprudencia Constitucional*, Madrid, Dirección de Estudios y Documentación del Congreso de los Diputados. Vol. IV, núm. 3, p. 126-170.

13 Es obligada la referencia a la obra: Lucas Murillo de la Cueva, Pablo (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos.

14 Pérez, Antonio Enrique, (1990). Los derechos humanos en la sociedad tecnológica. *Libertad informática y leyes de protección de datos personales*. Madrid: CEC, p. 133 -213. Asimismo, STC 254/1993, de 20 de julio.

15 Cuestión controvertida, expuesta brillantemente en: Martínez, Ricard (2004). *Op. cit.* Capítulos IV y V.

16 Con el precedente de las SSTC 134/1999, de 25 de julio y 144/1999, de 22 de julio.

sus datos personales[17], conocidas como derechos A.R.C.O.[18] y un cauce procedimental para obtener prestaciones positivas del Estado en su ejercicio. Dichas facultades vienen a concretar el contenido general del derecho, que incluye: i) Habeas data o control del uso de los datos y ii) el derecho de oposición al uso de datos con fines distintos al que justificó su obtención[19].

La jurisprudencia española define el objeto del derecho a la protección de datos en términos amplios, como cualquier tipo de dato personal, cuyo conocimiento o empleo por terceros pueda afectar los derechos de su titular[20]. Sin embargo, su ejercicio no es absoluto, pues puede someterse a restricciones, necesarias y proporcionadas, que respeten su contenido esencial (artículo 53 de la CE). Al respecto, la jurisprudencia española, enriquecida por las aportaciones del Tribunal de Estrasburgo, reconoce diversos límites a este derecho, entre otros, la seguridad del Estado, la persecución y castigo de delitos o el control en materia tributaria[21]. En todo caso, un adecuado examen del derecho a la protección de datos requiere la remisión a la amplia doctrina en la materia, limitándose el presente estudio a examinar las especialidades propias de los datos judiciales.

2. RÉGIMEN JURÍDICO DE LOS DATOS INCORPORADOS EN FICHEROS Y ARCHIVOS JUDICIALES

2.1. La creación de ficheros de datos judiciales y su régimen jurídico

La LOPD se aprobó con vocación de universalidad, por ello, los ficheros de datos de la Administración de Justicia se someten a la LOPD y su normativa de desarrollo. Así se deduce del artículo 230.5 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ), que consagra la competencia del Consejo General de Poder Judicial (en adelante, CGPJ) para determinar reglamentariamente los requisitos y condiciones que afecten al establecimiento y gestión de los ficheros automatizados bajo la

17 Martínez, Ricard, (2004). *Op. cit.,* p. 254-255.

18 Martínez, Ricard, (2007). El derecho fundamental a la protección de datos: perspectivas. III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. UOC. N.º 5. (p. 50). Consulta 19 de abril de 2013 en: http://www.uoc.edu/idp/5/dt/esp/martinez.pdf.

19 Reconocido, entre otras, en SSTC 254/1993, de 20 de julio (fundamento jurídico 7º); 11/1998, de 13 de enero (fundamento jurídico 4º) o 202/1999, de 8 de noviembre (fundamento jurídico 2º).

20 STC 292/2000, de 30 de noviembre (fundamento jurídico 6º).

21 Sentencia de 26 de marzo de 1987 (caso Leander) y sentencia de 25 de febrero de 1993 (caso Funke).

responsabilidad de los órganos judiciales, asegurando el cumplimiento de las garantías y derechos establecidos en la LOPD.

En el ejercicio de dicha competencia, el CGPJ aprobó una normativa específica en la materia, encabezada por el Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales (en adelante, RAE), aprobado por Acuerdo del Pleno del CGPJ de 15 de septiembre de 2005 (*BOE* 27 de septiembre de 2005). El RAE dedica su título V (artículos 86 a 97) a regular el establecimiento y la gestión de ficheros automatizados bajo la responsabilidad de los órganos judiciales. Y conforme a sus criterios, el Pleno del CGPJ aprobó el Acuerdo de creación de ficheros de carácter personal dependientes de los órganos judiciales de 30 de septiembre de 2006 (en adelante, ACF), publicado en el *BOE* de 12 de octubre de 2006.

Asimismo, la Comisión de Informática Judicial de 29 de marzo de 2007 aprobó el protocolo para la gestión del acceso a los usuarios a los servicios del Punto Neutro Judicial[22] que trae causa de la Instrucción 2/2003, de 26 de febrero, sobre el «Código de conducta para usuarios de equipos y sistemas informáticos al servicio de la Administración de Justicia»[23] y se complementa con el Protocolo a seguir ante el uso indebido de las consultas accesibles, adoptado por Acuerdo del Pleno del CGPJ de 26 de febrero de 2009[24]. La referencia al Punto Neutro Judicial no es baladí pues constituye una red de servicios que permite a los órganos judiciales el acceso directo a las bases de datos del CGPJ, organismos de la Administración General del Estado y otras instituciones. Se trata, por tanto, de la mayor base de datos personales de los ciudadanos.

Finalmente, el 13 de septiembre de 2007 el Pleno del CGPJ aprobó los «Criterios Generales de Seguridad en los sistemas de información al servicio de la Administración de Justicia»[25]. Criterios que se incorporaron al test de compatibilidad de los Sistemas Informáticos de Gestión Procesal para garantizar la homogeneidad de las medidas de seguridad. Una competencia modulada en los artículos 44 y 45 de la LUTICAJ que atribuyen al Comité Técnico estatal de la Administración judicial electrónica la competencia de definir las bases del Esquema Judicial de Interoperabilidad y Seguridad, sin perjuicio de las competencias del CGPJ como garante de la compatibilidad. Se atiende así al carácter poliédrico de la interoperabilidad[26] que exige la coordinación y coope-

22 Disponible en: www.poderjudicial.es (Consulta 18 de abril de 2013).

23 *BOE* 10 de marzo de 2003.

24 Disponible en: www.poderjudicial.es (Consulta 18 de abril de 2013).

25 Disponible en: http://www.poderjudicial.es/cgpj/es/Temas/e_Justicia/Documentacion_y_publicaciones (Consulta 24 de abril de 2013).

26 Cerrillo, Agustí. (2009). La interoperabilidad y la protección de datos. La interconexión de los registros y la protección de datos. En Pablo Lucas Murillo. *La Protección de datos en la administración electrónica.* Cizur Menor (Navarra): Aranzadi Thomson Reuters, p. 30.

ración de los diversos actores. Exigencia que se atiende con la estructura del Comité, integrado por representantes del Ministerio de Justicia, Comunidades Autónomas con competencias en la materia, CGPJ y Fiscalía General del Estado.

2.2. Los ficheros dependientes de los órganos judiciales y la protección de los datos que contienen

El artículo 87.1 del RAE distingue dos tipos de ficheros de datos personales dependientes de los órganos judiciales: jurisdiccionales y gubernativos. Una cuestión fundamental al respecto es la determinación de la responsabilidad, que se bifurca entre el responsable y encargado del tratamiento[27].

Los ficheros jurisdiccionales contienen los datos personales derivados de actuaciones jurisdiccionales. Son de dos tipos: de asuntos jurisdiccionales y de registro de asuntos.

a) En los ficheros de asuntos jurisdiccionales, el responsable del tratamiento es el órgano judicial que conoce del procedimiento si bien, precisa el ACF, su funcionamiento queda «bajo la dependencia directa del Secretario Judicial». Entendido el funcionamiento como la llevanza práctica del fichero, la doctrina considera que esta referencia carece de virtualidad, pues el funcionamiento del fichero opera automáticamente acorde a las directrices técnicas del responsable de su diseño. Así, el Secretario se limita a utilizarlo conforme a sus facultades[28], sin ostentar ninguna competencia decisoria al respecto.

b) En los ficheros de registro de asuntos, el responsable del tratamiento es el Secretario Judicial encargado del registro.

Los ficheros gubernativos contienen los datos personales derivados de procedimientos gubernativos y los definitorios de la relación funcionarial o laboral de las personas destinadas en tales órganos y de las situaciones e incidencias que en ella acontezcan. Son de dos tipos: ficheros propiamente gubernativos y ficheros de usuarios. Su responsable es el órgano gubernativo con competencia conforme a lo dispuesto en la LOPJ.

En todos los ficheros, el encargado del tratamiento será el Ministerio de Justicia en coordinación con el Gabinete Técnico de Información y Documentación del Tribunal

27 La AEP en R/02325/2009 (fundamento jurídico 9º) no sanciona al CGPJ como responsable del fichero por su creación, al entender que la normativa que ha aprobado en la materia demuestra su diligencia en orden a «concienciar e instruir a los usuarios de los sistemas informáticos de gestión judicial sobre como cumplir con la LOPD».

28 Rodríguez, María Teresa. (2011). «Protección de datos, ficheros judiciales y el secretario judicial». *Artículos doctrinales. Ilustre Colegio Nacional de Secretarios Judiciales.* Disponible en: http://coseju.com/articulos-doctrinales/item/599-proteccion-datos-ficheros-judiciales (consulta 12 de abril de 2013).

Supremo o la Administración competente en la dotación de medios, en su respectivo ámbito territorial.

La doble responsabilidad del responsable y encargado del tratamiento plantea especialidades, pues la vinculación de ambos sujetos, que regula la LOPD, no se traslada de forma perfecta al ámbito judicial. En efecto, el encargado del tratamiento se establece por la estructura competencial del Estado sobre gestión de la Administración de Justicia. Por tanto, no puede ser determinado por el responsable del tratamiento ni sometido a sus indicaciones, acorde al artículo 12.2 y 4 de la LOPD. En consecuencia, se somete a las indicaciones de los artículos 98 y siguientes del RAE, respondiendo de la adopción de medidas técnicas y organizativas que garanticen la seguridad de los datos[29].

En todo caso, el tratamiento de los datos judiciales presenta características específicas. Los datos personales de los sujetos implicados en un proceso se incorporan a los archivos judiciales sin necesidad del consentimiento inequívoco de los afectados (artículo 6.2 de la LOPD). Sin embargo, sus titulares mantienen su derecho a la autodeterminación informativa y pueden ejercer sus derechos de acceso, rectificación y cancelación en la sede del órgano judicial o gubernativo titular del fichero y ante el responsable del mismo (artículo 93 del RAE). Si bien, no pueden modificarse o cancelarse datos que reflejen hechos constatados en un procedimiento jurisdiccional o expediente gubernativo.

La incorporación no consentida de datos resulta especialmente significativa por su naturaleza pues, generalmente, son datos especialmente protegidos del artículo 7 de la LOPJ[30]. Por ello, su protección se garantiza con medias de seguridad de nivel medio-alto conforme al Título VII del RLOPD. Se trata así de reducir las posibilidades de divulgación indebida[31]. Esta exigencia se refuerza con el ACF, al exigir un nivel de seguridad alto para todos los ficheros, salvo los ficheros de usuarios.

3. EL PRINCIPIO DE PUBLICIDAD PROCESAL Y LA PROTECCIÓN DE LOS DATOS

3.1. Las facetas de la publicidad procesal

La CE consagra la publicidad procesal en sus dos facetas clásicas: interna, concretada en el derecho fundamental a un proceso público del artículo 24.2; y externa, que consagra el artículo 120.1 como principio de publicidad de las actuaciones judiciales, relacionado con la demanda de transparencia de la Justicia.

---

29 R/02338/2009 (fundamento jurídico 12º).

30 Datos sobre ideología, afiliación sindical, religión, creencias, origen racial o étnico, salud, vida sexual o comisión de infracciones penales o administrativas.

31 Mira, Corazón. (2010). *El expediente judicial electrónico*. Madrid: Dykinson S.L., p. 104.

La publicidad procesal así configurada, redefine sus términos en relación con el derecho a la protección de datos[32]. Así, el artículo 230 de la LOPJ, permite a los Juzgados y Tribunales utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y ejercicio de sus funciones[33] con las limitaciones previstas en la normativa de protección de datos. Y reconoce la validez y eficacia de los documentos emitidos si se garantiza el cumplimiento de los requisitos legales. En concreto, el artículo 31.2 de la LUTICAJ exige el cumplimiento de los requisitos de seguridad exigibles.

La referencia a la seguridad constituye el anclaje legal necesario para la garantía de la protección de datos judiciales, que depende del establecimiento de medidas de seguridad específicas. Más allá, el estudio de la publicidad externa excede los límites de este trabajo. Baste señalar que publicidad procesal, libertad de información y derecho a la protección de datos guardan un delicado equilibrio que ha suscitado controversia. Especialmente, respecto a la publicación de datos judiciales obtenidos en audiencia pública o la reutilización de datos que figuran en la publicación de sentencias no anonimizadas. Circunstancia que se agrava por la dificultad en el ejercicio del derecho de cancelación de los datos incorporados a la red. El conocido como derecho al olvido, en proceso de ser reconocido en la Unión Europea[34].

3.2. Protección de datos y publicidad procesal interna: el acceso a archivos y ficheros judiciales

El principio de publicidad procesal interna suele cumplirse mediante comunicaciones procesales[35]. Comunicaciones cuya práctica electrónica tiñe de sospecha de vulnerabilidad la protección de los datos anexados, si las medidas de seguridad resultan insuficientes para impedir divulgaciones indeseadas. En general, la protección de datos se garantiza con la adecuada regulación del acceso al expediente y la obtención de copias electrónicas, consagrados como derechos de ciudadanos y profesionales de la Justicia en los artículos 4.2 y 6.2 de la LUTICAJ. Estos derechos se reconocen a las partes o los sujetos con un interés legítimo[36], sin perjuicio de limitaciones excepcionales en caso de reserva de las actuaciones (artículo 232

32 Rodríguez, María Teresa (2010). Principio de publicidad procesal y derecho a la protección de datos de carácter personal: aproximación a la problemática actual en Juzgados y Tribunales españoles. *La Ley Penal: Revista de derecho penal, procesal y penitenciario*. Nº 71, p.74.

33 En las que se incluye la satisfacción del principio de publicidad procesal.

34 Cernada, Rosa (2013). Derecho al olvido judicial en la red. En Corredoira, Loreto; Cotino, Lorenzo. *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, (p. 521-541). Madrid: CEPC.

35 Almagro, José. (1984). *Constitución y proceso*. Barcelona: Editorial Bosch, p.246,

36 Exige acreditar una conexión concreta y singular con el objeto del proceso o algunos de sus actos procesales que constan en autos (STS 1227/1995, de 3 de marzo, fundamento jurídico 5º).

de la LOPJ) o prohibición de acceso a las sentencias (artículo 266.1 de la LOPJ). En todo caso, ambos derechos se ejercen mediante el acceso al expediente por parte del interesado[37] mediante comunicaciones judiciales clásicas o a través de la sede judicial electrónica.

3.2.1. Acceso al expediente judicial mediante comunicaciones judiciales clásicas

El principio de publicidad procesal interna se ejerce tradicionalmente mediante comunicaciones judiciales, bajo la responsabilidad del Secretario Judicial (artículos 234 y 235 de la LOPJ). Corresponde pues, al Secretario Judicial garantizar la protección de datos mediante la valoración de la condición de interesado, denegando el acceso cuando afecte a los derechos fundamentales de las partes o terceros que intervengan en el proceso[38]. La responsabilidad del Secretario Judicial ha sido criticada por la doctrina, al considerar que excede de su status jurídico[39] y puede suscitarle dudas, por ejemplo, respecto al acceso a datos de terceros no implicados en el proceso. Por ello, propone MIRA[40] que el control del acceso se efectúe *ratione materiae,* atendiendo a la naturaleza de la información, en lugar del solicitante y sus razones de interés legítimo.

En todo caso, siempre que actúe con la diligencia debida en el uso de los medios electrónicos, la responsabilidad del Secretario Judicial no alcanza al elemento técnico, del que responde la Administración competente en materia de Justicia. Esta bifurcación en la responsabilidad exige cuestionarse si el sistema de seguridad arbitrado impide un acceso o tratamiento no autorizado. Por ello, en la práctica, las comunicaciones se efectúan a través de *Lexnet*[41], que al hacer uso de sistemas de firma digital, garantiza la identidad del solicitante y la integridad y autenticidad de las informaciones. Sin embargo, al no ser *Lexnet* accesible para los ciudadanos, las medidas de seguridad del medio elegido por los particulares que no son parte en el proceso son fundamentales para garantizar la protección de datos.

3.2.2. Acceso al expediente judicial a través de la sede judicial electrónica

El acceso telemático al expediente judicial a través de la sede judicial electrónica se ejercita mediante un servicio electrónico de acceso restringido, previa identificación

37 Cotino, Lorenzo; Montesinos, Ana. (2012). Derechos de los ciudadanos y los profesionales en las relaciones electrónicas con la Administración de Justicia. En Eduardo Gamero; Julián Valero. *Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la ley 18/2011, de 5 de julio*. Cizur Menor, Navarra: Thomson Reuters-Aranzadi, p.204.

38 STS 8722/2006, de 18 de septiembre, (fundamento jurídico 8º).

39 Rodríguez, María Teresa (2010). *Op. cit*., p. 73-74.

40 Mira, Corazón. *Op. cit.,* p. 104.

41 Sistema informático creado por el Ministerio de Justicia para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos.

y autenticación (artículo 41 de la LUTICAJ). Asimismo, pueden incorporarse datos personales al expediente por la presentación de documentos a través del Registro electrónico de la subsede judicial electrónica.

La ventaja fundamental de estos sistemas es que no precisan la intervención del Secretario Judicial, de modo que la protección de datos se garantiza por el sistema de acceso, limitado a las partes y sus representantes[42]. Sin embargo, en este caso también se bifurca la responsabilidad sobre los datos, pues de la integridad y veracidad responde el órgano judicial (artículo 12 de la LUTICAJ[43]) o la parte que presenta el documento, pero de los elementos de seguridad (como los sistemas de autenticación), responde la Administración competente en materia de Justicia que gestiona la sede judicial electrónica (artículo 9 de la LUTICAJ).

3.2.3. El edicto electrónico como caso específico

La sede judicial electrónica constituye el medio para la publicación de los edictos, cuya práctica electrónica se regula como imperativa en el artículo 35 de la LUTICAJ. La naturaleza del edicto y su finalidad informativa impide el establecimiento de medidas de seguridad de acceso restringido, de forma que los datos necesariamente obrantes en el edicto pueden ser conocidos por cualquier usuario de la red. En ese caso, la protección de datos se asegura en dos momentos:

a) En sede jurisdiccional, por la incorporación de los datos estrictamente necesarios para el cumplimiento de la comunicación, con atención particular a los datos especialmente protegidos (artículo 7 de la LOPD) y los sujetos especialmente vulnerables, como menores o víctimas, omitiendo sus datos o cualquier referencia que pudiera permitir su identificación.

b) Publicado el edicto, la tutela se complica por la finalidad de la figura, destinada a publicitar la resolución que incorpora. Es por ello que, si bien el edicto electrónico no es una fuente accesible al público del artículo 3.j) de la LOPD[44], incorpora las resoluciones judiciales íntegras. En este sentido, su tratamiento como fuente no accesible al público a efectos de reutilización[45] resulta esencial para garantizar la protección de datos de los afectados.

---

42 La relación profesional entre abogados y procuradores y sus patrocinados implica la dación del consentimiento del afectado y la prohibición de aquéllos de divulgar los datos que conocen por su profesión.

43 Valero, Julián. (2012). La sede judicial electrónica. En Eduardo Gamero; Julián Valero. *Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la ley 18/2011, de 5 de julio*. Cizur Menor, Navarra: Thomson Reuters-Aranzadi, p. 235-238.

44 SAN, sección 1ª, de 18 de enero de 2007.

45 Dicho tratamiento se traduce en una exigencia alternativa para la reutilización: la obtención del consentimiento o la práctica de un proceso de anonimización.

4. EL CONTROL DEL DERECHO A LA PROTECCIÓN DE DATOS: EL EFECTO VENTILADOR

La tutela del derecho a la protección de datos en España se completa con una garantía institucional: la protección que brinda AEP[46], regulada en el título VI de la LOPD (artículos 35 a 42) y su Estatuto, aprobado por Real Decreto 428/1993, de 26 de marzo (en adelante EAEP).

La AEP es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia. Se configura pues, como una autoridad de control que, con carácter básicamente preventivo[47], tutela el derecho a la protección de los datos personales. El sistema de control es compartido, pues en general, la tutela de los derechos fundamentales transgredidos corresponde a los Tribunales[48]. Por ello, resulta esencial determinar las relaciones de la AEP con los Tribunales y su órgano de Gobierno.

En su relación con los Tribunales, se ha entendido que:

a) corresponde a la AEP, supervisar la aplicación de la normativa sobre protección de datos y ejercitar la potestad sancionadora ante las infracciones de la misma.

b) Corresponde a los Tribunales, la interpretación de las normas de protección de datos, la determinación de las indemnizaciones y el control de la actividad de la AEP, por la resolución de recursos contencioso-administrativos frente a las resoluciones del Director de la AEP.

Más compleja resulta la articulación de las relaciones entre la AEP y el CGPJ. Tradicionalmente, se consideró que la competencia del CGPJ para la creación y gestión de ficheros no abarcaba las funciones de control y tutela de la protección de datos, que correspondía a la AEP. Si bien, ambos órganos firmaron el 3 de mayo de 2010 un convenio de colaboración sobre inspección de órganos judiciales en materia de protección de datos[49]. Convenio que preveía la realización de inspecciones conjuntas, cuya efectividad garantizaba una Comisión de Seguimiento formada por representantes del CGPJ y la AEP.

---

46 Sin perjuicio de las funciones de las Agencias Autonómicas de protección de datos, cuyas relaciones con la AEP han sido analizadas, entre otras, en STC 290/2000, de 30 de noviembre.

47 STC 290/2000, de 30 de noviembre (fundamento jurídico 9º).

48 Lesmes, Carlos. (2012). Las potestades de fiscalización de la agencia española de protección de datos en el ámbito de la Administración de Justicia. *Revista de Jurisprudencia. El Derecho.* 1 de julio de 2012.

49 Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/convenios/conveniossectoriales/common/pdfs/CONVENIO_CGPJ_AEPD.pdf

Dicha *entente cordiale* se vio perturbada en 2011 por una sentencia del Tribunal Supremo[50] en la que desbroza las relaciones entre ambos órganos a partir de la definición de la AEP como verdadera Administración Pública. El Tribunal fundamentó su tesis en dos criterios:

a) Su régimen jurídico, pues conforme artículo 2.2 del EAEP, a falta de normativa sobre protección de datos, la AEP se rige supletoriamente por las normas de procedimiento de la Ley 30/1992, de 26 de noviembre para el ejercicio de sus funciones públicas y los preceptos aplicables de la Ley General Presupuestaria, Texto Refundido aprobado por Real Decreto Legislativo 1091/1988, de 23 de septiembre.

b) La naturaleza gubernativa del cargo del Director de la AEP, que goza de los mismos honores y tratamiento que los Subsecretarios, se sujeta a las incompatibilidades de los altos cargos y en su nombramiento, cesación y separación interviene el Gobierno (artículos 14 a 16 del EAEP).

Por ello, ante el mandato constitucional de independencia del Poder Judicial, el Tribunal Supremo sustrae las funciones de control y potestades de fiscalización y sanción de la AEP respecto de los órganos del Poder Judicial. En consecuencia, la AEP remitió al CGPJ los expedientes incoados en el ámbito de la Administración de Justicia. Sin embargo, el CGPJ no se mostró satisfecho con dicha doctrina y, por Acuerdo del Pleno de 31 de mayo de 2012[51], constituyó un grupo de trabajo para delimitar las competencias del CGPJ y la AEP y adecuar el Convenio a la nueva situación.

La reacción de ambos órganos responde a la ausencia de medios que acompaña el honor de la competencia. Circunstancia trágicamente clásica en la Administración de Justicia, y reflejada en las Disposiciones Adicionales de la LUTICAJ que establecen un plazo de cinco años para la efectiva dotación de medios electrónicos. Plazo que, en ausencia de mecanismos efectivos de exigencia, podría alargarse *sine die* bajo el amparo de la falta de disponibilidad o carencia de medios.

El realismo de este criterio no puede servir de válvula de escape a la efectividad del derecho a la protección de datos. Al efecto, el CGPJ analiza esta cuestión en su Informe de 6 de febrero de 2013[52] sobre Anteproyecto de Ley Orgánica de reforma del CGPJ, por la que se modifica la LOPJ[53]. Así, el artículo 560.19 de dicho Anteproyecto de Ley Orgánica atribuye al CGPJ «el ejercicio de las competencias propias de la autoridad de

50 Sentencia (Sala Tercera) 8497/2011, de 2 de diciembre (recurso de casación 2706/2008).

51 Fuente: www.poderjudicial.es (Consulta 24 de abril de 2013)

52 Disponible en: http://www.poderjudicial.es/cgpj/es/Poder_Judicial/Consejo_General_del_Poder_Judicial/Actividad_del_CGPJ/Informes

53 Disponible en: www.mjusticia.gob.es/cs/Satellite/1292366239349?blobheader=application%2Fpdf&blobheadername1=ContentDisposition&blobheadervalue1=attachment%3B+filename%3DANTEPROYECTO_DE_LEY_ORG%C3%81NICA_DE_REFORMA_DEL_CGPJ.pdf

control en materia de protección de datos respecto a la Administración de Justicia». Sin embargo, el CGPJ considera dicha interpretación excesivamente maximalista pues ignora las atribuciones de los órganos dependientes del Ministerio de Justicia en el diseño de la Nueva Oficina Judicial. Por ello, entiende que sus competencias como Autoridad de Control deberían circunscribirse «al efectivo gobierno del Poder Judicial, en concreto, en lo que afecta a la labor jurisdiccional o gubernativa de Jueces y Magistrados».

Si el CGPJ asume tales competencias, actuaría como autoridad de control en los términos de los artículos 46 a 54 de la PRGPD, que plantean problemas de encaje[54]:

a) Los artículos 47.3 y 48.2 exigen como requisitos de sus miembros: exclusividad, independencia, experiencia y aptitudes acreditadas para el ejercicio de sus funciones, particularmente, en la protección de datos personales.
b) Conforme al artículo 53, la consideración de autoridad de control conlleva la adopción de potestades sancionadoras, de las que carece en la actualidad el CGPJ.
c) Asimismo, la limitación en la potestad reglamentaria que propone el Anteproyecto de Reforma del CGPJ, no podría afectar a las materias propias de protección de datos, de acuerdo con el artículo 52 de la PRGPD, especialmente, respecto a la aprobación de normas vinculantes.

CONCLUSIONES

El proceso de informatización de la Justicia debe efectuarse con pleno respeto a las garantías procesales y los derechos fundamentales. Específicamente, exige el respeto a la normativa de protección de datos en materia de archivos y ficheros judiciales y de acceso a los datos a través de la sede judicial electrónica o mediante comunicaciones judiciales.

Esta normativa se aplica sin perjuicio de las especialidades derivadas del ejercicio independiente de la función jurisdiccional, que justifica dos matizaciones esenciales:

a) La competencia del CGPJ para la creación y determinación del régimen jurídico de los ficheros dependientes de los órganos judiciales.
b) La excepción al consentimiento para el tratamiento de datos de los archivos judiciales, sin perjuicio del ejercicio de los derechos ARCO. Circunstancia que, unida al carácter especialmente protegido de los datos, justifica la adopción de medidas de seguridad de nivel alto.

La tutela de la protección de datos en el ejercicio del derecho de acceso se garantiza mediante los sistemas de acceso restringido a la sede judicial electrónica y el control del

54 También modifica aspectos del proceso de reclamación. Así, el artículo 72 amplía la legitimación activa.

concepto de interesado por el Secretario Judicial. No obstante, en los edictos electrónicos, la protección vendría dada por la contención del órgano judicial en la plasmación de datos innecesarios y por la aplicación al edicto del tratamiento de fuente no accesible al público a efectos de reutilización.

En todo caso, la responsabilidad por vulneraciones en la protección de datos judiciales se bifurca en relación con las competencias sobre gestión de la Administración de Justicia, que modulan las relaciones entre responsable y encargado del tratamiento y apunta a un diverso responsable según la vulneración tenga su origen en un fallo de seguridad o un tratamiento excesivo.

La tutela del derecho a la protección de datos en la Administración de Justicia se garantiza en último término por la autoridad de control. Función que, de acuerdo con la última doctrina del Tribunal Supremo, corresponde al CGPJ en lo que respecta a la fiscalización de los Juzgados y Tribunales. La escasez de medios para el ejercido de dicha competencia ha propiciado un conflicto de competencias socavado, pues la AEP se vio (y, en cierto modo, se mostró) liberada de una competencia que el CGPJ no terminó de asumir. La solución a esta problemática es previsible que se adopte en el proyecto de reforma del CGPJ, que adopta la doctrina del Tribunal Supremo con un criterio amplio. Sin embargo, es de esperar que el legislador tenga muy presente las exigencias de la PRGPD respecto a la autoridad de control. Si la cuestión de la reforma del CGPJ y, en particular, del nombramiento de sus miembros, ha generado controversia, la exigencia de exclusividad y especialización en materia de protección de datos puede resultar la gota que colme el vaso. Sin embargo, la estudiada procrastinación a la que se ha visto sometida esta materia no podría extenderse en caso de incumplimiento de un Reglamento europeo. Ello exige un esfuerzo especial de cooperación entre los sujetos implicados. Un principio del que se hace eco la LUTICAJ y que, sin duda, va a ponerse a prueba en un aspecto tan delicado como esencial para el desarrollo de una verdadera justicia electrónica.

BIBLIOGRAFÍA

Almagro, José. (1984). *Constitución y proceso*. Barcelona: Editorial Bosch.

Cernada, Rosa (2013). Derecho al olvido judicial en la red. En Corredoira, Loreto; Cotino, Lorenzo. *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales* (p.521-541). Madrid: CEPC.

Cerrillo, Agustí. (2007). Las tecnologías de la información y el conocimiento al servicio de la justicia iberoamericana en el siglo XXI. En: *«E-justicia» [monográfico en línea]. IDP. Revista de Internet, Derecho y Política*. N.º 4. UOC. (p. 2-12). Fecha de consulta 8 de noviembre de 2012 en: http://www.uoc.edu/idp/4/dt/esp/monografico.pdf

Cerrillo, Agustí. (2009). La interoperabilidad y la protección de datos. La interconexión de los registros y la protección de datos. En Pablo Lucas Murillo. *La Protección de datos en la administración electrónica,* (p. 23-58). Cizur Menor (Navarra): Aranzadi Thomson Reuters.

Cotino, Lorenzo; Montesinos, Ana. (2012). Derechos de los ciudadanos y los profesionales en las relaciones electrónicas con la Administración de Justicia. En Eduardo Gamero; Julián Valero. *Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la ley 18/2011, de 5 de julio*. (p. 181-228). Cizur Menor, Navarra: Thomson Reuters-Aranzadi.

Daranas, Manuel. (1984). Sentencia de 15 de diciembre de 1983: Ley del Censo. Derecho de la Personalidad y Dignidad Humana. *Boletín de Jurisprudencia Constitucional*, Madrid, Dirección de Estudios y Documentación del Congreso de los Diputados. Vol. IV, núm. 3, p. 126-170.

Lesmes, Carlos. (2012). Las potestades de fiscalización de la agencia española de protección de datos en el ámbito de la Administración de Justicia. *Revista de Jurisprudencia. El Derecho.* 1 de julio de 2012.

Lucas Murillo de la Cueva, Pablo. (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos.

Martínez, Ricard. (2004). *Una aproximación crítica a la autodeterminación informativa*. Madrid: Thomson-Civitas.

– (2007). El derecho fundamental a la protección de datos: perspectivas. *III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas [monográfico en línea]. IDP. Revista de Internet, Derecho y Política. UOC.* N.º 5. (p. 47-51). Fecha de consulta: 6 de octubre de 2012. En: http://www.uoc.edu/idp/5/dt/esp/martinez.pdf

Mira, Corazón. (2010). *El expediente judicial electrónico*. Madrid: Dykinson S.L.

Mora, Manuela. (2012). Los registros judiciales electrónicos. En Eduardo Gamero; Julián Valero. *Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la ley 18/2011, de 5 de julio*. (p. 181-228). Cizur Menor, Navarra: Thomson Reuters-Aranzadi.

Ordóñez, David. (2012). La protección de datos personales en la jurisprudencia europea después del Tratado de Lisboa. En Javier Díez-Hochleitner; Carmen Martínez; Irene Blázquez; Javier Frutos. *Últimas tendencias en la jurisprudencia del Tribunal de Justicia de la Unión Europea. (2008-2011)*. (p. 137-170). Las Rozas (Madrid): La Ley.

Pérez, Antonio Enrique. (1990). Los derechos humanos en la sociedad tecnológica. *Libertad informática y leyes de protección de datos personales*. (p. 133-213). Madrid: CEC.

Rodríguez, María Teresa. (2010). Principio de publicidad procesal y derecho a la protección de datos de carácter personal: aproximación a la problemática actual en

Juzgados y Tribunales españoles. *La Ley Penal: Revista de derecho penal, procesal y penitenciario*. Nº 71, p. 73-80.

– (2011). «Protección de datos, ficheros judiciales y el secretario judicial». *Artículos doctrinales. Ilustre Colegio Nacional de Secretarios Judiciales.* Disponible en: http://coseju.com/articulos-doctrinales/item/599-proteccion-datos-ficheros-judiciales

Troncoso, Antonio. (2012). «Hacia un nuevo marco jurídico europeo de la protección de datos personales». *Civitas. Revista española de derecho europeo*. Nº 43, p. 25-184.

Valero, Julián. (2012). La sede judicial electrónica. En Eduardo Gamero; Julián Valero. Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la ley 18/2011, de 5 de julio. (p. 231-259). Cizur Menor, Navarra: Thomson Reuters-Aranzadi.

ANÁLISIS DE LA NORMATIVA EUROPEA SOBRE TRANSFERENCIA DE DATOS CONTENIDOS EN EL REGISTRO DE NOMBRES DE PASAJEROS (PNR) EN EL MARCO DE LA LUCHA CONTRA EL TERRORISMO INTERNACIONAL

Alicia Chicharro
Profesora contratada doctora de Derecho Internacional Público de la Universidad Pública de Navarra

RESUMEN: En la actualidad, el triunfo en la batalla contra fenómenos como el terrorismo internacional u otros delitos graves de carácter transnacional, requiere un fluido intercambio de información a escala mundial. En este ámbito se enmarcan los acuerdos que la Unión Europea ha venido concertando con terceros países, a fin de transferir datos personales de los pasajeros recabados por las aerolíneas e incluidos en el *Passenger Name Record* (PNR). Dichos compromisos, además de servir a la cabal finalidad apuntada, deberán respetar el nivel de protección de los datos de carácter personal y del derecho a la intimidad y a la privacidad que garantiza el Derecho de la Unión. Un equilibrio adecuado entre seguridad y respeto de los derechos fundamentales, requiere una respuesta global más estructurada que reduzca las divergencias no solo entre las normas internas, sino también entre los distintos acuerdos internacionales en la materia.

PALABRAS CLAVE: Transferencia de datos, terrorismo internacional, Derecho comunitario, PNR, Passenger Name Record.

1. INTRODUCCIÓN

En el contexto de la lucha contra el terrorismo internacional, la Unión Europea ha llevado a cabo diversos acuerdos con terceros Estados, como Estados Unidos, Canadá o Australia, con el objetivo de transferir datos personales de los pasajeros que tomen un avión o hagan escala en cualquier Estado miembro de la Unión con destino a cualquier aeropuerto situado en el territorio de esos países. Igualmente, se ha diseñado a nivel europeo un sistema que regula la retención, la transmisión y el procesamiento de esos datos, que ya ha sido desarrollado satisfactoriamente por la mayoría de las compañías aéreas.

La justificación de todas estas iniciativas legislativas y acuerdos internacionales se asienta en el carácter transnacional de un fenómeno como el terrorismo internacional y en la necesidad de cooperar para combatirlo con el intercambio de información tanto a nivel interno –autoridades de los Estados miembros, Europol, Eurojust y otras agencias europeas–, como a nivel internacional.

A pesar de servir a fines tan dignos de amparo como la erradicación del terrorismo o la delincuencia transnacional, algunos de los instrumentos concertados adolecen de

una falta de equilibrio con la protección de los datos de carácter personal, causando un grave quebranto al derecho a la intimidad, amparado tanto en la Carta de los Derechos Fundamentales de la Unión como en el Convenio Europeo de los Derechos Humanos[1].

A estas alturas nadie discute la conveniencia de disponer de un sistema armonizado de obtención de datos del PNR para toda la Unión, pero también es ineludible que ese sistema respete los principios fundamentales de las normas reconocidas en materia de protección de datos. Igualmente, los acuerdos internacionales que servirán de base a la transmisión de grandes cantidades de datos del PNR a terceros Estados, no pueden traspasar las líneas rojas que garantizan la vida privada de las personas en los Estados europeos, a la vez que deberían responder a un enfoque multilateral coordinado para que esos acuerdos con terceros países sean lo más parecidos posible.

2. ¿QUÉ ES EL PNR?

Las siglas PNR son el acrónimo de *Passenger Name Record*. Se trata de los ficheros creados por las compañías aéreas cada vez que un pasajero realiza una reserva. Los datos almacenados en estos ficheros permiten identificar fácilmente a cada pasajero y proporcionan ciertas informaciones útiles para las aerolíneas en sus relaciones con los clientes.

En realidad, los desplazamientos de las personas entre diferentes países suponen la recolección y el procesamiento de dos categorías de datos de carácter personal. Por una parte, los mencionados datos del PNR (*Passenger Name Records*) que se extraen y recogen de varios documentos de viaje, normalmente pasajes aéreos, y pueden incluir el nombre, la fecha de nacimiento, el número de teléfono, otras referencias de contacto como el domicilio, el número del pasaporte, la compañía aérea con la que se viaja, la agencia de viajes que hizo la reserva, la fecha y su identificador, número de tarjeta de crédito u otros apuntes sobre la forma de pago, el itinerario del viaje, el número de vuelo o vuelos, el asiento asignado, la referencia del equipaje y otros elementos[2]. Estos datos ya se recogían y almacenaban por las líneas aéreas antes del 11-S, aunque no a efectos policiales, sino comerciales.

Por otra parte, las aerolíneas también recogen los datos del APIS (*Advance Passenger Information System*), contenidos en los documentos de viaje, esto es, el nombre, la nacionalidad, el número de pasaporte o de documento nacional de identidad, la fecha y lugar de nacimiento y otros detalles sobre el desplazamiento. Se trata de datos oficiales que se incluyen en la parte de lectura óptica de los pasaportes, por tanto son más limitados que

1 Artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión y artículo 8 del Convenio Europeo de los Derechos Humanos.

2 Véase Dictamen 6/2002 del Grupo de Trabajo sobre Protección de Datos Artículo 29, de 24 de octubre de 2002, relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, WP 66.

los obtenidos a través del sistema PNR[3]. Además, esta información anticipada sobre los pasajeros se pone a disposición de las autoridades de aduanas, con el fin de mejorar los controles fronterizos y combatir la inmigración clandestina. Su empleo para otros fines represivos está permitido por la Directiva 2004/82/CE, por ejemplo, para identificar a sospechosos o a personas buscadas, pero se trata más de una excepción que de la regla.

Los datos del PNR, sin embargo, se utilizan principalmente como instrumento de investigación penal, más que como medio de control de identidad. Autoridades aduaneras y servicios de seguridad siempre han tenido acceso a este tipo de datos reclamándolos a las compañías aéreas, aunque su tratamiento era manual, relativo a un número restringido de vuelos y una vez realizado el desplazamiento. Hasta ahora no había sido tecnológicamente posible acceder a estos datos electrónicamente y por anticipado. En la actualidad, a través de un sistema *push*, las compañías aéreas realizan una transmisión anticipada de grandes cantidades de datos a las agencias relacionadas con la lucha contra delitos graves o, en el peor de los casos, usando el método *pull*, permiten el acceso a sus propias bases de datos a dichas agencias.

La gran masa de datos obtenida del PNR sirve para investigaciones en marcha sobre delitos ya cometidos o continuados en el tiempo, pero también para prevenir la perpetración de crímenes a través del análisis de determinados indiciadores de riesgo. Además, la búsqueda de personas contrastando diversas bases de datos, permite identificar a sospechosos y descubrir sus modelos de comportamiento general y de viaje, si los datos se conservan durante el tiempo adecuado.

3. ORIGEN DEL PROBLEMA EN TORNO A LA TRANSFERENCIA DE DATOS DE PASAJEROS

En 2001, en Estados Unidos se adoptó la *Aviation and Transportation Security Act* (ATSA), imponiendo a las compañías aéreas que operan vuelos hacia y desde dicho país la transmisión a las autoridades aduaneras competentes de los datos contenidos en el PNR. Esta obligación, en el caso de los ciudadanos europeos, entraba en clara colisión con la legislación comunitaria en materia de protección de datos, encabezada por la Directiva 95/46/CE[4].

La ATSA fue aprobada el 19 de noviembre de 2001, entre otras muchas medidas adoptadas a raíz de los atentados terroristas del 11-S. Es indudable que esta norma se enmarca

3 Artículo 3 de la Directiva 2004/82/CE del Consejo, de 29 de abril de 2004, sobre la obligación de los transportistas de comunicar datos de las personas transportadas, DO L 261, 6.8.2004.

4 Directiva 95/46/CE, 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, DO L 281, 23.11.1995, modificada por el Reglamento (CE) 1882/2003, DO L 284, 31.10.2003.

dentro del preocupante proceso de recorte de los derechos fundamentales al que venimos asistiendo desde la perpetración de diversos ataques terroristas en diferentes partes del globo.

Desde la Unión Europea, la Directiva 95/46/CE sobre protección de datos no permite a las compañías aéreas que realizan vuelos desde Europa transmitir datos del PNR a terceros países que no garanticen un nivel adecuado de protección de los datos de carácter personal. Igualmente, gracias a la adaptación de las legislaciones internas de los Estados miembros al contenido de esta Directiva, hoy en día los datos personales de los ciudadanos europeos cuentan con una protección equivalente en toda la Unión[5].

La Directiva otorga a la Comisión la facultad de determinar, sobre la base del procedimiento establecido en el artículo 25.6, si un país tercero garantiza o no un nivel adecuado de protección de los datos de carácter personal, «atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países»[6].

Si se comprueba que un tercer país no garantiza «un nivel adecuado de protección», los Estados miembros impedirán que se le transfieran datos personales. Como excepción se señala que podrá efectuarse dicha transferencia a un país tercero que no garantice un nivel de protección adecuado cuando sea necesaria o legalmente exigida para la salvaguardia de «un interés público importante». Parece que este concepto jurídico indeterminado incluiría las transmisiones requeridas para combatir el terrorismo internacional[7], aunque el Considerando 58º al aclarar el término sólo menciona las transferencias entre administraciones fiscales o aduaneras o los servicios de Seguridad Social. Por tanto, la transmisión es ilícita, a menos que se den unas condiciones de licitud, que son la existencia de un nivel de protección adecuado en el Estado de destino o, en defecto de tal nivel, una de las excepciones enumeradas en la propia Directiva.

---

5 Véase Téllez Aguilera, A. (2002). *La protección de datos en la Unión europea. Divergencias normativas y anhelos unificadores*, Madrid: Edisofer.

6 Artículo 25.2 Directiva 95/46/CE. El procedimiento para la adopción de estas decisiones aparece expresamente recogido en el artículo 31.2 de la Directiva con arreglo a la Decisión 468/1999 del Consejo, de 28 de junio (DO L 184, 17.7.1999) e implica: 1.- Propuesta de la Comisión dirigida al Comité al que se refiere el artículo 31.1 de la Directiva; 2.- Este Comité debe emitir un dictamen al respecto por mayoría cualificada; 3.- En caso de que el dictamen del Comité fuera favorable, la Comisión puede adoptar la decisión; sin embargo, en caso de que el dictamen del Comité no fuera favorable, la Comisión deberá aplazar su decisión por un plazo de tres meses y notificarlo al Consejo quien, en dicho plazo y por mayoría cualificada, podrá adoptar una decisión diferente.

7 Memoria de la Propuesta de Directiva presentada en 1992, COM (92) 422 final (LCEur 1992, 3472), DO C 311, 27.11.1992.

La Comisión ha anunciado la modernización de esta Directiva para responder a los nuevos desafíos tecnológicos[8]. Se trata de una propuesta que pretende poner en práctica el objetivo del Programa de Estocolmo relativo a la mejora de la protección de datos de los ciudadanos en todas las políticas de la Unión y en las relaciones con los socios internacionales[9].

En 2001 se dictó el Reglamento 2001/45/CE[10] que no solo asume todo el acervo comunitario en materia de protección de datos de carácter personal, sino que introduce algunas novedades destacables como el establecimiento de una autoridad europea independiente que controlará su cumplimiento (*Supervisor Europeo de Protección de Datos*) y la posibilidad de apelar, inicialmente ante dicha autoridad y, después, en vía de recurso ante el Tribunal de Justicia.

En relación con el intercambio de información entre los propios Estados miembros, el sistema Schengen[11] posee un sistema de información (SIS), que permite la mejora de la coordinación policial y la cooperación judicial para controlar el flujo transfronterizo de datos de carácter personal en relación con investigaciones criminales de conformidad con el Convenio Nº 108 del Consejo de Europa[12] y de su Protocolo adicional de 2001[13], y la Recomendación (87) 15 del Comité de Ministros a los Estados miembros en rela-

---

8 Comunicación de la Comisión, de 20 de abril de 2010, Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos – Plan de acción por el que se aplica el Programa de Estocolmo, COM (2010) 171 final.

9 Consejo Europeo, Programa de Estocolmo: una Europa abierta y segura que sirva y proteja al ciudadano, doc. 17024/09, 2 de diciembre de 2009.

10 Reglamento (CE) 45/2001, 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 órganos comunitarios y a la libre circulación de estos datos, DO L 8, 12.1.2001. Véase Rebollo Delgado, L. (2008). *Vida privada y protección de datos en la Unión Europea*, Madrid: Dykinson.

11 El acervo de Schengen procede del Acuerdo Schengen de 14 de junio de 1985 y fue definido por la Decisión 1999/435/CE del Consejo, de 20 de mayo de 1999. Se incorporó a los tratados a través del Protocolo Schengen anejo al Tratado de la UE y al Tratado constitutivo de la Comunidad Europea.

12 Convenio Nº 108 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. Entró en vigor el 1 de octubre de 1985. Véase García Aguilar, N. (1999). Origen y significado del Convenio 108 del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. *Revista Internauta de Práctica Jurídica*, 2, 1-22.

13 Protocolo Adicional, de 8 de noviembre de 2001, al Convenio Nº 108 del Consejo de Europa. Entró en vigor el 1 de julio de 2007. Sobre el contenido de este Protocolo, véase el análisis que realiza Pavón Pérez, J. (2001-2002). La protección de datos personales en el Consejo de Europa: el Protocolo Adicional al Convenio 108 relativo a las autoridades de control y a los flujos transfronterizos de datos personales. *Anuario de la Facultad de Derecho de la Universidad de Extremadura*, 19-20, 235-252.

ción con la utilización policial de datos de carácter personal[14]. En la regulación relativa al Sistema de Información Schengen (SIS) se establece el principio de que las partes sólo podrán utilizar los datos con los fines enunciados para cada una de las descripciones que se mencionan. Sin embargo, existe la posibilidad de excepciones aduciendo diversos motivos, como la amenaza inminente para el orden y la seguridad públicos, razones serias de seguridad del Estado o la prevención de un hecho delictivo grave, donde evidentemente se enmarca el terrorismo internacional[15].

En resumen, la Unión Europea es consciente de la importancia de los datos del PNR en la lucha contra el terrorismo y otras formas graves de delincuencia, pero también de la necesidad de asegurar un nivel adecuado de protección de los datos de los pasajeros. Por ello, las transferencias de datos contenidos en el PNR deben respetar las normas europeas que protegen los datos de carácter personal, en cuya cúspide se sitúa su reconocimiento en la Carta de los Derechos Fundamentales de la Unión.

Ante este panorama, cuando los Estados Unidos, Canadá y Australia pidieron a las compañías aéreas que les transmitieran datos del PNR sobre vuelos con destino a sus países, no supieron cómo responder, ya que si obedecían el mandato estaban quebrantando la normativa europea y si no lo hacían, podían sufrir no solo sanciones sino también represalias comerciales por parte de los Estados solicitantes. Con el fin de sacar de este atolladero a las aerolíneas, la Unión Europea reaccionó con celeridad negociando y firmando acuerdos internacionales separados con cada uno de los tres países. Dichos acuerdos proporcionaron la base jurídica para la transferencia de datos del PNR fuera de la Unión a los servicios de seguridad de los terceros Estados. Como se observa, hasta hoy la celebración de este tipo de convenios se ha resuelto caso por caso, pactando acuerdos bilaterales que tratan de cuestiones comunes y regulan la misma materia, pero cuyas disposiciones no son idénticas.

4. ACUERDOS CELEBRADOS POR LA UNIÓN EUROPEA CON TERCEROS PAÍSES

4.1. Vicisitudes del anhelado acuerdo entre la Comunidad Europea y Estados Unidos

La incompatibilidad entre las exigencias que la ATSA impone a las compañías aéreas y la protección que la normativa europea garantiza a los datos de carácter personal se puso de relieve inmediatamente. De un lado, las aerolíneas se enfrentaban a fuertes sanciones e incluso al riesgo de ver retirados sus derechos de aterrizaje en Estados Unidos

14 Recommendation Nº R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, 410th meeting, 17 September 1987.

15 Artículo 102 del Acuerdo Schengen.

si no cumplían con lo preceptuado en la ATSA; mientras del otro, la transferencia sin más de la información contenida en el PNR violaba claramente la normativa europea, pudiendo ser objeto de múltiples recursos judiciales en los diferentes Estados miembros.

Para salir momentáneamente del paso en 2003, la Comisión Europea y Estados Unidos realizaron una Declaración conjunta, donde se reconocía expresamente la incompatibilidad entre las legislaciones de ambos lados del Atlántico y donde, en definitiva, la Comisión claudicaba ante las autoridades americanas asegurando que las compañías aéreas que transmitieran los datos conforme a la ATSA no serían sancionadas ni a la luz del Derecho comunitario ni en virtud de las disposiciones nacionales incumplidas[16].

En este instrumento *sui generis* al que se denomina Declaración conjunta, ambas partes se mostraban de acuerdo en trabajar para la consecución de un acuerdo bilateral que permitiera a la Comisión adoptar una decisión conforme al artículo 25.6 de la Directiva 95/46/CE[17]; luego el propio texto de la Declaración no es tal «acuerdo bilateral», aunque en la misma se llegue a excluir la prohibición de acceso a datos garantizada por la normativa europea[18].

El 1 de marzo de 2004, la Comisión sometió a la consideración del Parlamento Europeo el proyecto de decisión sobre el carácter adecuado de la protección de los datos, al que se adjuntaba una propuesta de compromisos a pactar con Estados Unidos. En su respuesta, el Parlamento estimó que el proyecto de decisión sobrepasaba las competencias atribuidas a la Comisión en virtud del artículo 25 de la Directiva 95/46/CE. Además, propuso que se negociara un acuerdo internacional adecuado que respetara los derechos fundamentales en relación con diversos aspectos, presionando así a la Comisión para que le sometiera un nuevo proyecto de decisión. Asimismo, se reservó el derecho a pedir al Tribunal de Justicia que comprobase la legalidad del acuerdo internacional proyectado y, en particular, su compatibilidad con la protección del derecho a la intimidad.

A su vez, el 17 de marzo de 2004, la Comisión remitió al Parlamento Europeo una propuesta de decisión del Consejo relativa a la celebración de un Acuerdo con Estados Unidos, relativo a la transferencia de datos sobre pasajeros de aerolíneas[19].

---

16 Véase Argomariz, J. (2009). When the EU is the 'Norm-taker': The Passenger Name Record Ageerment and the EU's Internalization of the US Border Security Norms. *European Integration*, 31(1), 119-136.

17 Muñoz, R. (2004). La protection des données des passagers. *Revue du Droit de l'Union européenne*, 4, 771-784.

18 Sobre la controvertida naturaleza de la Declaración conjunta Comisión-Estados Unidos, de 17-18 de febrero de 2003, véase Alcoceba Gallego, M.A. (2004). El acceso de las autoridades norteamericanas a datos de pasajeros de compañías aéreas europeas: reflexiones sobre la Declaración conjunta Estados Unidos-Comisión Europea. *Noticias de la Unión Europea*, 230, 53-56.

19 El Consejo invocó el procedimiento de urgencia y le dio al Parlamento la fecha límite del 22 de abril de 2004 para emitir su dictamen conforme al artículo 300.3 TCE. Sin embargo, el

El 14 de mayo de 2004, la Comisión adoptó la Decisión sobre el carácter adecuado de la protección[20], mientras el 17 de mayo de 2004 el Consejo acordó la Decisión 2004/496/CE[21], anexo a la cual se encontraba el Acuerdo entre la Comunidad Europea y Estados Unidos sobre el tratamiento y la transferencia de los datos del PNR. Ambas Decisiones fueron recurridas por el Parlamento Europeo ante el Tribunal de Justicia, dando lugar a los asuntos C-318/04 y C-317/04. El Tribunal estimó pertinentes los recursos y anuló las dos Decisiones[22].

El Acuerdo anulado garantizaba a la Oficina de aduanas y protección de fronteras estadounidense el acceso electrónico a los datos de los expedientes de los pasajeros procedentes de los sistemas de control de reservas/salidas situados en el territorio de los Estados miembros de la Unión, solo hasta que se hubiera establecido un sistema satisfactorio de transferencia de esos datos por las compañías aéreas[23]. Las compañías que efectuaran vuelos de pasajeros en líneas de transporte aéreo con el extranjero con punto de origen o de destino en los Estados Unidos tratarían los datos de los expedientes de los pasajeros incluidos en sus sistemas informatizados de reserva con arreglo a la legislación americana[24].

Tras la sentencia del Tribunal de Justicia de 30 de mayo de 2006, el Consejo y la Comisión notificaron al Gobierno de los Estados Unidos, con arreglo al punto 7 del

---

Parlamento desestimó la urgencia y atribuyó a una comisión la elaboración del informe sobre la propuesta de decisión del Consejo.

20 Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos, DO L 235, 6.7.2004.

21 Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de Seguridad Nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos, DO L 183, 20.5.2004.

22 STJCE de 30 de mayo de 2006, *Parlamento Europeo v. Consejo de la Unión Europea y Parlamento Europeo v. Comisión Europea*, asuntos acumulados, C-317/04 y C-318/04, DO C 178, 29.7.2006. El Tribunal constató que la Comisión había utilizado una base jurídica inadecuada al elegir el artículo 95 TCE en relación con el artículo 25 de la Directiva 95/46/CE, ya que los tratamientos de datos a que se refiere no están comprendidos en el ámbito de aplicación de la Directiva, y anuló el Acuerdo. Véase Méndez, M. (2007). Annulment of Commission Adequacy Decision and Council Decision Concerning Conclusion of Passenger Name Record Agreement with US Grand Chamber Judgment of 30 May 2006. *European Constitutional Law Review*, 3, 127-147.

23 Punto 1 del Acuerdo UE-EEUU de 2004.

24 Punto 2 del Acuerdo UE-EEUU de 2004. *The Privacy Act* 1974 (as amended). Véase Tanaka, H., Bellanova, R., Ginsburg, S., De Hert, P. (2010). *Transatlantic Information Sharing: At a Crossroads*. Washington DC: Migration Policy Institute.

Acuerdo que el mismo debía derogarse con efecto a partir del 30 de septiembre de 2006. La Comisión y las agencias estadounidenses implicadas volvieron a negociar un acuerdo provisional que se aplicó desde octubre de 2006 hasta el 31 de julio de 2007[25], cuando fue sustituido por un acuerdo definitivo.

Este Acuerdo provisional de 2006 era menos preciso en cuanto a los datos objeto de tratamiento y transferencia, ampliaba el número de autoridades norteamericanas facultadas para el tratamiento de los datos del PNR y mantenía un método de transferencia no discriminatorio de los mismos, con lo que resultaba más susceptible de abusos que el pactado en 2004.

En 2007, se firmó un nuevo Acuerdo entre la Unión Europea y Estados Unidos que se aplicó de manera provisional hasta que finalmente se logró que el nuevo acuerdo mejorado de 14 de diciembre de 2011 pasase la criba de la Eurocámara. La Decisión del Consejo incluye el texto del Acuerdo y una carta de las autoridades estadounidenses dirigida a la Unión donde se explican las modalidades de almacenamiento, uso y transferencia de datos del PNR por parte del Departamento de Seguridad del Territorio Nacional[26].

Los datos obtenidos de las compañías aéreas se utilizarían «con el propósito de prevenir y combatir: a) el terrorismo y los delitos asociados, 2) otros delitos graves de carácter transnacional, incluida la delincuencia organizada, y 3) la fuga en caso de orden de arresto o pena de reclusión por los delitos anteriormente mencionados». Además, las autoridades norteamericanas podían atesorar y procesar los datos del PNR con el fin de proteger «los intereses vitales del interesado o de otras personas, o en todo procedimiento judicial penal, o cuando lo exija la ley» [27].

Los eurodiputados criticaron duramente este Acuerdo de 2007. Se apuntó que dejaba importantes lagunas en materia de seguridad jurídica, protección de datos y derecho de recurso para los ciudadanos de la Unión, «en particular debido al carácter general y vago de las definiciones y las numerosas excepciones previstas». En este mismo sentido, el Grupo de Trabajo del artículo 29 señaló que «los fines que justifican la transferencia

25 Decisión 2006/729/JAI del Consejo, de 16 de octubre de 2006, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos del registro de nombres de pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, DO L 298, 27.10.2006.

26 Decisión 2007/551/PESC/JAI del Consejo, de 23 de julio de 2007, relativa a la firma, en nombre de la Unión Europea, de un Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos del registro de nombres de pasajeros (PNR) por las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, DO L 204, 4.8.2007.

27 Título I de la Carta del DHS a la UE adjunta a la Decisión 2007/551/PESC/JAI del Consejo, de 23 de julio de 2007.

de datos, incluidas las numerosas excepciones, no están lo suficientemente especificados y sobrepasan los contemplados por la normativa sobre protección de datos»[28].

Por lo que se refiere a los campos de datos que se transferían, el Acuerdo de 2007 reducía la cantidad a 19 frente a los 34 del Acuerdo de 2004[29]. El Parlamento Europeo señaló que dicha reducción era más bien «cosmética», ya que se debía a la fusión y al renombramiento de campos de datos, y no a una verdadera supresión. El Pleno manifestó además su preocupación porque se facilitasen datos sensibles.

Con el Acuerdo de 2007, aumentaron las autoridades norteamericanas autorizadas para la recepción y tratamiento de los datos del PNR. Recordemos que el Acuerdo de 2004 identificaba un número limitado de organismos dentro del Departamento de Seguridad del Territorio Nacional. Sin embargo, el Acuerdo de 2007 establecía que el responsable del procesamiento de tales datos era dicho Departamento, sin precisar los organismos específicos facultados, con lo que en la práctica se ampliaba el número de agencias que podían acceder a los datos de carácter personal de los pasajeros. Dada esta ampliación, el Parlamento Europeo se mostró a favor de la aplicación de la legislación de Estados Unidos sobre protección de la intimidad a los ciudadanos de la Unión, con el fin de que las entidades autorizadas se vieran compelidas a respetar dicha normativa en el tratamiento de sus datos personales. Sin embargo, llamó la atención sobre la persistencia de contradicciones entre el Derecho europeo y la legislación norteamericana en torno al tratamiento de datos personales.

En cuanto al tiempo de retención de los datos del PNR se ampliaba de tres años y medio a quince años, divididos en un período «activo» de siete años y un período «latente» de ocho años[30]. La Eurocámara criticó esta prórroga y que no se ofrecieran garantías sobre la destrucción definitiva de tales datos tras la conclusión de ese período total de 15 años de conservación. Asimismo, a los eurodiputados les preocupaba que la conservación durante siete años en «bases de datos analíticas activas», pudiera conllevar un importante riesgo de creación de perfiles y extracción de datos a gran escala, práctica incompatible con los principios esenciales europeos y cuestión todavía debatida en el propio Congreso de Estados Unidos.

Un cambio muy saludado respecto al Acuerdo de 2004, consistía en la adopción del sistema de transferencia *push*, frente al denominado sistema *pull*, que solo se mantiene para el caso de que las compañías aéreas no puedan emplear el método *push*. De esta manera, las autoridades norteamericanas no tenían acceso directo a los datos del

28 Dictamen 5/2007 del Grupo de Trabajo del artículo 29, relativo al nuevo Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por parte de las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, celebrado en julio de 2007.

29 Título III de la Carta del DHS a la UE.

30 Título VII de la Carta del DHS a la UE.

PNR, esto es a las bases de datos de las compañías aéreas, sino que eran estas últimas las encargadas de enviar esos datos a las agencias estadounidenses. Con este significativo cambio se consiguió frenar una invasión excesiva en la esfera de privacidad de los pasajeros, aunque la aplicación subsidiaria del sistema *pull* podía seguir acarreando algunos problemas.

En definitiva, el Acuerdo de 2007 supuso ciertas mejoras respecto al de 2004 en relación con el número de datos transferibles, la adopción del sistema *push* y la previsión de revisiones periódicas del Acuerdo. Sin embargo, aún quedaban algunas aristas por pulir si se quería garantizar una adecuada protección de los datos de carácter personal transmitidos a los servicios de seguridad norteamericanos[31].

4.2. Nuevo Acuerdo mejorado de 2011 entre la Unión Europea y Estados Unidos sobre transferencia de datos del PNR

Siguiendo las indicaciones de la Resolución del Parlamento Europeo, de 5 de mayo de 2010, en la que instaba al inicio de las negociaciones para los acuerdos relativos al registro de los nombres de los pasajeros (PNR) con los Estados Unidos, Australia y Canadá[32], el 14 de diciembre de 2011, la Unión Europea y Estados Unidos firmaron un nuevo Acuerdo, que finalmente fue aprobado por el Parlamento Europeo el 19 de abril de 2012[33].

Los datos obtenidos de las compañías aéreas se recopilarán, utilizarán y tratarán con el fin de prevenir, detectar, investigar y enjuiciar: a) el terrorismo y los delitos relacionados, b) otros delitos sancionados con una pena de tres o más años de privación de libertad y que sean de carácter transnacional. En el primer apartado, se especifica qué se entiende por «delitos relacionados» y, en el segundo, qué se considerará delito de «carácter transnacional»[34]. A pesar de este ejercicio de concreción, lo cierto es que el Acuerdo de 2011 sigue incluyendo términos demasiado generales y definiciones excesivamente vagas, con numerosas excepciones, lo que redunda en un riesgo tangible para la adecuada protección de los datos personales de los ciudadanos europeos.

---

31 Véase Tukdi, I. (2008-2009). Transatlantic Turbulence: The Passenger Name Record Conflict. *Houston Law Review*, 45(2), 587-620.

32 Decisión del Consejo, de 13 de diciembre de 2011, relativa a la celebración del Acuerdo entre la Unión Europea y Australia sobre tratamiento y transferencia de datos del registro de nombres de los pasajeros (PNR) por los transportistas aéreos al Servicio de Aduanas y de Protección de las Fronteras de Australia, DO L 186, 14.7.2012.

33 Decisión del Consejo, de 26 de abril de 2012, relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, DO l 215, 11.8.2012.

34 Artículo 4 del Acuerdo UE-EEUU de 2011.

En este nuevo Acuerdo se mantiene la lista de 19 campos de datos transferibles, haciendo caso omiso a las advertencias del Parlamento Europeo en cuanto a su desproporción respecto a los fines perseguidos. Por lo que respecta a los datos sensibles, es decir, datos sobre el origen racial o étnico, ideología política, creencias religiosas o filosóficas, afiliación sindical y datos sobre la salud o la vida sexual de las personas[35], el Departamento de Seguridad del Territorio Nacional utilizará sistemas automatizados para filtrarlos y enmascararlos. Se garantiza que solo se utilizarán en circunstancias excepcionales que puedan poner en riesgo o en grave peligro la vida de una persona y serán suprimidos permanentemente en los 30 días siguientes a la última recepción del PNR que los contenga. No obstante, podrán conservarse durante el tiempo especificado en la legislación estadounidense para realizar una acción específica de investigación, enjuiciamiento o ejecución[36]. Esto significa que desde el punto de vista cualitativo la transferencia de datos a las autoridades de Estados Unidos continúa siendo demasiado amplia y no resultaba proporcional a los objetivos perseguidos por el Acuerdo.

Respecto al método de acceso a los datos del PNR, la regla general será la utilización del sistema *push*, obligando a las aerolíneas a adoptarlo a más tardar a los 24 meses de la entrada en vigor del Acuerdo. No obstante, excepcionalmente se podrá «solicitar a las compañías que faciliten de otro modo el acceso», luego se sigue dejando abierta la puerta a servirse del método *pull*, cuando las líneas aéreas no sean capaces de responder a su debido tiempo a las peticiones de las autoridades norteamericanas.

Una novedad poco significativa en la práctica se refiere al tiempo de retención de los datos: se prevé un período «activo» que se rebaja a cinco años y un período «latente» que aumenta a diez años[37], aunque el plazo total continúe siendo de 15 años.

Por otra parte, se asegura que la transmisión ulterior de los datos del PNR a las autoridades públicas de terceros países solo se hará para contribuir a los casos que sean objeto de examen o investigación y, como ya exigía el Acuerdo de 2007, en base a compromisos que prevean una protección de la intimidad de los datos personales comparable a la que aplica el Departamento de Seguridad del Territorio Nacional a los PNR.

Sin embargo, el Acuerdo sigue mostrando algunas de las deficiencias de las que ya adolecía su predecesor, como son la falta de concreción de los fines a conseguir con la transferencia de datos, la carencia de discriminación entre datos pertinentes y otros especialmente sensibles, la no identificación clara de las autoridades facultadas para recibir y tratar los datos, el pequeño resquicio dejado al sistema *pull* y, por último, en general la escasa permeabilidad

35 En este sentido, véase la Resolución del Parlamento Europeo, de 12 de julio de 2007, sobre el Acuerdo PNR con los Estados Unidos de América (Textos aprobados, P6_TA (2007) 0347).

36 Artículo 6 del Acuerdo UE-EEUU de 2011.

37 Título VII de la Carta del DHS a la UE.

del texto del Acuerdo a los principios firmemente asentados en la Unión en materia de protección de datos personales y preservación del derecho a la intimidad.

A pesar de que, como señaló el Supervisor Europeo de la Protección de Datos, el nuevo Acuerdo revisado entre la Unión y Estados Unidos no había cumplido prácticamente con ninguna de las sugerencias efectuadas por el Parlamento Europeo[38], éste finalmente lo aprobó, entrando en vigor el 27 de abril de 2012.

Desde la Dirección General de libertad, seguridad y justicia de la Comisión Europea, Jonathan Faull confió en que en esta ocasión fuera un acuerdo definitivo de siete años de duración y añadió que en su opinión cumplía los criterios tanto de seguridad como de protección de los datos individuales.

4.3. Acuerdo de 2005 sobre la transferencia de los datos API/PNR entre la Unión Europea y Canadá

En 2005, la Comunidad Europea suscribía con Canadá un acuerdo sobre la transferencia de datos de los pasajeros de líneas aéreas que se dirigiesen a aeropuertos situados en territorio canadiense[39]. Este nuevo instrumento internacional que entró en vigor el 22 de marzo de 2006, ha sido menos criticado que los acuerdos logrados a lo largo de estos años con Estados Unidos.

Ello se debe singularmente a una actitud por parte de las autoridades canadienses más abierta a la conciliación entre seguridad y protección de la intimidad. Asimismo, Canadá cuenta con un sistema legislativo de protección de la privacidad y los datos de carácter personal, que frena cualquier intento de injerencia en la intimidad de los pasajeros que no tenga una justificación apropiada en la consecución de fines superiores. Concretamente, la Ley canadiense de protección del derecho a la intimidad otorga a las personas físicas los derechos de acceso, rectificación y oposición respecto a toda la información que les concierna[40], derechos de los que también dispondrán los pasajeros cuyos datos se transmitan a Canadá. Además, una autoridad independiente, el Comisario de Datos, se encarga de vigilar el tratamiento de los datos por parte de las autoridades canadienses.

---

38 Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, 9 December 2011.

39 Acuerdo entre la Comunidad Europea y el Gobierno de Canadá, firmado en Luxemburgo el 3 de octubre de 2005, sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros y de los expedientes de pasajeros, DO L 82, 21.3.2006.

40 *Canadian Privacy Act 1983*. Véase también *Personal Information Protection and Electronic Documents Act 2000*.

El Acuerdo establece que la transferencia y tratamiento de los datos personales API/PNR provenientes de la Unión Europea estarán regulados por las condiciones establecidas en los «compromisos»[41] de la Agencia de Servicios de Fronteras de Canadá (*Canada Border Services Agency*), en relación con su programa sobre PNR, así como por la legislación nacional canadiense sobre la materia.

Durante el proceso de negociación, la propuesta de acuerdo fue sometida a dictamen del Grupo de Trabajo del artículo 29, donde se puso de manifiesto que algunas disposiciones atentaban contra el derecho a la privacidad y a la protección de datos personales[42]. Las autoridades europeas hicieron llegar sus reservas a las canadienses, quienes finalmente aceptaron los puntos de vista de la Unión, modificándose la propuesta original.

En cuanto a los datos a transferir, el Acuerdo establece una lista de 25 elementos, de la cual se excluyen los datos sensibles. Además las categorías son concretas, evitando la confusión que pueden originar las «categorías abiertas» con las que se corre el riesgo de incluir también «aspectos sensibles de la conducta de los pasajeros y de las personas que los acompañan»[43]. Así, lo han puesto de manifiesto tanto el Parlamento Europeo, como el Grupo de Trabajo del artículo 29[44] y el Supervisor Europeo de Protección de Datos[45].

Las autoridades canadienses recibirán esos datos aplicando el método *push*, para lo cual se ha creado un Sistema de Información de Pasajeros, denominado PAXIS, a través del cual las compañías aéreas envían los datos de la API y del PNR a la Agencia de Servicios de Fronteras de Canadá. Esto significa, que las autoridades canadienses en ningún

41 Decisión 2006/253/CE de la Comisión, de 6 de septiembre de 2005, relativa al carácter adecuado de la protección de datos personales incluidos en los registros de nombres de los pasajeros (PNR) que se transfieren a la Canada Border Services Agency, DO L 91, 29.3.2006. En el Anexo de esta Decisión se incluyen los «compromisos» de la Agencia Servicios de Fronteras de Canadá en relación con la aplicación de su Programa de PNR.

42 Dictamen 3/2004 del Grupo de Trabajo del artículo 29, de 11 de febrero de 2004, sobre el nivel de protección garantizado por Canadá para la transmisión de datos de pasajeros y de la información avanzada de pasajeros de las compañías aéreas.

43 Informe Final A6-0226/2005 del Parlamento Europeo, de 4 de julio de 2005, sobre la Propuesta de Decisión del Consejo relativa a la celebración de un Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre el tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros (API) y de los expedientes de los pasajeros (PNR), COM (2005) 0200.

44 Dictamen 1/2005 del Grupo de Trabajo del artículo 29, de 19 de enero de 2005, sobre el nivel de protección garantizado por Canadá para la transmisión del PNR e información previa sobre pasajeros procedente de las compañías aéreas.

45 Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Consejo relativa a la celebración de un Acuerdo entre la Comunidad Europea y el Gobierno de Canadá sobre tratamiento de datos procedentes del sistema de información anticipada sobre pasajeros (API) y de los expedientes de los pasajeros (PNR), COM (2005) 200 final, DO C 218, 6.9.2005.

caso tienen acceso directo a las bases de datos de las aerolíneas, preservando así en mayor medida el derecho a la intimidad.

Por principio, solo la mencionada Agencia recibe los datos y las transferencias posteriores a otras autoridades canadienses o a terceros países únicamente podrán tener lugar en casos específicos relacionados con el terrorismo o delitos conexos, con países considerados idóneos según decisión con arreglo a la Directiva 95/46 y con respecto a una cantidad mínima de datos a transmitir. Este es precisamente uno de los puntos más positivos del Acuerdo entre la Unión y Canadá, ya que a la hora de posteriores transferencias de los datos de pasajeros la vara de medir vuelve a ser la protección europea del derecho a la intimidad.

En cuanto al tiempo de retención de los datos obtenidos, se diferencia entre los de personas que están siendo objeto de investigación en Canadá, los cuales se conservarán durante 6 años, y los de personas que no sean objeto de investigación en dicho país, cuyos datos se guardarán por un periodo de tres años y medio. La distinción parece plenamente justificada y además los lapsos temporales, claramente más cortos que los que establece el Acuerdo con Estados Unidos, cumplen adecuadamente con el principio de proporcionalidad.

Aunque el balance final del Acuerdo con Canadá es bastante positivo, todavía existen cuestiones que plantean ciertas dudas y que deberían ser tenidas en cuenta de cara a su renovación o renegociación. En este sentido, aquí también sería bienvenida una mayor concreción de los fines que se pretenden alcanzar con la transferencia de datos. La referencia al «terrorismo o delitos relacionados con el terrorismo u otros delitos graves, incluida la delincuencia organizada, cuando tengan carácter transnacional» deja abierta la posibilidad de una interpretación demasiado amplia, sobre todo en cuanto a qué se considera un «delito grave»[46]. Dicha interpretación podría alejarse del propósito básico y fundamental de todos los acuerdos que venimos analizando, que no es otro que la prevención y represión de los actos terroristas.

A pesar de que la Resolución del Parlamento Europeo, de 5 de mayo de 2010, instaba al inicio de negociaciones para alcanzar un nuevo acuerdo PNR también con Canadá, todavía no se ha alcanzado un nuevo consenso al respecto[47].

4.4. Acuerdo de 2011 entre la Unión Europea y Australia sobre transferencia de datos del PNR

En la línea de los acuerdos anteriormente analizados, en 2008 la Unión Europea también suscribió un primer acuerdo con Australia sobre tratamiento y transferencia de

46 Véase Pérez Francesch, J.L., Gil Márquez, T., Gacitúa Espósito, A. (2011). Informe sobre el PNR. La utilización de datos personales contenidos en el registro de nombres de pasajeros: ¿fines represivos o preventivos?. *ICPS Working Papers*, 297, 1-24.

47 Resolución del Parlamento Europeo, de 5 de mayo de 2010, cit.

los datos contenidos en el PNR que gestionan las compañías aéreas a los Servicios de Aduanas de Australia[48].

Tras la mencionada Resolución del Parlamento Europeo, de 5 de mayo de 2010, en la que instaba al inicio de las negociaciones para alcanzar nuevos acuerdos relativos al PNR, el 29 de septiembre de 2011 la Unión suscribió un segundo Acuerdo con Australia[49].

El objeto de este acuerdo son los datos del PNR originados en la Unión sobre los pasajeros con destino a Australia, procedentes de dicho país o con escala en él. Al igual que en los otros casos, la transmisión y gestión de los datos del PNR que recopilan las compañías aéreas y que transfieren a las autoridades aduaneras de Australia se rigen por la legislación australiana[50]. Según el Grupo de Trabajo del artículo 29, dicha legislación garantiza un nivel adecuado de protección de los datos de carácter personal de acuerdo con el Derecho de la Unión[51].

El Acuerdo establece un sistema de acceso, rectificación y borrado de los datos a favor de las personas afectadas, con independencia de su nacionalidad o país de residencia, garantizando a su vez el derecho a reclamar[52].

En cuanto al tiempo de retención de los datos obtenidos, «a lo largo de tres años a partir de la recepción inicial, todos los datos del PNR deberán ser accesibles para un número limitado de funcionarios del Servicio de Aduanas y de Protección de las Fronteras de Australia […]; pasados los tres primeros años siguientes a la recepción inicial y hasta el final del periodo de cinco años y medio, los datos deberán conservarse en el sistema del PNR, pero todos los elementos de los datos que puedan servir para identificar a los pasajeros a los que se refieren los datos del PNR deberán ser enmascarados». En el Acuerdo previo, las Aduanas conservaban los datos del PNR generados en la Unión un máximo de tres años y medio desde la fecha en que los habían recibido, y una vez transcurrido ese plazo los datos podían quedar archivados dos años más. En ambos casos, entre ambos plazos, los datos se retienen por un total de cinco años y medio, el lapso

48 Acuerdo entre la UE y Australia sobre el tratamiento y la transferencia de los datos, generados en la Unión Europea, del registro de nombres de los pasajeros (PNR) por las compañías aéreas a los Servicios de Aduanas de Australia, DO L 213, 8.8.2008.

49 Decisión del Consejo, de 13 de diciembre de 2011, relativa a la celebración del Acuerdo entre la Unión Europea y Australia sobre tratamiento y transferencia de datos del registro de nombres de los pasajeros (PNR) por las transportistas aéreos al Servicio de Aduanas y de Protección de las Fronteras de Australia, DO L 186, 14.7.2012.

50 *Australian Privacy Act 1988*.

51 Dictamen 1/2004 del Grupo de Trabajo del artículo 29, de 16 de enero de 2004, sobre el nivel de protección garantizado por Australia en la transmisión de datos del registro de nombres de pasajeros de las compañías aéreas.

52 Artículo 13 del Acuerdo UE-Australia de 2011.

temporal más corto de los Acuerdos analizados. Sin embargo, como ya puso de relieve el Parlamento Europeo, la falta de concreción de los fines para los que se retienen los datos, no permite realizar un juicio adecuado de proporcionalidad en relación al tiempo de conservación establecido en el Acuerdo[53].

El Servicio de Aduanas de Australia recibe los datos y puede transferirlos a determinados departamentos y agencias del Gobierno australiano especificados en el anexo 2 del Acuerdo. Por lo que se refiere a terceros países, el Acuerdo de 2011 ha mejorado las garantías que ya ofrecía el de 2008[54]. En primer lugar, las transferencias únicamente podrán tener lugar tras un análisis caso por caso. En segundo lugar, el Servicio de Aduanas y de Protección de las Fronteras de Australia deberá valorar detenidamente la pertinencia de los datos correspondientes, poniéndose en común solo los elementos específicos de los datos del PNR probadamente necesarios en determinadas circunstancias. Y por último, se transferirá exclusivamente la mínima cantidad. Además de todo esto, la autoridad del tercer país que reciba los datos habrá aceptado aplicar las mismas salvaguardas de este Acuerdo a los datos transferidos.

Como ya hemos apuntado, las dudas respecto al Acuerdo con Australia también radican en la falta de especificación de los fines que se pretenden alcanzar con la transferencia de datos. La referencia al «terrorismo y graves delitos de carácter transnacional» se ha querido concretar aludiendo a qué incluirán los «delitos terroristas» y qué se entiende por delito grave de «carácter transnacional»[55]. A pesar de este ejercicio de concreción, lo cierto es que el Acuerdo de 2011 sigue incluyendo términos demasiado generales, abiertos a diferentes interpretaciones, lo que redunda en un riesgo tangible para la adecuada protección de los datos personales de los ciudadanos europeos. De nuevo aquí, esta indeterminación podría alejarse del propósito básico y fundamental de todos los acuerdos que venimos analizando, que no es otro que la prevención y represión de los actos terroristas[56], y este punto debería ser tenido en cuenta de cara a revisiones posteriores del Acuerdo.

---

53 Recomendación del Parlamento Europeo, de 22 de octubre de 2008, destinada al Consejo sobre la celebración de un Acuerdo entre la UE y Australia sobre el tratamiento y la transferencia de datos, generados en la Unión Europea, del registro de nombres de los pasajeros (PNR) por las compañías aéreas a los Servicios de Aduanas de Australia (2008/2187 (INI)).

54 El Acuerdo UE-Australia de 2008 había sido criticado porque no especificaba ni los criterios ni los requisitos para admitir la difusión de los datos del PNR a terceros Estados. A través de esta vía podía cercenarse el nivel de protección de los datos de carácter personal de los pasajeros, ya que tampoco se exigía que el tercer país en cuestión garantizase una adecuada seguridad.

55 Artículo 3 del Acuerdo UE-Australia de 2011.

56 A este respecto véase la Propuesta de Resolución del Parlamento Europeo, de 3 de noviembre de 2010, sobre el enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a terceros países y las Recomendaciones de la Comisión al Consejo para

5. FUTURO PNR EUROPEO Y CRITERIOS ARMONIZADOS PARA LOS ACUERDOS INTERNACIONALES

La Unión Europea reconoce, por un lado, la importancia de los datos del PNR en la lucha contra el terrorismo y otros delitos afines y, por el otro, la sensible naturaleza de los datos individuales que están contenidos en dicho registro, que han de ser especialmente protegidos. En un mundo caracterizado por la movilidad constante de las personas, la seguridad y la prevención de la delincuencia grave y, sobre todo, del terrorismo, deben ir acompañadas de un intercambio de datos más eficaz, focalizado y rápido en Europa y a nivel mundial[57].

De momento la conjugación entre ambos intereses en los tratados internacionales suscritos con terceros países se ha realizado de una forma un tanto precaria. Hasta hoy, la celebración de acuerdos sobre el PNR ha estado dictada por la «demanda» y se ha resuelto caso por caso.

Todos los convenios tratan de cuestiones comunes y regulan la misma materia, pero sus disposiciones no son idénticas. Por ejemplo, existen diferencias en cuanto a los fines a lograr, cuando se supone que todos ellos van dirigidos a la prevención y represión del terrorismo; tampoco se transfieren ni la misma cantidad ni la misma calidad de datos; los plazos de tratamiento y retención son sensiblemente diversos; y, lo que es más importante, la protección de los datos de carácter personal difiere en cada caso al hacerla depender de la legislación interna del Estado al que se transmiten y de las garantías para el acceso, rectificación y cancelación que la misma ofrezca.

Esta falta de uniformidad llevó al Consejo a presentar en 2007 una propuesta de Decisión marco sobre utilización de los datos del PNR con fines represivos[58]. Su objetivo radicaba en armonizar las disposiciones de los Estados miembros relativas a la obligación de las compañías aéreas, que ofrecen vuelos hacia o desde la Unión Europea, de transmitir los datos PNR a las autoridades competentes con el fin de prevenir y combatir los atentados terroristas y la delincuencia organizada. Sin duda, hacía falta una armo-

---

autorizar la apertura de negociaciones para un Acuerdo entre la UE y Australia, Canadá y los Estados Unidos, B7-0604/2010/rev.2.

57 Así lo ha puesto de relieve el Parlamento Europeo, reiterando su determinación de luchar contra el terrorismo y de la delincuencia organizada y transnacional y, al mismo tiempo, su firme convicción con respecto a la necesidad de proteger las libertades civiles y los derechos fundamentales, especialmente los derechos a la intimidad, a la autodeterminación informativa y a la protección de datos; Propuesta de Resolución del Parlamento Europeo, de 3 de noviembre de 2010, cit.

58 Propuesta de Decisión Marco del Consejo, de 6 de noviembre de 2007, sobre utilización de datos del registro de nombres de pasajeros con fines represivos, COM (2007) 654 final. Véase Brouwer, E. (2009). The EU Passenger Name Record (PNR) System and Human Rights. Transferring Passenger Data or Passenger Freedom?. *CEPS Working Documents*, 320, 1-29.

nización de las legislaciones internas de los Estados miembros, pues algunos ya tenían normativa y otros la estaban desarrollando en esos momentos[59]. Más tarde, algunos de ellos han reclamado que sus autoridades aduaneras también tengan acceso a los datos del PNR y API cuando los trayectos en avión se realicen dentro de la propia Unión o en el caso de los pasajeros en tránsito[60].

Pero la uniformización interna también podría haber respondido a una coherencia externa en cuanto al contenido de los tratados a suscribir en esta materia con terceros países. De hecho, una de las críticas que se hizo a la Propuesta de Decisión marco del Consejo fue precisamente que sus disposiciones se parecían demasiado a las del Acuerdo de la Unión Europea con Estados Unidos sobre el PNR que, como hemos apuntado, es el menos adecuado al nivel de protección de los datos de carácter personal que garantiza el Derecho europeo[61].

Llama poderosamente la atención que no se haya tratado de armonizar hasta el máximo posible el contenido de dichos instrumentos, máxime cuando es probable que la «demanda» de nuevos acuerdos con otros países aumente en un futuro próximo[62].

Un marco global concertado y delimitado sobre transferencia y tratamiento de datos del PNR proporcionaría un molde a partir del cual se desarrollarían las negociaciones de los distintos tratados internacionales con terceros países, a la vez que marcaría las

59 Los Estados miembros debían tomar las medidas necesarias para dar cumplimiento a lo dispuesto en estaPropuesta de Decisión Marco antes del 31 de diciembre de 2010, fecha ampliamente sobrepasada sin que se haya producido su adopción u otra propuesta en el mismo sentido.

60 Los gobiernos de algunos Estados miembros se hacían eco de esta reclamación proveniente de las agencias y servicios de seguridad internos. Especial atención le prestó la presidencia chipriota del Consejo que promovió un proyecto para investigar las posibilidades que brindaría el uso de los datos de pasajeros por parte de las autoridades aduaneras de los Estados. Lo cierto es que aunque las delegaciones de algunos Estados consideraban positivo el proyecto, a su vez también se mostraban satisfechos con los actuales instrumentos legales de control de pasajeros aéreos. Véanse Note Aviation Security against Terrorism Threats – Conclusions of the Conference of 31 October 2012, Nicosia, Cyprus, doc. 16252/12; Customs Cooperation Working Party, Experts meeting and Plenary meeting 11 December 2012, doc. 17977/12; Cyprus Delegation, Threat assessment on air transit passengers 11 January 2013, doc. 5208/13; Study by the Presidency on Advanced Passenger Information and Passenger Name Records, 6 February 2013, doc. 5947/13.

61 Según la Propuesta de Decisión marco se transferirán 19 elementos, que coinciden con los datos señalados en el Acuerdo UE-EEUU de 2011; se prevé como método general a utilizar el *push*, pero cuando la compañía aérea no posea la capacidad técnica para utilizarlo, se permitirá a las autoridades de los terceros países acceder a la información de las aerolíneas mediante el método *pull*; el tiempo total de retención de datos se limita a 13 años, muy cercano a los 15 del Acuerdo con EEUU. Véase De Busser, E. (2010). EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal?. *Utrecht Law Review*, 6(1), 86-100.

62 Comunicación de la Comisión, de 21 de septiembre de 2010, sobre el enfoque global de las transferencias de datos de los registros de nombres de pasajeros (PNR) a los terceros países, COM (2010) 492 final, p. 6.

pautas a seguir por las legislaciones internas de los Estados. Así mismo, la armonización resulta primordial para las compañías aéreas ya que proporcionaría un marco jurídico coherente y relativamente uniforme para la transmisión de datos del PNR, garantizando unas condiciones de competencia equitativas en el sector.

Siguiendo esta línea, la Comisión y el Parlamento Europeo abogan por un enfoque global de las transferencias de datos de los registros de nombres de los pasajeros (PNR) a los terceros países. Reconsiderando su posición en esta materia, en 2010 la Comisión presentó una comunicación con el objetivo clave de establecer, por primera vez, un conjunto de criterios generales que se convertirá en la base de las negociaciones futuras de los acuerdos PNR con los terceros países.

6. A MODO DE CONCLUSIÓN

Desde hace una década la Unión Europea viene enfrentándose al difícil reto de conjugar la lucha contra el terrorismo internacional a través de todos los medios a su alcance, con el mantenimiento de un nivel adecuado de protección de los derechos a la intimidad, a la privacidad y a la salvaguarda de los datos de carácter personal.

La relevancia del intercambio de información a escala mundial con el fin de prevenir, detectar, investigar y enjuiciar las actividades terroristas y otros delitos graves de carácter transnacional, aboca a permitir, a través de tratados bilaterales, que los servicios de seguridad de países terceros accedan y gestionen los datos de pasajeros europeos recogidos por las compañías aéreas al comercializar sus billetes.

Si bien en los primeros años, la Unión se vio un tanto abrumada por las circunstancias respondiendo a las exigencias de otros países de forma un tanto torpe, a partir de ahora, y aprendida la lección, debería establecer las líneas rojas en materia de protección de los datos personales y del derecho a la intimidad, que no podrán traspasarse con los acuerdos concertados con terceros países.

A su vez, resulta encomiable la labor, comenzada ya por la Comisión, de fijar un conjunto de criterios generales que se convertirán en la base de las negociaciones futuras de los acuerdos PNR con otros Estados, lo que dará como resultado una armonización del contenido de los mismos. Tanto las compañías como los pasajeros deben tener la mayor certeza posible sobre los datos transferibles, la finalidad a alcanzar con los mismos e, incluso, su plazo de conservación, sin que estos elementos fluctúen dependiendo del país al que se viaja.

Si se siguieran rigurosamente estas pautas, los acuerdos sobre tratamiento y transferencia de datos del PNR dejarían de ser sospechosos de sacrificar en el altar del «dios de la seguridad», derechos fundamentales reconocidos al ciudadano no solo por la legislación interna de los Estados, sino por la propia normativa europea.

9

PRESERVING PRIVACY IN TIMES OF COUNTER CYBER-TERRORISM DATA MINING

Liane Colonna
The Swedish Law and Informatics Research Institute, Stockholm University, Doctoral Candidate

ABSTRACT: Terrorists are embedded and operate in the online environment. Analyzing this alternate side of the Internet, sometimes referred to as the «Dark Web», can ostensibly provide important clues regarding the nature of the terrorist threat. The problem is, however, that the massive amounts of data available to be intercepted and analyzed is so enormous that it overwhelms traditional methods of monitoring and surveillance.

One solution to this problem of information «overload» is data mining, which is increasingly being recognized as one of the most salient technologies for counter-terrorism in general and for cyber security in particular. While data mining presents many possibilities to combat cyber-terrorism, the widespread use of the technology by governments around the world has been criticized for raising serious human rights concerns. Large-scale, governmental data mining projects have been met with fierce criticism with issues of privacy, data protection, surveillance and government «snooping» being brought to the forefront.

This paper seeks to explore how to preserve privacy in an age of counter cyber terrorism data mining. Specifically, it will evaluate the advancing technology of data mining and the privacy concerns raised by it. The paper will conclude with a discussion about how states seek to ensure both privacy and security in times of cyber terrorism from the perspective of the European Court of Human Rights.

KEYWORDS: Data mining, cyber security, privacy, human rights, terrorism.

1. INTRODUCTION

Terrorists are embedded and operate in the online environment: they communicate in chat rooms between members and supporters; they recruit through Web sites; they train via online manuals; they broadcast propaganda videos and Webcasts; and they plan and implement attacks in cyberspace.[1] Analyzing this alternate side of the

1 Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council. (2008). Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment. The National Academic Press. (hereinafter referred to as «Protecting Individual Privacy in the Struggle Against Terrorists.»

Internet, sometimes referred to as the «Dark Web», can ostensibly provide important clues regarding the nature of the terrorist threat.[2] The problem is, however, that the massive amounts of data available to be intercepted and analyzed is so enormous that it overwhelms traditional methods of monitoring and surveillance.[3]

One solution to this problem of information overload is data mining, which is increasingly being recognized as one of the most salient technologies for counter terrorism in general and counter-cyber terrorism in particular.[4] Although the concept of data mining is in a state of conceptual muddle, it can broadly be understood to be an advancing collection of computational techniques for automatic analysis of huge data sets with the purpose of identifying key trends and previously unknown patterns.[5] Data mining is often regarded as the most essential step in «knowledge discovery in databases», which denotes the entire process of using data to generate information that is easy to use in a decision-making context.[6]

While data mining presents many possibilities to combat cyber terrorism[7], the widespread use of the technology by governments around the world has been criticized for raising serious human rights concerns. Large-scale, governmental data mining projects, such as the Swedish data-mining project authorized by the so-called «FRA Law,» have been met with fierce criticism with issues of privacy, data protection, surveillance and government «snooping» being brought to the forefront. Essentially, the fear is that these programs will lead not only to an invasion of the individual's secret or private world but also to a loss of the individual's control over his/her personal data with attendant real-world consequences.[8]

---

2 Id.*: see also,* United States. Dept. of Defense. Technology and Privacy Advisory Committee. (2004). Safeguarding privacy in the fight against terrorism report of the Technology and Privacy Advisory Committee. Washington, D.C. (stating that «the ubiquity of information networks and digital data has created new opportunities for tracking terrorists and preventing attacks.»).

3 Cloete, L. (2012). Dark Web: Exploring and Data Mining the Dark Side of the Web. Online Information Review, Vol. 36 (Issue 6), pp.932 – 933.

4 Last, M. (2008). Data Mining. In L. A. M. Colarik & J. Janczewski (eds.), Cyber Warfare and Cyber Terrorism (pp. 358-365). Hersbey, PA: Information Science Reference.

5 Id.

6 Protecting Individual Privacy in the Struggle Against Terrorists.

7 *C.f.* Schneier, B. (March 2006). Why Data Mining Won't Stop Terror. Wired Magazine. (contending that data mining is not useful for identifying individuals planning terrorist activities).

8 Solove, D. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale University Press.

While the aforementioned concerns are legitimate it is also true the right to privacy is not normally held to be absolute.[9] The right sometimes competes with other rights and interests such as national security although, it is important not to view privacy and security as a zero-sum game.[10] The question of how to secure both the right to privacy and the duty of society to protect its people from terrorism through the use of this important technology is rather open-ended with international courts such as the European Court of Human Rights (ECtHR), increasingly grappling with the issue.[11]

The outline of this paper is as follows: first, it will explore the way terrorist are able to exploit the ubiquity of information networks and digital data. Then it will explore the advancing technology of data mining and how it can assist law enforcement in its investigation of cyber terrorism and other serious crime. Next the paper will consider privacy issues and the concerns raised by governmental data mining projects. The paper will conclude with a discussion about how states can obtain both privacy and security in times of cyber terrorism from the perspective of the ECtHR.

2. TERRORISM AND THE INTERNET

2.1. The way terrorist use the Internet

The Internet can be defined as «an international supernetwork linking all varieties of computers and computer networks together to exchange information.»[12] It is a «network of networks» which, allows for the transfer of complex messages in many different formats: email, chat in real-time, speech (VoIP), transmission of photographs and video, satellite images, as well as software and other applications.[13] The Internet has become a tool to distribute incalculable amounts of knowledge for ordinary people, the potential of which is so far-reaching that all of its possibilities have not yet been imagined.[14]

---

9 *See e.g.*, *Convention for the Protection of Human Rights and Fundamental Freedoms* (1950)(where Article 8 provides a right to respect for one's «private and family life, his home and his correspondence,» subject to certain conditions).

10 Solove, D. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale University Press.

11 *See e.g., Centrum för rättvisa v. Sweden, Application no. 35252/08*, ECtHR, lodged on 14 July 2008.

12 Waters, R.C. (February 1997). An Internet Primer. *Federal Lawyer*, Vol. 44, 33.

13 Golumbic, M.C.. (2008). *The Balance Between Security and Civil Rights in Fighting Terror Online* Springer, 15-61: *see also*, Waters, R.C. (February 1997). An Internet Primer, Federal Lawyer, Vol. 44 (The Federal Bar Association) 33.

14 Waters, R.C. (February 1997). An Internet Primer. *Federal Lawyer*, Vol. 44, 33.

Alongside the legal activity on the Web, the Internet also serves as a communications means for terrorist.[15] Indeed, the ubiquity of information networks and digital data has created a new frontier for terrorism: cyberspace. And, from the perspective of a terrorist, there are a myriad of highly attractive features about the Internet: it is unregulated, fairly anonymous, fast, easy to access and can be used to reach huge audiences.[16]

There are a number different ways that terrorist are taking advantage of the Web. They communicate between members and supporters.[17] They recruit and fundraise through Web sites. [18] They train via online education manuals as well as provide online directions to training camps.[19] They use propaganda videos to sustain the converted, to intimidate the enemy, to win recruits and to raise funds.[20] They disseminate racists and xenophobic material online.[21] Finally, they not only threaten the commission of terrorists acts but they also plan and implement attacks online.[22] As indicated by the former US Deputy Defense Secretary Wolfowitz, the Internet has become «a tool that the terrorists use to conceal their identities, to move money, to encrypt messages, even to plan and conduct operations remotely.»[23]

Broadly, the kinds of attacks that terrorist implement in cyberspace can be grouped into two main categories: attacks that are aimed «only» at other computer systems and those that are intended to harm human lives.[24] Attacks that are aimed at computer systems can be used to, among other things, deface computer servers to demonstrate a certain level of technological dangerousness, to manipulate central government databases, to acquire information about opponents (i.e. data espionage), to create a denial

15 Golumbic, M.C.. (2008). *The Balance Between Security and Civil Rights in Fighting Terror Online* Springer, 15-61.

16 Weimann, G. (Springer 2005). How Modern Terrorism Uses the Internet. *The Journal of International Security Affairs*, Vol. 8.

17 Protecting Individual Privacy in the Struggle Against Terrorists.

18 Id.

19 Id.

20 Id.

21 Sieber, Ulrich, Brunst, Phillip. (2007). Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions. In: Council of Europe (ed(s).): Cyberterrorism – The use of the Internet for terrorist purposes. Strasbourg, Council of Europe Publishing, 94.

22 Protecting Individual Privacy in the Struggle Against Terrorists.

23 Lipton, E. and Eric Lichtblau. (September 23, 2004). Even Near Home, a New Front Is Opening in the Terror Battle, *The New York Times*.

24 Brunst, Phillip. (2009). Terrorism and the Internet. In: Wade, Marianne / Maljevic, Almir (ed(s).): A War on Terror? The European Stance on a new threat, changing laws and human rights implications. New York, Springer, 51 - 78.

of important services or to limit the ability of individuals to gain access to Internet communication.[25] Attacks that are intended to harm human lives include, for example, those aimed at critical infrastructures such as hydroelectric dams, traffic control systems and nuclear power plants.[26]

It is important to mention that aside from performing activities online, terrorist also interact with society at large. Terrorist use cell phones, pay with credit cards, travel commercially, rent vehicles and apartments, and otherwise engage in conventional commercial activities. All of these are activities that leave digital footprints that may subsequently be tracked, combined with data collected online and processed to give rise to important clues about terrorist activities.[27]

2.2. The surveillance challenge

There are several important surveillance challenges to detecting terrorist threats on the Web. First, the communications of intelligence targets must be filtered out of the massive amounts of data available on the Internet, usually in real-time, in order to prevent fast-spreading threats. This is sometimes more colloquially referred to as the «the needle in the haystack problem.»[28] Furthermore, the communications must be located within a huge civilian environment which, poses risk to the liberty of the great majority of individuals whose communications are lawful.[29]

It is also important to note that terrorist groups will make calculated efforts to conceal their identity and mask their behaviors, and will use various strategies to obfuscate the data they are generating and exchanging.[30] For example, terrorist will encrypt their online messages, apply code words, and use multiple identities.[31] Terrorists also create extremely dynamic Web sites to relay their ideas.[32] Last explains that, «(t)errorist orga-

25 Brunst, Phillip. (2009). Terrorism and the Internet. In: Wade, Marianne / Maljevic, Almir (ed(s).): A War on Terror? The European Stance on a new threat, changing laws and human rights implications. New York, Springer, 51 - 78.

26 Brunst, Phillip. (2009). Terrorism and the Internet. In: Wade, Marianne / Maljevic, Almir (ed(s).): A War on Terror? The European Stance on a new threat, changing laws and human rights implications. New York, Springer, 51 - 78.

27 Protecting Individual Privacy in the Struggle Against Terrorists.

28 Protecting Individual Privacy in the Struggle Against Terrorists.

29 Golumbic, M.C.. (2008). *The Balance Between Security and Civil Rights in Fighting Terror Online* Springer, 15-61.

30 Protecting Individual Privacy in the Struggle Against Terrorists.

31 Protecting Individual Privacy in the Struggle Against Terrorists.

32 Hsinchun Chen , Dark Web: Exploring and Data Mining the Dark Side of the Web (Integrated Series in Information Systems) (Springer 2011).

nizations can post their information on the Web at any location (Web server), in any form (Web page, Internet forum posting, chat room communication, e-mail message, etc.), and in any language.»[33] Frequently Web pages emerge overnight and then swiftly disappear by changing their URLs, which are later announced via online forums.[34]

3. DATA MINING

3.1. The technology of data mining

Every day, quintillions of bytes of data are created: the amount of data is growing so rapidly that that scientists are no longer talking in terms of megabytes, gigabytes, terabytes or even petabytes, but have, instead, had to create new terms such as «zettabyte» to describe it.[35] Although this data offers great potential, humans do not have the capacity, on their own, to reap all of the benefits that may be revealed from a more comprehensive understanding of all of these data.[36] In this respect, data mining can be understood as the response to this problem of information «overload.» The idea is that «big data» should be met with «big processing power.»

Data mining is often thought to be the most essential step in the process of «knowledge discovery in databases», which denotes the entire process of using data to generate information that is easy to use in a decision-making context.[37] The data-mining step itself consists of the application of particular algorithms or machine learning techniques to the cleansed data in order to identify certain previously unknown characteristics of the data set.[38] Data mining techniques can include, for example, association analysis (finds interesting correlations among a large set of data items), cluster analysis (describes

33 Last, M and Alex Markov, Abraham Kandel. (2008). «Multi-lingual Detection of Web Terrorist Content in Intelligence and Security Informatics Studies.» In *Computational Intelligence*. Vol. 135, 79-96.

34 Chen, H. (2011). Dark Web: Exploring and Data Mining the Dark Side of the Web. *Integrated Series in Information Systems*. Springer.

35 A «zettabyte» is equivalent to about 250 billion DVDs. *For more*, *see* Arthur, C. (2011). «What's a Zettabyte? By 2015, The Internet Will Know, says Cisco,» Technology Blog at The Guardian UK Newspaper; *see also*, Kuner, C. Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson. (2012). The Challenge of 'Big Data' for Data Protection.» *International Data Privacy Law* Vol. 2(2), 47.

36 Han, J. and Micheline Kamber. (2006). *Data Mining: Concepts and Techniques (Second Edition).* San Francisco: Morgan Kaufmann Publishers.

37 Id.

38 Han, J. and Micheline Kamber. (2006). *Data Mining: Concepts and Techniques (Second Edition).* San Francisco: Morgan Kaufmann Publishers.

the available datasets by grouping them into common categories), predictive modeling (predicts future outcomes based on automated analysis of historic data) or anomaly detection (discovers events that typically do not conform to expected normal behavior).[39] Data mining also has a multiplicity of different application domains ranging from the banking/finance sector (e.g. detection of fraudulent credit card usage patterns, risk management related to attribution of loans) to retail/ marking sector (e.g. discovery of buying behavior patterns) to medical sector (e.g. computer assisted diagnoses of illnesses) to, of course, the law enforcement sector which will be explained in more depth below.

It is important to understand that data mining is a relatively new field that differs from the data processing of the recent past for a number of reasons and as such it raises concerns that have hitherto not been the object of extensive study. For example, unlike earlier forms of data processing, data mining is usually conducted on huge volumes of complex data and it can extract value from such volume.[40] Furthermore, it generates «new» knowledge: instead of simply extracting «what» is in a database, data mining can turn data into something novel and more useful such as a more compact summary or a more useful form such as a prediction.[41] It is also worth mentioning that data mining is not necessarily limited by the creativity of humans to create hypotheses because some forms of data mining are able to explore the dataset and generate hypotheses automatically.[42]

3.2. Applications of data mining in the cyber terrorism context

Counterterrorism data mining can broadly be understood to denote the use of various mathematical and machine learning techniques to sift through large data repositories to identify threats to law enforcement and national security.[43] It often involves extracting information from databases, as well as text, voices, other audio, video, graphs,

39 *See generally*, Taipale, K.A. (2003). Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data. *Columbia Science & Technology Law Review*, 1-229; Seifert, J.W.. (Dec. 16, 2004).Data Mining: An Overview. *Congressional Research Service* 1.

40 Lloyd-Williams, M. (1997). Discovering the Hidden Secrets in Your Data - the Data Mining Approach to Information, *Information Research: An International Electronic Journal* available online at http://informationr.net/ir/3-2/paper36.html

41 Taipale, K.A. (2003). Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data. *Columbia Science & Technology Law Review*, 1-229.

42 Custers, B. (2013). Data Dilemmas in the Information Society: Introduction and Overview. In Bart Custers, Tal Zarsky, Bart Schermer, Toon Calders)(eds.), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases.* Springer.

43 Ramasastry, A. (January 7, 2004). *The Safeguards Needed for Government Data Mining*. Retrieved from http:// writ.news.findlaw.com/ramasastry/20040107.html.

images, maps, and equations and chemical formulas.[44] It then uses this information to search for threats using specific techniques such as clustering, association and classification, described above.[45]

Meaningful discussions about governmental counter cyber terrorism data mining programs are difficult because so little is known about how these programs work in practice. This is because they are confidential and classified for security reasons. As such, the goal here is to provide a couple of examples of where the scientific research is being done in order to help elucidate how governments *might* apply data mining in the counter cyber terrorism context.

A first example of a data mining application in the cyber terrorism context is intrusion detection.[46] Network-intrusion is defined as «a special form of cyber threat analysis to identify malicious actions that could affect the integrity, confidentiality, and availability of information resources.» [47] Data mining-based intrusion-detection mechanisms are extremely useful in discovering security breaches for a variety of reasons.[48] That is, data mining can be used to assist in locating anomalous events on a network by building a model of normal behavior and automatically detecting significant deviations from it.[49] Data mining can also be used to assist in locating patterns and signatures of previously known attacks. [50] Furthermore, research is being done to apply data mining to not just detect intrusions in real time but to also *predict* attacks in advance.[51]

Web link and content analysis is another example of where data mining is being applied in the cyber-terrorism context. On this point, the work being done at the US-based Dark Web project is illustrative. The Dark Web Project, funded by the American National Science Foundation, relies solely on open source data. The aim of the Project

---

44 (Feb. 23, 2004). *Controversial Government Data Mining Research Lives On*. Retrieved from http:// www.siliconvalley.com/mld/siliconvalley/news/editorial/8022436.htm.

45 Seifert, J.W.. (Dec. 16, 2004).Data Mining: An Overview. *Congressional Research Service* 1.

46 Thuraisingham, B. (2009). Data Mining for Security Applications and Its Privacy Implications, Privacy, Security, and Trust. *KDD Lecture Notes in Computer Science*, Volume 5456, pp 1-6.

47 Al-Shawi, A. (2011), Data mining techniques for information security applications. *WIREs Comp Stat*, Volume 3, 221–229.

48 Al-Shawi, A. (2011), Data mining techniques for information security applications. *WIREs Comp Stat*, Volume 3, 221–229.

49 Han, J. and Micheline Kamber. (2006). *Data Mining: Concepts and Techniques (Second Edition).* San Francisco: Morgan Kaufmann Publishers.

50 Al-Shawi, A. (2011), Data mining techniques for information security applications. *WIREs Comp Stat*, Volume 3, 221–229.

51 Thuraisingham, B. (15-18 Sept. 2009). Data Mining for Malicious Code Detection and Security Applications. *Web Intelligence and Intelligent Agent Technologies*, 2009. WI-IAT '09. IEEE/ WIC/ACM International Joint Conferences.

is to collect all web content generated by international terrorist groups including web sites, forums, chat rooms, blogs, social networking sites, videos, virtual world, etc. and to apply various data mining techniques to make sense of it. [52] The amount of data collected for this project is enormous: two terabytes of data, 500 million pages, files and postings from over 10,000 sites.[53] This huge amount of data would quickly overwhelm traditional methods of monitoring and surveillance.

More specifically, data mining is being applied in the Project to visualize hyperlinked communities. By analyzing and visualizing hyperlink structures between terrorist-generated web sites and their content, the Project contends that it can discover a deeper understanding of structure and organization of terrorist group networks.[54] By visualizing a picture of hyperlinked communities, for example, it is possible to see that terrorist groups are linked to each other through complex networks and to uncover hidden Web communities.[55] Hyperlink analysis can also help identify how relationships between groups are formed and dissolved. [56] It can further enable governments to decipher the communication channels among terrorist groups across different jurisdictions. [57]

The project is also applying data mining to help identify and trace terrorists operating in cyberspace. It is doing this through the development of multilingual authorship analysis.[58] In authorship analysis, data mining techniques can be applied to find out who is creating «anonymous» content online. [59] The idea is to find the digital analogue to the «fingerprint» – the «writeprint.»[60]

Dark Web's software, called Writeprint, samples 480 different factors to identify whether the same people are posting to multiple radical forums.[61] It can analyze everything from a fragment of an email to videos depicting American soldiers blown

52 Chen, H. (2011). Dark Web: Exploring and Data Mining the Dark Side of the Web. *Integrated Series in Information Systems*. Springer.

53 Fox News. (November 11, 2007). Internet Tool Hopes to Capture Online Terrorists. Associated Press.

54 Chen, H.. (2006). Intelligence and Security Informatics for International Security: Information Sharing and Data Mining. *Integrated Series in Information Systems*, Volume 10, 55-73. Springer.

55 Id.

56 Id.

57 Id.

58 Id.

59 Id.

60 Id.

61 Fox News. (November 11, 2007). Internet Tool Hopes to Capture Online Terrorists. Associated Press.

up in Humvees and fuel tankers.[62] It looks at writing style, word usage and frequency and greetings, and at technical elements ranging from Web addresses to the coding on multimedia attachments. [63] It also looks at linguistic features such as special characters, punctuation, word roots, font size and color. [64]

3.3. Sweden, the FRA and data mining

Signals intelligence is a special form of intelligence collection that, as its name suggests, is derived from the interception of signals, including communications signals, electronic emissions, and telemetry. [65] One of the purposes of signals intelligence is to give advance warning of circumstances in the international environment that may affect a state from a security and/or military perspective. For example, signals intelligence could provide warning of an armed attack or violation of territorial integrity.[66] Data mining is extremely useful in the context of signals intelligence insofar as it offers the possibility to transform the huge amounts of communication messages into a higher form of knowledge so that threats can be discerned and actionable intelligence can be provided to national leadership.[67]

The National Defense Radio Establishment (Försvarets Radioanstalt, «FRA») is the national authority for signals intelligence in Sweden.[68] It is a civilian agency, formed in 1942, with the main task of supplying signals intelligence services to the Swedish government, the Swedish Armed Forces and state agencies.[69] At the time of its creation, the FRA was formally authorized to monitor radio, but not cable, communications. There is, however, some evidence that it had also been authorized by secret decree to access cable communications.[70]

---

62 Id.

63 Id.

64 Id.

65 Knight, J. SIGINT (Signals Intelligence), in Encyclopedia of Espionage, Intelligence, & Security retrieved at http://www.espionageinfo.com/Se-Sp/SIGINT-Signals-Intelligence.html (defining signals intelligence).

66 Observations of the Government of Sweden on Admissibility, Application no. 35252/08 Centrum för rättvisa v. Sweden (ECtHR).

67 (2004). *Getting Up to Speed: The Future of Supercomputing*. Washington, DC: The National Academies Press.

68 Observations of the Government of Sweden on Admissibility, Application no. 35252/08 Centrum för rättvisa v. Sweden (ECtHR).

69 Id.

70 Agrell, W. (11 July 2008). Regeringen borde talat klarspråk. Expressen; *see also*, Palfrey, J. (Winter 2008). *The Public and the Private at the United States Border With Cyberspace*. Mississippi Law Review, Volume 78, 241.

Over time, the FRA asserted that it was frustrated with its ability to intercept communications because of technological advances. That is, communications began to travel less by satellite, microwave relay link and more in fiber-optic cable.[71] This made interception more difficult for the FRA because, unlike with satellite and microwave relay links, which leak communications that are accessible with an antenna, interception of communications in a fiber optic cable must be accessed with the knowledge and consent of the communications service provider at certain points where the communication is routed.[72]

As a result of the FRA's complaints that without the right to intercept cable traffic it was unable to discharge its duty to support Sweden's foreign, security and defense affairs the New Signal Surveillance Act or the so called «FRA Law» was passed by the Swedish Parliament in 2008.[73] The system put in place by the new legislation requires that all telecom operators in Sweden who carry data across the country's border must adjust their systems to enable the FRA to tap the traffic at designated transfer points.[74] Although domestic surveillance is not the objective of the law, commentators have pointed out that because of the way that information travels on the Internet, it is not technically possible to distinguish between pure domestic communication and international communication: messages between two persons in the same country are divided into small packets and often routed across the world.[75]

Pursuant to the FRA Law, the FRA is given permission to both «collect» and «process» huge amounts of phone and email communications passing through cables or wires across the country's borders. With respect to the collection of data, it has been documented that the FRA stores large amounts of information, which subsequently is searched through the use of search concepts.[76] The search concepts refer to technical

---

71 Klamberg, M. (2010). FRA and the European Convention on Human Rights- A Paradigm Shift in Swedish Electronic Surveillance Law. *Nordic Yearbook of Law and Information Technology*, pp. 96-134 (herein after referred to as «A Paradigm Shift in Swedish Electronic Surveillance Law»).

72 «A Paradigm Shift in Swedish Electronic Surveillance Law»

73 Riese, B. (2008). Mind what you say. *European Lawyer*.

74 Id.

75 «A Paradigm Shift in Swedish Electronic Surveillance Law»; *see also* Observations of the Government of Sweden on Admissibility, Application no. 35252/08 Centrum för rättvisa v. Sweden (ECtHR) (stating «For network configuration reasons, domestic traffic (signals between a sender and a recipient who are both located in Sweden) could also cross the national border.»).

76 «A Paradigm Shift in Swedish Electronic Surveillance Law»; see also Observations of the Government of Sweden on Admissibility, Application no. 35252/08 Centrum för rättvisa v. Sweden (ECtHR)(explaining, «Cable collection must be done automatically. When signals are collected automatically, via cable or wireless, theymust have been identified by selectors. Selectors are applied to specify one or more terms to search through a mass of information and find the items

parameters such as frequencies, email addresses and phone numbers. [77] Search concepts should be distinguished from the narrower notion of «key words», which would imply that words such as «bomb» or «al-Qaida» are used to screen the content of all messages.[78]

With respect to the processing of data, the FRA may only process personal data if it is necessary for defense intelligence operations.[79] Little is publicly known about the techniques applied by the FRA. Arguably, however, such techniques include data mining given the massive amounts of communications data sets involved.

It has further been documented that the FRA distinguishes between how it handles content data and traffic data.[80] Generally, content data is described as the kind of communications that would exist inside a sealed letter whereas traffic data is the kind of communications that would exist on the outside of the envelope.[81] The emphasis is being placed on traffic data since it is easier to store in large volumes and can be analyzed to sidestep the problems of encryption.[82]

In its first incarnation, the FRA Law authorized the FRA to monitor communications without a court order. Following widespread public protest, the law was amended to allow such wiretapping only in cases where external military threats were suspected. It was also subsequently amended to allow only the government and the military from requesting surveillance, and to require notification to individuals who have been monitored subject to several important exceptions.[83]

---

or constellations of data which a term matches. A selector may also contain parameters that exclude large volumes of information. Selectors are to be formulated and used in such a way that they involve as little infringement as possible on people's personal privacy. Selectors may not be directly attributable to a specific natural person unless this is of utmost importance to the foreign intelligence objectives.»).

77 «A Paradigm Shift in Swedish Electronic Surveillance Law»

78 Id.

79 (10 September 2008). Signals intelligence, Regeringskansliet (Government Offices of Sweden) website, retrieved at http://www.government.se/sb/d/10941

80 «A Paradigm Shift in Swedish Electronic Surveillance Law»

81 Much has been written on the problems of differentiating between content and traffic data. See e.g. Solove, D. J.. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security.* New Haven: Yale University Press)(explaining «The law wrongly protects envelope information much less than content information. Envelope information can reveal a lot about a person's private activities, sometimes as much (and even more) than can content information. We may care more about keeping private WHO we are talking to than WHAT we are saying.»).

82 «A Paradigm Shift in Swedish Electronic Surveillance Law»

83 Observations of the Government of Sweden on Admissibility, Application no. 35252/08 Centrum för rättvisa v. Sweden (ECtHR).

In 2008, the Centrum för rättvisa (Center for Justice), a Swedish public interest law organization, lodged a complaint with the European Court of Human Rights (ECHR) against Sweden. In its complaint, the organization requests a review of whether the Act violates, inter alia, articles 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. A judgment from the court is likely to have far-reaching consequences for the FRA Law. It could also affect other member states of the Council of Europe should they want or attempt to implement a similar system.[84]

3.4. Limitations of a data mining as a terrorist detection tool

While data mining can be very helpful in the cyber security context, it is subject to several important limitations. For example, Seifert explains, «(t)o be successful, data mining requires skilled technical and analytical specialists who can structure the analysis and interpret the output that is created.»[85] Furthermore, data mining can identify connections between variables, but it cannot necessarily identify a causal relationship. [86] Also, the effectiveness of data mining is dependent upon the type of criteria or assumptions that are built into any model or algorithm.[87] Likewise, there are many possibilities for error due to do, among other things, problems with the quality of the underlying data set: if the data set is inaccurate, incomplete, inconsistent or structured in a faulty way then there is a possibility for false positives, the generation of an incorrect inference, or false negatives, the failure to generate a crucial inference. [88]

4. PRIVACY CONCERNS RAISED BY DATA MINING IN THE CYBER TERRORISM CONTEXT

Privacy is a nebulous concept.[89] As a starting point, therefore, it is useful to think about the values that underlie the notion of privacy so as to better understand what is at

84 Riese, B. (2008). Mind what you say. *European Lawyer*.

85 Seifert, J.W.. (Dec. 16, 2004).Data Mining: An Overview. *Congressional Research Service* 1.

86 Id.

87 Ramasastry, A. (2006). Lost in Translation? Data Mining, National Security and the 'Adverse Inference' Problem. Santa Clara Computer & High Tech Law Journal, Vol. 22:4, 757.

88 Seifert, J.W.. (Dec. 16, 2004).Data Mining: An Overview. *Congressional Research Service* 1.

89 Lyon, D. (2001), Facing the Future: Seeking Ethics for Everyday Surveillance. *Ethics and Information Technology*, Volume 3, number 3, 171-180 (Undoubtedly, the term privacy is at once the most popular and the most slippery term used in this field. It is culturally and historically relative, it has strong spatial overtones (that go with other aspects of privacy discourse such as 'invasion' or 'intrusion' that pepper the pages of much surveillance literature in the Big Brother mode), is highly subjective, is gendered, especially in contexts where private is associated with

stake when privacy is pitted against security. Privacy is generally considered essential to human wellbeing, development, creativity, mental health, liberty, dignity, emotional release, self-evaluation, and inter-personal relationship of love, friends and trust.[90] Privacy is also considered necessary condition for autonomy: without privacy, people could not experiment in life and develop their own personality and own thoughts, because they would constantly be subjected to the judgment of others.[91] Furthermore, it is important to note that privacy is has benefits to society: it is necessary for meaningful democratic participation, and ensures human dignity and autonomy.[92]

Although data mining presents many possibilities to combat terrorism, the widespread use of the technology by governments around the world undermines many of the values underpinning privacy.[93] Taipale identifies three major privacy concerns that are implicated by employing data mining for proactive law enforcement activities. First, he explains that there is a chilling effect that information access and data sharing by the government might have on innocent behavior.[94] Here, the concern is that individuals will act differently if they know that their conduct might be observed and individual autonomy will be compromised. For example, people's ability to express themselves, protest ideas they find repugnant or associate with whom they choose may be affected by encouraging «conformity with a perceived norm, discouraging political dissent, or otherwise altering participation in political life.»[95]

Second, Taipale explains that there is a slippery slope that may result when powerful data mining tools are used for increasingly pettier needs until finally society is smothered under a veil of constant surveillance.[96] Here, the fear is the creation of an oppressive,

---

the women and public with men, and tends to bring the discussion down to an individualistic level).

90 See generally, Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, California: Stanford Law Books.

91 See generally, Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

92 Regan, P. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: The University of North Carolina Press.

93 *c.f.* Schneier, B. (March 2006). Why Data Mining Won't Stop Terror. *Wired Magazine* (contending that data mining is not useful for identifying individuals planning terrorist activities).

94 Taipale, K.A.. (2004-2005). Technology, Security and Privacy: The Fear of Frankenstein, The Mythology of Privacy and the Lessons of King Ludd. *Yale Journal of Law and Technology*, Volume 7, 123.

95 US Department of Defense. (March 2004). *Safeguarding Privacy in the Fight Against Terrorism*, The Report of the [Department of Defense] Technology and Privacy Advisory Committee.

96 Taipale, K.A.. (2004-2005). Technology, Security and Privacy: The Fear of Frankenstein, The Mythology of Privacy and the Lessons of King Ludd. *Yale Journal of Law and Technology*, Volume 7, 123.

Big Brother government that regulates all aspect of individual existence, including the regulation of individual, private thoughts. Taipale notes that, «this fear is particularly relevant when one recognizes that there will always be an insatiable need for more security and there will always exist a bureaucratic imperative for additional control.»[97]

Third, Taipale contends that the lack of transparency associated with data mining creates the potential for abuse or misuse by government bureaucrats.[98] This abuse could range from anything from government agents looking up their neighbor's tax returns to law enforcement officials sharing information with criminal suspects. [99] More recently, Zarsky explains:

> «A basic (and intuitive) justification for transparency is that it facilitates a check on governmental actions. Generally, society constantly fears that the acts of its government might be flawed, biased, ineffective or inefficient. The relevant officials might be improperly balancing rights and interests, led by their own bigotry, or are over-influenced by private interests.»[100]

The concerns raised above are echoed in Solove's Kafka Mataphor, which provides a useful way to better understand the privacy issues raised by data mining.[101] In Kafka's The Trial, the main character is placed in jail without being told what crime he committed or what evidence was collected against him. The story is about a bureaucracy that uses his personal information to make important decisions about his life, yet denies him the ability to participate in or understand how the information is used against him. [102] The harms depicted are bureaucratic ones: indifference, error, abuse, frustration, and lack of transparency and accountability. [103] Solove makes the point that inhibition may be less of concern than in the traditional «panoptic» surveillance scenario where individual behavior is constrained because they are aware that they are being watched. This is because, in the data-mining scenario, individuals do not usually know that they are being surveilled.

---

97 Id.

98 Id.

99 Id.

100 Zarsky, T. (2013). Transparency in Data Mining: From Theory to Practice. *Discrimination and Privacy in the Information Society: Studies in Applied Philosophy, Epistemology and Rational Ethics*, Volume 3, 301.

101 Solove, D. J.. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security.* New Haven: Yale University Press).

102 Id.

103 Id.

5. PRESERVING PRIVACY IN TIMES OF CYBER TERRORISM FROM A EUROPEAN PERSPECTIVE

5.1. The right to privacy

The right to privacy is recognized by most, if not all, democratic states in the world. From a European perspective, the right to privacy is enshrined in Article 8 of the European Convention for the protection of Human Rights which states: «Everyone has the right to respect for his private and family life, his home and his correspondence.»[104] Article 8 imposes a minimum requirement for the protection of privacy and provides a mechanism for the enforcement of such rights by individuals where they have been infringed by states and there is no remedy under domestic law to address such infringement.

Although the right to privacy is established in Article 8, there are certain circumstances in a democratic society when it may be necessary for the state to interfere with this right. The circumstances whereby state authorities are allowed to encroach upon the right to privacy are set forth in the second paragraph of Article 8 ECHR: interferences are justified if they are «in accordance with the law»(the «legality requirement»), pursue one or more of the legitimate aims such as protecting state security (the «legitimacy requirement) and are «necessary in a democratic society» in order to achieve them (the «proportionality» requirement).[105]

It is also important to mention that aside from satisfying these minimum fundamental human rights standards, the specific requirements of The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE Convention) must also be met.[106] The CoE Convention sets forth a number of important data protection principles concerning the collection and processing of personal data. For example, it outlaws the processing of «sensitive» data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. It also enshrines the individual's right to know what information is stored on him or her and, if necessary, to have it corrected. Like derogations from

104 In addition, the Charter of Fundamental Rights of the European Union calls for the respect of privacy in its Article 7. That provision states that «[e]veryone has the right to respect for his or her private and family life, home and communications.»

105 ECtHR, Weber and Saravia v. Germany, Application no. 54934/00, Judgment, 29 June 2006, Para. 80.

106 *See, ECtHR, S. and Marper v. the United Kingdom*, Applications nos. 30562/04 and 30566/04, Judgment, 4 December 2008 (making numerous citations to the Council of Europe's Data Protection Convention, indicating that the Court will also enforce that Convention through the ECHR).

Article 8, restrictions on the rights laid down in the CoE 108 are only possible when overriding interests are at stake.[107]

5.2. Justifying an interference with the right

The ECtHR has determined that any collection, storage, and/or processing of data pertaining to individuals represents an interference with the right to respect for private life.[108] And, in the case of secret monitoring of communications by the state, it is not necessary to prove that the measures were specifically taken against the complainant individual as the Court has determined that «the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied.»[109] Accordingly, there can be little doubt that a state-operated, cyber terrorism data mining program would represent an interference with the right to privacy under the ECHR. The question then becomes whether the interference with the right to privacy is justified pursuant to Article 8(2).

The *Liberty* and *Weber and Saravia* cases are highly relevant when trying to understand how the Court might assess the interference with private life caused by a cyber terrorism data-mining program. While neither *Weber* nor *Liberty* explicitly use the term «data mining,» both cases concerned broad surveillance in the form of signals intelligence like that which is authorized under the Swedish FRA Law.[110] In the case of *Liberty*, the UK government was capturing all communications –including telephone, facsimile, and email communications– that were sent along a particular channel and then used a search engine to «filter» out those communications that were likely to be of most interest.[111] In *Weber*, the surveillance concerned the performance of «strategic monitoring»

---

107 Article 9(2)(derogations must be «provided for by the law of the Party» and represent «a necessary measure in a democratic society in the interests of... protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences» or «protecting the data subject or the rights and freedoms of others.»).

108 *See Marper,* para. 103. (where the Court stated that the «mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8» and that «protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention.»)

109 ECtHR, *Liberty and Others v. the United Kingdom*, (Application no. 58243/00), Judgment, 1 July 2008., para. 16.

110 Even if data mining was not used, the type of catchword-assisted surveillance applied by Germany and the UK is a similar phenomenon.

111 *Liberty*, para. 43. According to the applicants, between 1990 and 1997 the government intercepted all public communications transmitted between British Telecom's radio stations at Clwyd and Chester, with the result that the majority of electronic communications between Ireland and England and Wales had been made the subject of routine covert surveillance.

by the German government to avert «serious dangers» to national security.[112] The German legislation also included provisions governing the use of «catchwords» which served a function akin to the search engine-driven «filtering» referred to in *Liberty*.[113] Despite the fact that similar forms of surveillance were at issue in the two cases, the Court found a violation of Article 8 in *Liberty* but no violation in *Weber*.

The central issue in both cases was whether the interference with privacy was in accordance with the law. In interpreting the legality requirement of Article 8(2), the Court emphasized in both *Weber* and *Liberty* that there must be a clear legal basis for the surveillance program provided under domestic law. The Court explained in both cases that the law should be accessible to the person concerned, who must be able to foresee its consequences for him/her.[114] The Court made clear, however, that the legality requirement does not mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he/she can change his/her behavior to avoid surveillance. Rather, it implies that the domestic law is sufficiently clear in its terms to afford citizens an adequate indication as to the circumstances in which a public authority is empowered to resort to any such measures.[115]

The Court further explained that, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[116] In this respect, certain minimum safeguards should be set out in statutory law in order to avoid abuses of power. Relying on previous case law, the Court set forth a list of safeguards that should be included in the law to avoid abuses of power related to secret surveillance which include: the nature of the offenses which may give rise to an interception order; a definition of the categories of people who may be subject to surveillance; a limit on the duration of the surveillance; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which the data may or must be destroyed. [117]

In *Weber*, the Court found that the German legislation set out on its face detailed provisions regulating the way in which individual communications were to be selected

112 «Strategic» monitoring involves the collection of large, untargeted volumes of data from which information of interest is subsequently extracted by filtering.

113 *Weber*, para. 32.

114 *Weber* para., 84.

115 *Weber* para,. 84; *Liberty* para. 45.

116 *Weber* para., 93-94, *Liberty* para. 62-64.

117 *Weber* para., 93-94, *Liberty* para, 62-64 (noting that while these had been developed in relation to surveillance targeted at specific individuals or addresses, they apply equally to generalized strategic monitoring).

from the pool of material derived from «strategic interception.»[118] The law not only explained how selected material would be disclosed among various agencies of the German State and the use that each agency could make of the material but it also included provisions on the retention and destruction of the material.[119] The Court further relied upon the fact that the discretion of the executive was limited by both the Federal Constitutional Court and the provisions of the Federal Constitution.[120]

In contrast, in *Liberty*, the Court found that the UK did not have an adequate basis in domestic law, and that the existing law was neither publicly accessible nor formulated in such a way as to make such interception foreseeable.[121] Specifically, the Court determined that the UK law afforded the State a virtually unfettered discretion for the capture of communications.[122] It also conferred a wide discretion on the Government as to which of the captured communications were listened to or read. The only protections against an abuse of power were internal regulations, manuals and instructions. The details of these «arrangements,» however, were not contained in legislation or otherwise made available to the public.[123] The Court explained, that the domestic law failed to set out «in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material.»[124]

In *Liberty*, the Court's interpretation of Article 8(2) concluded after it held that the interference with the applicants' Article 8 rights was not «in accordance with the law.» In *Weber*, however, the Court also analyzed the other requirements of Article 8(2). With respect to the second requirement, «legitimacy,» the Court did not challenge the aim referred to by Germany. Instead it stated: «(it) shares the Government's view that the aim of the … (German law) was indeed to safeguard national security and/or to prevent crime, which are legitimate aims within the meaning of Article 8.»[125]

In interpreting the third requirement, «proportionality,» the Court found in *Weber* that the interference by the surveillance programs must be «necessary in a democratic society.» The Court's proportionality examination concentrated on whether there

118 *Weber* para., 96, *Liberty* para. 45.

119 *Weber* para., 131.

120 *Weber* para. 92-102.

121 Goold, B. (2009). Liberty and others v The United Kingdom: a new chance for another missed opportunity. *Public Law*, 5-14.

122 Id.

123 (2008). Case: Liberty v United Kingdom (58243/00). *European Human Rights Law Review*, Vol. 6, 788-792.

124 *Liberty*, para. 69.

125 *Weber*, para. 104.

were sufficient procedural safeguards against abuse of the State's powers of surveillance.[126] In this respect, its analysis of proportionality echoed its analysis of legality.

Here, the *Weber* Court noted that pursuant to the German law, the state administrator responsible for authorizing interceptions and other surveillance measures was obliged to report to a special board comprised of, among others, nine members of Parliament. The Court also relied upon the fact that anyone who had been the subject of monitoring was notified after the danger of jeopardizing the purpose of the monitoring or use of the data obtained has passed.[127] The Court further relied upon the fact that the German law contained specific provisions governing the use of search terms: although the law did not demand that the State reveal what the search terms were, the law prohibited the use of catchwords that permitted for the interception of specific communications.[128]

It is also important to note that in *Weber*, the Court reiterated that when assessing the interest of the State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, it has consistently recognized that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security.[129] In other words, States should have room to assess for themselves how to ensure both privacy and security. The Court further elaborated, however, «in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse.»[130]

Finally, it is worth commenting that the Court in *Weber*, in finding in favor the State, made several references to Germany's compliance with the principles set forth in the CoE Convention and its additional protocols, albeit without explicit reference. First, the Court, referring to the purpose limitation principle, stated that the «…German authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them.»[131] The Court also relied upon the fact that the law contained strict provisions concerning the storage and destruction of data.[132]

126 *Weber*, para. 82.

127 Goold, B. (2009). Liberty and others v The United Kingdom: a new chance for another missed opportunity. *Public Law*, 5-14.

128 Id.

129 *Weber*, para. 106, 116.

130 *Weber*, para. 106.

131 *Weber*, para. 100.

132 *Weber*, para. 116.

The Court further noted that although the German law authorized the transmission of personal data obtained by general surveillance measures without any specific prior suspicion in order to allow criminal proceedings to be brought against those being monitored, it only permitted this transfer of personal data in order to prevent or prosecute a specified list of serious criminal offenses.[133] Lastly, with respect to the fact that personal data was collected and processed without individual consent, the Court relied upon the fact that individuals monitored were to be informed that their telecommunications had been intercepted as soon as notification could be carried out without jeopardizing the purpose of monitoring.[134]

6. CONCLUSION

Governmental data mining programs create serious privacy concerns such as the intrusion into the individual's secret world and a loss of the individual's control over his/her personal data with very real consequences like being identified as a terrorist suspect. [135] When information about an individual is collected, analyzed and mined without his/her knowledge, consent or understanding, that individual's autonomy is compromised and his/her freedom to determine his/her own lives by themselves is limited.[136] This creates not only a sense of powerlessness and vulnerability but also an unequal power relationship between individuals and the institutions of the modern state.[137]

The problem is, however, that in today's ubiquitous computing environment, governments legitimately need a way to make sense of the massive amounts of data available in digital format in order to protect society from serious risks of terrorism. In many ways, cyber terrorism data mining involves a catch-22 situation: if governments reveal the techniques they use then «terrorists» would simply avoid those activities that give rise to suspicion.[138] Without public accountability, however, data mining programs can be used as tools of arbitrary power.

133 *Weber*, para. 126.

134 *Weber*, para. 136.

135 Solove, D. J.. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security.* New Haven: Yale University Press).

136 Golumbic, M.C.. (2008). *The Balance Between Security and Civil Rights in Fighting Terror Online* Springer, 15-61 («When information about us is collected without our knowledge, consent or understanding, that is, when we are unaware of any privacy threat, we lose control over ourselves, our autonomy is compromised and our freedom to determine our own lives by ourselves is limited.»).

137 *See* Van den Hoven, J. (2007). Information Technology, Privacy and The Protection of Personal Data. In *Information Technology, Privacy and The Protection of Personal Data*. Cambridge: University Press.

138 Solove, D. J.. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security.* New Haven: Yale University Press).

In determining how to secure both privacy and security in the context of cyber-terrorism data mining, the case law of the ECtHR is highly informative. According to an analysis of its recent case law on the subject, the key to establishing a permissible data-mining program lies in the formulation of a domestic law that is sufficiently clear in its terms allow citizens to foresee the circumstances in which the state might resort to data mining. It is also critical to provide a precise description of the state's authority and to have in place clear procedures that safeguard against the abuse of the state's powers of surveillance. Adherence to the core European data protection principles is also critical to an evaluation of whether a state's intrusion into the private life of its citizens is proportionate to its security objectives.

7. BIBLIOGRAPHY

Agrell, W. (11 July 2008). Regeringen borde talat klarspråk. *Expressen*.

Al-Shawi, A. (2011), Data mining techniques for information security applications. *WIREs Comp Stat*, Volume 3, 221–229.

Arthur, C. (2011). «What's a Zettabyte? By 2015, The Internet Will Know, says Cisco,» Technology Blog at The Guardian UK Newspaper retrieved at http://www.guardian.co.uk/technology/blog/2011/jun/29/zettabyte-data-internet-cisco

Brunst, Phillip. (2009). Terrorism and the Internet. In: Wade, Marianne / Maljevic, Almir (ed(s).): A War on Terror? The European Stance on a new threat, changing laws and human rights implications. New York, Springer, p. 51 - 78.

Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals, National Research Council. (2008). Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment. The National Academic Press.

Cloete, L. (2012). Dark Web: Exploring and Data Mining the Dark Side of the Web. Online Information Review, Vol. 36 (Issue 6), pp.932 – 933.

Chen, H. (2011). Dark Web: Exploring and Data Mining the Dark Side of the Web. *Integrated Series in Information Systems*. Springer.

Chen, H. (2006). Intelligence and Security Informatics for International Security: Information Sharing and Data Mining. *Integrated Series in Information Systems*, Volume 10, 55-73. Springer.

Custers, B. (2013). Data Dilemmas in the Information Society: Introduction and Overview. In Bart Custers, Tal Zarsky, Bart Schermer, Toon Calders)(eds.), *Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases.* Springer.

Fox News. (November 11, 2007). Internet Tool Hopes to Capture Online Terrorists. Associated Press.

Goold, B. (2009). Liberty and others v The United Kingdom: a new chance for another missed opportunity. *Public Law*, 5-14.

Golumbic, M.C. (2008). *The Balance Between Security and Civil Rights in Fighting Terror Online* Springer, 15-61.

Han, J. and Micheline Kamber. (2006). *Data Mining: Concepts and Techniques (Second Edition).* San Francisco: Morgan Kaufmann Publishers.

Hsinchun Chen, Dark Web: Exploring and Data Mining the Dark Side of the Web (Integrated Series in Information Systems) (Springer 2011).

Klamberg, M. (2010). FRA and the European Convention on Human Rights- A Paradigm Shift in Swedish Electronic Surveillance Law. Nordic Yearbook of Law and Information Technology, pp. 96-134.

Knight, J. SIGINT (Signals Intelligence), in Encyclopedia of Espionage, Intelligence, & Security retrieved at http://www.espionageinfo.com/Se-Sp/SIGINT-Signals-Intelligence.html (defining signals intelligence).

Kuner, C. Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson. (2012). The Challenge of 'Big Data' for Data Protection.» *International Data Privacy Law* Vol. 2(2), 47.

Last, M. (2008). Data Mining. In L. A. M. Colarik & J. Janczewski (eds.), Cyber Warfare and Cyber Terrorism (pp. 358-365). Hersbey, PA: Information Science Reference.

Last, M and Alex Markov, Abraham Kandel. (2008). «Multi-lingual Detection of Web Terrorist Content in Intelligence and Security Informatics Studies.» In *Computational Intelligence*. Vol. 135, 79-96.

Lipton, E. and Eric Lichtblau. (September 23, 2004). Even Near Home, a New Front Is Opening in the Terror Battle, *The New York Times*.

Lloyd-Williams, M. (1997). Discovering the Hidden Secrets in Your Data - the Data Mining Approach to Information, *Information Research: An International Electronic Journal* available online at http://informationr.net/ir/3-2/paper36.html

Lyon, D. (2001), Facing the Future: Seeking Ethics for Everyday Surveillance. *Ethics and Information Technology*, Volume 3, number 3, 171-180

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, California: Stanford Law Books.

Observations of the Government of Sweden on Admissibility, Application no. 35252/08 Centrum för rättvisa v. Sweden (ECtHR). Retrieved at http://centrumforrattvisa.se/wp-content/uploads/2012/09/Regeringens-svar-FRA.pdf.

Palfrey, J. (Winter 2008). *The Public and the Private at the United States Border With Cyberspace*. Mississippi Law Review, Volume 78, 241.

Ramasastry, A. (January 7, 2004). *The Safeguards Needed for Government Data Mining*. Retrieved from http:// writ.news.findlaw.com/ramasastry/20040107.html.

Ramasastry, A. (2006). Lost in Translation? Data Mining, National Security and the 'Adverse Inference' Problem. Santa Clara Computer & High Tech Law Journal, Vol. 22:4, 757.

Regan, P. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: The University of North Carolina Press.

Riese, B. (2008). Mind what you say. *European Lawyer*.

Schneier, B. (March 2006). Why Data Mining Won't Stop Terror. Wired Magazine. (contending that data mining is not useful for identifying individuals planning terrorist activities).

Sieber, Ulrich, Brunst, Phillip. (2007). Cyberterrorism and Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions. In: Council of Europe (ed(s).): Cyberterrorism – The use of the Internet for terrorist purposes. Strasbourg, Council of Europe Publishing.

Seifert, J.W. (Dec. 16, 2004).Data Mining: An Overview. *Congressional Research Service* 1.

Solove, D. (2011). *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven: Yale University Press.

Taipale, K.A. (2003). Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data. *Columbia Science & Technology Law Review*, 1-229.

Taipale, K.A. (2004-2005). Technology, Security and Privacy: The Fear of Frankenstein, The Mythology of Privacy and the Lessons of King Ludd. *Yale Journal of Law and Technology*, Volume 7, 123.

Thuraisingham, B. (2009). Data Mining for Security Applications and Its Privacy Implications, Privacy, Security, and Trust. *KDD Lecture Notes in Computer Science*, Volume 5456, pp 1-6.

Thuraisingham, B. (15-18 Sept. 2009). Data Mining for Malicious Code Detection and Security Applications. *Web Intelligence and Intelligent Agent Technologies*, 2009. WI-IAT '09. IEEE/WIC/ACM International Joint Conferences.

US Department of Defense. (March 2004). *Safeguarding Privacy in the Fight Against Terrorism*, The Report of the [Department of Defense] Technology and Privacy Advisory Committee.

Van den Hoven, J. (2007). Information Technology, Privacy and The Protection of Personal Data. In *Information Technology, Privacy and The Protection of Personal Data*. Cambridge: University Press.

Waters, R.C. (February 1997). An Internet Primer. *Federal Lawyer*, Vol. 44, 33.

Weimann, G. (Spring 2005). How Modern Terrorism Uses the Internet. *The Journal of International Security Affairs*, Vol. 8.

Westin, A. (1967). *Privacy and Freedom*. New York: Atheneum.

Zarsky, T. (2013). Transparency in Data Mining: From Theory to Practice. *Discrimination and Privacy in the Information Society: Studies in Applied Philosophy, Epistemology and Rational Ethics*, Volume 3, 301.

– (Feb. 23, 2004). *Controversial Government Data Mining Research Lives On*. Retrieved from http:// www.siliconvalley.com/mld/siliconvalley/news/editorial/8022436.htm.

– (2004). *Getting Up to Speed: The Future of Supercomputing*. Washington, DC: The National Academies Press.

– (2008). Case: Liberty v United Kingdom (58243/00). *European Human Rights Law Review*, Vol. 6, 788-792.

Statutes

– Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950.

– European Union, *Charter of Fundamental Rights of the European Union*, 7 December 2000, Official Journal of the European Communities, 18 December 2000.

Cases

– ECtHR, *Centrum för rättvisa v. Sweden, Application no. 35252/08*, ECtHR, lodged on 14 July 2008.

– ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Judgment, 29 June 2006, Para. 80.

– *ECtHR, S. and Marper v. the United Kingdom*, Applications nos. 30562/04 and 30566/04, Judgment, 4 December 2008.

– ECtHR, *Liberty and Others v. the United Kingdom*, (Application no. 58243/00), Judgment, 1 July 2008., para. 16.

10

BIG DATA: A CHALLENGE FOR DATA PROTECTION

Philipp E. Fischer
Ph.D. candidate (IN3 Research Institute, UOC Barcelona),
LL.M. in intellectual property law (Queen Mary University of London / TU Dresden)

Ricardo Morte Ferrer
Lawyer (Abogado), Master of Laws (UOC)
Tutor for law studies (Grado en Derecho) at the UOC
Legal adviser for the TClouds Project at the ULD, Kiel

ABSTRACT: We live in the era of «Big Data». In many areas, significantly growing quantities of data are being collected and processed in digital form, either by the technical progress (Cloud Computing, Data Analysis, Data Mining) or through social development (social networks, RFID). Questions like «Who owns this data» and «Who can use this data and for what purposes?» will undoubtedly arise in the near future because many experts agree that Big Data is a new market with specific values («data is the new oil»[1]).

In order to make more profit, the Spanish telecommunications group Telefónica now dares to approach its best-kept treasure: customer data. In early October, the Telefónica group founded –in Germany largely unnoticed– a new division in London. This business unit called «Telefónica Dynamic Insights» has been chosen to dig, drill and pan for gold within the mountain of customer data of O2 Germany, a direct subsidiary of Telefónica. As the first group in Europe, Telefónica combined inventory data –e.g. age and sex– with transaction data for the advertising industry.

Big Data projects, such as O2´s «Smart Steps» are just the beginning. The recently announced SCHUFA (the biggest German credit investigation company) project aiming at the evaluation of data from social networks to assess the creditworthiness and the analysis of 52 million anonymous patient records in the UK show the potential of Big Data, but also the risks from a data protection perspective.

All these data controllers argue to «comply with the respective data protection regulations». Data protection advocates, practitioners and authorities doubt it. Under German and Spanish data protection law, Big Data methods could probably be permitted in a number of cases. The legal challenges are to assess in which contractual relationships the data processing is necessary, to provide effective consent and to apply suitable methods for Privacy-preserving Data Mining. Above all it is important to examine the legality of a Big Data application already in the course of the elaboration of a business case and through «Privacy by Design» principles because legality frequently depends on the design of the process.

The focus of this paper will be to highlight the current German, Spanish and European legal as well as practical approaches to the issue of Big Data from a data protection perspective.

KEYWORDS: Big Data, Data Analytics, Data Protection, Privacy, Legal Framework, Germany, Spain, Consent, Data Subject, Cloud Computing, European Data Protection Directive, General Data Protection Regulation, Privacy by Design, Privacy by ReDesign.

1 (Rath, J., 2012).

1. BIG DATA: CHALLENGES AND OPPORTUNITIES FOR TODAY´S SOCIETY

1.1. Term of Big Data

Big Data is not just the processing of huge amounts of data. The term Big Data refers to the collection and use of decision-relevant knowledge from different data sources. This may include information from a range between proprietary databases and the free Internet. This data is also subject to a rapid change and is being collected in an unprecedented scale.

Big Data is not a single new technology. The term includes a bunch of concepts, methods, technologies, IT architectures and tools that help to direct a huge amount of information into the right channels; so to say, techniques and technologies that make the handling of data at an extreme scale affordable.

Big Data represents a new level of handling data –characterized by the 4 V´s[2]:

- Variety: different formats that make integration challenging,
- Variability: variable interpretations that confound analysis,
- Volume: approaches or exceeds limits of vertical scalability and
- Velocity: decision window small compared with change rate.

The combination of these features is at the same time the challenge and innovation of Big Data.

1.2. Commercial relevance

Data is a new form of value. In the digital world, it appears as the fourth factor of production in addition to capital, labor and raw materials. Therefore, data is sometimes named as the «oil of the future». The value is not the data itself, but the insights that can be derived from the predominantly unstructured data through a new method. This scientific discipline is called «analytics». Its global sales in 2012 amounted to about 4.6 billion euros, as a calculation of the Experton Group showed.[3] The growth of this market segment will reach more than 30 percent - annually. Companies that process large amounts of data, such as banks or insurance companies, rank IT assets now at the «core of their business». Big Data technologies play an important role in such departments wherever qualitatively different data is being collected in high volumes; so in research and development, production, distribution and logistics, finance and risk control as well as in marketing and sales.

---

2 (IBM Newsroom, 2012).

3 (Gerick, T., 2012).

1.3. Everyday application examples

The applications of Big Data are already countless and affect all aspects of the consumers´ daily routine, e.g.:

Smart grids: Energy consumption can be controlled via smart meters and other facilities in order to shift peak loads. For this purpose, data on energy consumption, network utilization, current electricity production and price information is constantly collected. Its analysis through Big Data methods allows a much more efficient energy management for both providers and consumers.

Intelligent transport systems: Through the analysis of various data sources such as traffic, weather or large public events, traffic can be properly directed and traffic jams be managed. That protects not only drivers but also the environment.

Health sector: The analysis of anonymized health data helps to use better targeted therapies and drugs. In the UK, medical records of about 52 million people will be centralized and used for medical research purposes. Subsequently, this database will be supplemented by additional information, including social data and data related to industrial pollution.

Search engines: Personalized search operations on Google or Facebook are also analyzed, e.g. with which persons the user socializes, for which sites he shows his interest. This data is being linked by Google and Facebook with every snippet of information these companies do know about the seeker.

Dynamic and usage data: Last fall, an outcry went through the public, as Telefónica announced their intention to sell the dynamic data of its German customers (company «O2 Germany», a Telefónica subsidiary). Because of public protest O2 has withdrawn his plan. Telecom Italia tries to analyze on the basis of call –and message– connections of their customers, to whom they are connected as closest in order to identify different social roles within communities. This knowledge is then matched with information on contract changes and important customers can be targeted to prevent a provider switch or to attract new customers.

1.4. Social challenges and opportunities

These examples illustrate the importance of Big Data. On the one hand it could help to tackle major social challenges of the present and the future:

- Big Data creates additional transparency through the analysis of existing data. More transparency will contribute to better informed decisions and gives impulses to innovations.
- Big Data improves customer access. Companies can use the information gained to better customize their services to specific customer segments and needs.

- Big Data supports the decision-making processes. The analysis of extensive data in real time, known as «embedded analytics», reduces business risks and improves business processes.
- Big Data enables advanced simulations. Experiments with performance data that is collected in real time provide better results.
- Big Data shows opportunities for new business models, products and services.

On the other hand, for example, medical records are particularly sensitive and must be protected. The protests against the analysis of dynamic data or of activities in social networks show that consumers feel uncomfortable whenever it comes to a possible evaluation of their personal data. The social challenge is to try not to just dig for gold among these «data resources» but to think about possible breaches of privacy rights, especially the right to informational self-determination and to find solutions to balance this conflict.

2. PERSONAL DATA AMONG BIG DATA SOURCES

«Personal data» means any information relating to an identified or identifiable natural person («data subject»); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (Art. 2 a EU-DPD[4]).

Among Big Data sources this personal data can be affected in the course of the processing of the whole data fraction, which then raises privacy concerns, as some commentators have put it: «When thinking about the importance of 'big data', it is critical to remember that access to so much data, from so many different sources, and to the computing power necessary to process it, increasingly means we can perceive patterns, engage in discoveries, and discover secrets that were heretofore hidden.»[5] Analyst Jeffrey Chester notes that «Big data is both a boon and a curse for users. Tens of thousands of data sources on individuals can be compiled in milliseconds. The profiles allow marketers, politicians and businesses to predict consumers' futures, whether we will be a big and low-wage lifetime earner, how we may respond to medical concerns, and whom we can be persuaded to vote for.»[6] What happens when even fractions of analyzed Big Data

4 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data («EU-DPD»), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

5 (Kuner, C., Cate, F., Millard, C., Svantesson, D., 2012, p. 47 - 48)

6 Jeffrey Chester, in (Gross, G., 2013)

fall into the wrong hands? Granted, the following indicative list of threats to personal data is somehow a collection of worst case scenarios, but should be anyway quoted at this point as «cautionary tales»:

- Patient records: Patient records falling into the hands of unauthorized persons can have a massive disadvantage to those being involved, e.g. the loss of a job.
- Search functions: It somehow changes social relations if it becomes possible to spotlight on people according to their specific preferences. Or it could lead to a denied bank loan or the refusal of similar contracts because the possible creditor has collected and analyzed personal data in order to check the customer's credit worthiness.
- Dynamic data: Knowledge of regular absences from home may e.g. be used for burglary. Dynamic data also allows even a complete supervision. If such data is freely offered for sale to anyone, any witness protection program could become ineffective.
- Evaluation of telecommunications data: The purpose of the data processing is already questionable. Telecommunications data is especially protected; the evaluation of costumer data for the purposes of customer acquisition must therefore be necessary and proportionate.

3. PERSPECTIVES AND LEGAL FRAMEWORKS FOR BIG DATA

3.1. German perspective

Big Data can only become a successful method in Germany if at the same time personal data is processed in accordance with German data protection laws.

3.1.1. Principles of the Federal Data Protection Act

Each data processing has to comply with the concept of data protection provided in the «Bundesdatenschutzgesetz»[7] (BDSG), the German Federal Data Protection Act. Three of the most important principles within the German concept of data protection are:

- Prohibition principle, Section 4 (1) BDSG: Personal data may only be collected, processed or used if the individual has given his prior consent or if a legal provision explicitly allows this.
- Principle of purpose, Section 3a BDSG: Personal data should be collected and processed for specified and explicit purposes.

7 Bundesdatenschutzgesetz as of 1 September 2009 («BDSG»), http://www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile

- Principle of data minimization, Section 3a BDSG: It should be processed as few personal data.

This does not mean that the processing of personal data within Big Data sources is in any case inadmissible under German law. Some examples[8] fall within the following categories and do allow the processing:

- The processing due to a person's consent,
- Data processing in contractual relationships, and
- Privacy-preserving data mining.

3.1.2. Fraud detection and credit scoring

One of the biggest problems of online payment services and credit card companies is the abuse through fraud. PayPal has developed the software application «Igor» to prevent such fraud and has thus become one of the most successful payment services. Visa and MasterCard also run powerful software to identify suspicious payments.

Under German data protection law, the use of fraud detection applications is generally admissible, because the processing of personal data is necessary so that the payment service provider can perform the contract; the service provider has to protect its customers from abuse of credit or debit cards.

Big Data improves the ability to find patterns in payment behavior and to immediately respond to anomalies. The more powerful the analysis, the better for the customer: It impedes fraud as well as erroneously positive cases. Payment service providers who use fraud detection must ensure that the data will be used only for this purpose and provide adequate data security measures.

Another example is credit scoring. A bank must, before deciding on a loan, evaluate the creditworthiness of its customers. For this purposeinformation on profession, income, wealth, previous payment history, etc. of the particular customer is evaluated.. In contrast to these relatively few parameters, some U.S. credit providers use scoring methods with thousands of indicators. Almost every business case processes personal data in advance of the agreement, or to settle contracts. The legal challenge under German law then is to examine in each individual case and to explain why the use of this particular customer data is required for the conclusion or performance of a contract.

3.1.3. Customer retention systems

Tesco, a large British supermarket chain, evaluates data collected whilst customer purchases to subsequently send coupons with tailor-made offers. Under German data

8 See 3.1.2, 3.1.3 and 3.1.4

protection law, it is legitimate to use customer databases to advertise products. Although advertising is no longer necessary to fulfill an existing contract, the company has a legitimate interest to inform customers about its range.

If a company wants to, however, create customer profiles by using data mining methods that enable targeted advertising, the consent of the customer to the analysis of his personal data is required. The legal prerequisites to obtain this consent are high. Consent to process the personal data may be included within the terms and conditions but must be highlighted within the text. The customer must then delete the respective text passages he does not agree with (opt-out). If the company wants to advertise products via e-mail, the customer must expressly agree, for example, by ticking this separately (opt-in). It is difficult to grasp the consent to such an extent that it covers all evaluations of personal data, but at the same time precisely clarifies the extent of the processing –otherwise it does not meet the legal criteria of an informed consent. Mere general phrases like «for the purpose of advertising» neither meet this requirement.

3.1.4. Privacy-preserving data mining

The BDSG applies to «personal data» only. Data without any reference to an identifiable person is not measured, e.g. technical data, such as product data, does not fall within the scope of the BDSG. A major German market research company collected data about the purchasing behavior of 15.000 households on a high-detail-level, but further processed anonymous data only. This privacy-preserving data mining not only increases the consumers' willingness to disclose information, but it makes it also much easier to comply with data protection laws.

«Anonymization» means to alter the data so it can no longer be determined to which person it refers. Its methods usually are to delete all identifying characteristics or to aggregate characteristics, for example, by replacing the address through the date of birth. It is not even necessary to completely delete the personal-related data in its first output state. An anonymized data set, derived from the raw data set can be lawfully passed to a third party as long as the third party is not able to restore the relation between raw and anonymized data. For this purpose one must meet contractual agreements that also factually exclude a merge. It also has to be considered that the third party does not have additional knowledge to deanonymize the data and that this additional knowledge cannot be attained.

Another method is to work with aliasing. Aliasing shall mean replacing the data subject's name and other identifying features with another identifier in order to make it impossible or extremely difficult to identify the data subject. This has the advantage that data can be further processed as a profile, which is important, for example, in medical research, when medical records are evaluated and longitudinal studies created.

There are different degrees of aliasing:

- One-way-aliasing, for example by assigning hash values without reversal possibility. In this case the data is generally losing its character as personal data and becomes anonymous data.
- The owner of a database created alias and assigned them to a reference table, which he keeps in his possession, so for him the data is still personal-related. He can pass on the aliased data to a third party, for which the data is not personal unless the content of the reference table is disclosed.

Privacy-preserving data mining is not only suitable for market research but also for web tracking, or in areas such as medical research, where special categories of personal data are processed. However, the use of privacy-preserving data mining is a challenging task. It is still controversial whether some data categories, such as dynamic IP addresses, are personal-related. Regarding anonymous data, the risk must be assessed, that it eventually can be merged with other data.

3.2. Spanish perspective

Due to the limited length of this paper we will focus on the following points: the principle of data quality, the consent of the data subject and data access for third parties.

3.2.1. Principle of data quality

The principle of data quality is included in Article 4 LOPD[9] and requires that a data collection is performed for a particular purpose and that this data may not be used for purposes incompatible with those for which it has been collected. It also requires that once exceeding the original purpose, data cannot be stored for a longer period than it is necessary to fulfill the original purpose. It seems clear that this principle is problematic for the use of Big Data methods, which involve the further use of data for purposes not directly related to the original collection. That does not implicit that those methods are impossible, but it requires the establishment of regulatory mechanisms that allow an adequate control.

Anexample of what should not happen poses an application[10] filed by IBM that uses large amounts of data to help detect internal and external risks, controlling social media and email, allowing to detect employees that may pose a risk, for example in the

9 La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal («LOPD»), http://www.agpd.es/portalwebAGPD/english_resources/regulations/common/pdfs/Ley_Orgaica_15-99_ingles.pdf

10 Part of the «Smarter Analytics» program, see (IBM Newsroom, 2012)

field of industrial espionage. An internal IBM Newsroom document explains the process: «By analyzing email you can say this guy is a disgruntled employee and the chance that he would be leaking data would be greater»[11]. And «a company could analyze employee emails that express a positive sentiment to a manager at work, but detect when he's talking to a peer or someone outside the company, the sentiment comes out a little different.»[12]

3.2.2. Consent of the data subject

LOPD article 6.1 provides: «The processing of personal data shall require the unambiguous consent of the data subject, unless laid down otherwise by law.» This aspect somehow repeats the problem mentioned in the previous point because the consent is granted for a specific treatment and cannot constitute blank consent that allows further treatment of personal data.

It is worth considering whether the legal instrument of consent is still applicable in cases where the data subject is in a weak position against organizations that have access to his data, especially when that person does not have sufficient information to give a free and informed consent, a prerequisite for its validity. It seems clear that in cases where the business model of a company is based on a collection, processing and usage of big and indiscriminate amounts of data, consent is not the appropriate instrument to validate the treatment of data. That problem could be solved only if this company would be able to provide sufficient transparency for a valid consent. It should be mentioned the case of Telefónica´s «Smart Steps», which «is dedicated to measure the movements of their subscribers. Based on this data, the traders will know, for example, the exact time and day whenever a teenager buys, which could help them capitalize on their promotions»[13][14] explained Stephen Shurrock, commercial director of Telefónica Digital. Shurrock said that some dynamic data is already used for services such as traffic management, but advances in computer storage and analysis resulted in large amounts of data (Big Data), which could be further exploited. Telefónica has partnered with GfK[15], dedicated to market research, to launch the service, which will be available in the UK and Brazil later this year whilst in Germany the attempt was stopped before the outcry.

But, in the midst of the development and deployment of Big Data, there are movements from consumers, data protection authorities and organizations of consumer

11 (Schectman, J., 2013)

12 (Schectman, J., 2013)

13 (El País, 2012)

14 (Dans, E., 2012)

15 http://www.gfk.com/

protection; the opposition on the side of the consumers seems to be growing . The latter have long thought they were protected by the law, but are gradually realizing that the security level is lower than expected.

A possible alternative could be a legal regulation to establish an appropriate legal framework for the processing of personal data whenever consent is impracticable. Unfortunately the legislature has, so far, not shown the pace needed, given the rapidness with which technological innovations are developed and implemented.

Another alternative, not necessarily easy but more plausible than the last, could be the implementation of authorization procedures for the development of data processing in which consent is not applicable. Procedures would then need to be raised much faster than the legislative process. One possibility could be to instruct the data protection authorities to establish documentation requirements and / or certifications required from organizations or businesses that request such authorizations.

Regarding the authorization procedures, we could differentiate two types: a) authorization procedures based on the type of codes of practice and codes of conduct and b) standard procedures for authorization. The essentials for a possible release of the second type would be the existence of special risks for personal data arising from a manifest imbalance between the data subject and the company that processes his personal data, large numbers of data subjects or the existence of particularly complicated procedures. One might ask whether any of these solutions are applicable to the case of Facebook, where the user´s consent touches all the problems discussed, since the user does not have all information to give his - properly informed - consent. An additional problem is that Facebook has a virtual monopoly, which means there are no real alternatives and that freedom of consent is limited if we also take into account the importance of wide ranged social networks.

3.2.3. Data access for third parties

Article 12.2 LOPD provides: «Processing on behalf of third parties shall be regulated in a contract which must be in writing or in any other form which allows its performance and content to be assessed, it being expressly laid down that the processor shall process the data only in accordance with the instructions of the controller, shall not apply or use them for a purpose other than that set out in the said contract, and shall not communicate the m to other persons even for their preservation. The contract shall also set out the security measures referred to in Article 9 of this Law, which the processor is obliged to implement.»

Big Data itself raises serious control difficulties, which makes it very difficult to determine the respective controller and thus to apply the model of collection, processing or use of personal data on behalf of others. As mentioned above, this does not mean a direct ban on Big Data methods, but requires the application of specific mechanisms

that enable compliance with the requirements of current legislation on data protection. Apart from the possible authorization procedures mentioned in the previous point, other mechanisms as Binding Corporate Rules or self-regulatory procedures could be applicable, build a legal basis and should be developed as quickly as possible.

3.3. European perspective

The EU-DPD is facing the same problems as the LOPD, as it is also focused on the data subject and on instruments such as consent, issues we have already addressed. The proposed «General Data Protection Regulation»[16] is currently in process and under strong pressure by the big business lobby of Information Technology and - Communication, who consider it a danger to their business model. Essential criteria in this Regulation are achieving regulatory harmonization at a European level and are improving the protection of the concerned persons. Although at some points it still has to allay fears that the first criteria basically attempts to improve the situation of companies, which confronts the proposed regulation with the second criteria and brings up a certain lack of coherence.

For these reasons it seems clear that European law is recurring problems in Spanish law. For example, the proposed regulation seeks to enhance the position of the person concerned by strengthening the concept of consent in Article 7.4; the latter provides that consent is not a legal basis for data treatment whenever there is a manifest imbalance in the relationship between the subject affected and the controller. It is a laudable attempt, but is not in the true center of the problem because it does not recognize that in many cases consent can only bring a semblance of legal certainty. Apart from the instruments mentioned in the previous point would strengthen measures from the point of view of Privacy by Design (PbD), Privacy by ReDesign (Pb^RD) and –generally speaking– other Privacy Enhancing Technologies (PETs).

Kuner, Cate, Millard and Svantesson, editors of the International Data Privacy Law Journal also ascertained defects:

> «Consider, for example, the fascination shown by the EU data protection directive and the proposed EU General Data Protection Regulation, similarly to law in most of the rest of the world, with 'notice' and 'choice' or 'consent' as key tools of data protection. Despite mounting evidence that individuals ignore notices, often do not understand the choices (which often aren't meaningful in any event), and resist making them unless compelled to do so (in

16 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), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

> which case they almost always make the choice required to obtain the desired service or product), regulators continue to cling to these concepts. But irrespective of the success of notice and choice to date, how will these tools fare in a world of ubiquitous surveillance, and thousands of data exchanges by and about every individual on the planet every day? In short order the largest database on the planet may be of legally required privacy notices that no one has read. Even where legislative drafters demonstrate awareness that data processing on a very large scale may raise particular concerns, evidence that the practical risk implications are understood may be lacking. For example, the draft EU General Data Protection Regulation provides for an exception to the general prohibition on transfers of personal data to countries that lack adequate protection where a transfer 'cannot be qualified as frequent and massive'. While the use of the term 'massive' hints at an appreciation of the challenge of big data, no attempt is made to define the concept or even to put it in a relative context.»[17]

3.4. International perspective[18]

Big data methods also arouse from sleep the discussion on (lacking) harmonization, or even standardization, in data protection standards. As personal data is universally collected, processed and used across federal and national boundaries, inconsistent data protection laws pose increasing threats to individuals, institutions, and society. Kuner, Cate, Millard and Svantesson state that «perhaps the greatest impact of big data is the pressure it brings for new thoughtful, informed, multinational debate about the key principles that should undergird data protection»[19]. Most data protection laws continue to rely on the 1980 OECD Guidelines[20] and it will be deeply interesting how international bodies identify common principles to undergird future data protection laws.

4. PROTECTING PRIVACY RIGHTS IN THE AGE OF BIG DATA

The legal challenges are to assess which data processing is necessary, to provide valid consent and apply suitable methods for privacy-preserving data mining. Above all it is

17 (Kuner, C., Cate, F., Millard, C., Svantesson, D., 2012, p. 48)

18 For a detailed analysis of the international framework see (Fischer, P., 2012)

19 (Kuner, C., Cate, F., Millard, C., Svantesson, D., 2012, p. 48)

20 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980, http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

important to examine the legality at the development of a Big Data method. The legal admissibility depends already on the design of the method. Therefor both actors as well as technical measures have to work together.

4.1. Actors

4.1.1. Policy

The political challenge is to find a legal framework for new types of data processing that allow both the use of Big Data and the protection of privacy rights. We are convinced that we need a high level of data protection as the basis for trust in electronic services. Legal provisions should be in the end close to a tried-and-tested best practice.

But it would be of little help if, under the provisions of data protection law, the processing of data becomes unattractive and difficult. Having a look at the revision of the European data protection framework one sometimes get exactly this impression. The already narrow corridors of admissible data processing are to be further narrowed and overburdened with additional, bureaucratic requirements. That seems to be far from being the solution for the digital world.

Privacy is important, but it must not become an end in itself. Data processing operations must be allowed to conduct daily business, meaning with the latter no complicated financial transactions but rather an order from online retailers or the appointment of a craftsman. As long as consumers are not threatened with serious drawbacks, the hurdles for the processing of their data should not be too high. This balancing act could be observed in the negotiations to the General Data Protection Regulation which will have a significant impact on Big Data methods and applications:

- The obligation to «Privacy by Design»[21]
- The establishment of the figure of explicitly consent

4.1.2. Provider

Provider companies struggle to assess whether a particular data processing is legal or not; but that is no reason to abdicate responsibility. The big amount of data leads to an aggravated risk for personal data, e.g. abuse and data breach. Even before the implementation of Big Data projects, providers must therefore assess these risks. In early project stages they need to consider its legality during the development of a Big Data method and structure the design process so that no privacy issues arise in the operation phase. The technical design should exclude the risks as much as possible. This means not only data security at a high level but also an evaluation of just this personal data,

21 See 4.2.2.

which is needed for the desired purpose. The self-determination of the data subjects must be respected, particularly when the purpose can only be achieved if individual records –possibly even without a name– can be isolated; this may be partly necessary in medical research issues. This usually requires the explicit consent of the data subject, as an adequate anonymization is impossible in these cases.

4.1.3. Consumer

Consumers should carry on using their market power. Their protests may sometimes lead companies to change their plans. To give just one example: Users protested against a modification of the terms and conditions that would have allowed the photo service «Instagram» to commercially use users´ uploaded photos; the user rate declined rapidly.[22]

4.2. Technology

4.2.1. Anonymization and aliasing

As mentioned above, the pivotal point of Big Data applications will usually be the anonymization of personal data. Many purposes can be achieved by using anonymous data. Also the use of aliased data could be permitted under alleviated conditions to provide an incentive for business models based on data usage.

4.2.2. Privacy by (Re)Design

Other solutions could offer the concepts of «Privacy by Design» (PbD) and «Privacy by ReDesign» (Pb^RD). The author of these principles was the Privacy Commissioner of Ontario, Canada, Ms. Ann Cavoukian.

PbD takes the view that the future of privacy can be assured not solely by compliance with the law, but data protection should become the standard mode of operation. PbD can be seen as the further development of PETs through the inclusion of a positive-sum approach (full functionality). PbD extends to a «trilogy» of applications: 1) IT systems, 2) business practices, and 3) physical design and networked infrastructures. The principles of PbD are applicable to all kinds of personal information, but they should be used with particular emphasis on «sensitive data» (the German Federal Data Protection Act calls it «special categories of personal data») such as certain medical and financial data, thus the intensity of the data protection measures must be adequate to the sensitivity of the data.

22 (Münzel, R., 2012)

The objectives of Privacy by Design –ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage– may be accomplished by practicing the 7 Foundational Principles.

«1. Proactive not Reactive; Preventative not Remedial

The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

2. Privacy as the Default Setting

We can all be certain of one thing – the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

3. Privacy Embedded into Design

Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum «win-win» manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Security – Full Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency – Keep it Open

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component

parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy – Keep it User-Centric

Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.«[23]

Many organizations operate with existing, sophisticated IT systems and business practices that they have developed over the years and which are inextricably linked to everyday business processes. It is usually not on their agenda to replace such systems. Responsible for the implementation of PbD in such systems is then Pb^{R}D, an extension of PbD. It must be the aim of getting closer to the final state of PbD, the highest standards for the protection of personal data. This should, according to the Ms. Cavoukian be supported by the «3 R's» of Pb^{R}D: «Rethink, Redesign, and Revive.»

New developments within the business may open windows of opportunity to either implement or improve privacy protection in existing aspects of the system, or to make choices about new system components that support responsible information management practices and render privacy the default condition. These are opportunities to Rethink, Redesign, and Revive aspects of the system, in whole or in part, based on the 7 Foundational Principles of PbD

«1. Rethinking invites organizations to review their risk mitigation strategies, existing systems, and processes –including information technologies, business practices, physical design, and networked infrastructure– and consider alternative approaches that are more privacy-protective. This may include revisiting assumptions about how much personal information is necessary for the system to operate, and how long it needs to be retained in identifiable form.

2. Redesigning represents the opportunity to enable or implement improvements in how the system functions from a privacy perspective, while also ensuring that it continues to achieve key business requirements in a doubly-enabling positive-sum, win/win relationship. Redesigning may likely require that less data be collected, and these changes may need to be cascaded back to stored databases where possible, to delete these unnecessary fields of data.

3. Reviving the system in a new, privacy-protective way is the ultimate goal!»[24]

23 Cavoukian, A., 2013, 7 Foundational Principles

24 Cavoukian, A., 2013, Privacy by ReDesign: Building a Better Legacy

As mentioned above, the current draft of the European General Data Protection Regulation includes the obligation to engage in technical and organizational measures. This means a significant progress for the acceptance of Pb^{R}D since «data protection by design and by default» as directly applicable law within the EU / EEA.

5. PROSPECTS

The scientific discussion about Big Data is just starting. In public, however, the topic is becoming increasingly important. Over the recent weeks there have been detailed background reports in the media. It's not just about the specific benefits of certain Big Data applications and the associated risk but it is also about the question in what kind of society we want to live. We need a broad discussion on how our society could suffer sensible changes, if our everyday behavior can be recorded and analyzed immediately or after a long time and how we want to deal with this change.

6. BIBLIOGRAPHY

Cavoukian, A. (2013). *7 Foundational Principles*. Retrieved March, 9th, 2013 from http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

Cavoukian, A. (2013). *Privacy by ReDesign: Building a Better Legacy*. Retrieved March, 9th, 2013 from http://privacybydesign.ca/content/uploads/2011/05/PbRD.pdf

Dans, E. (2012). *Tracking, publicidad y miedos*. Retrieved March, 9th, 2013 from http://www.enriquedans.com/2012/10/tracking-publicidad-y-miedos.html

El País (2012). *Telefónica venderá al comercio los datos de sus abonados*. Retrieved March, 9th, 2013 from http://tecnologia.elpais.com/tecnologia/2012/10/09/actualidad/1349766361_669426.html

Fischer, P. (2012). Global Standards: Recent Developments between the Poles of Privacy and Cloud Computing. *jipitec, 3* (1). urn:nbn:de:0009-29-33215

Gerick, T. (2012). *IT Analytics. Wege aus der Black Box*. Retrieved March, 9th, 2013 from http://www.manageit.de/Online-Artikel/20120910/f%20IT%20Analytics.htm

Gross, G. (2013). *Big data collection collides with privacy concerns, analysts say*. Retrieved March, 9th, 2013 from https://www.pcworld.com/article/2027789/big-data-collection-collides-with-privacy-concerns-analysts-say.html

IBM Newsroom (2012). *Big Data und Smarter Analytics*. Retrieved March, 9th, 2013 from http://www-03.ibm.com/press/de/de/presskit/33005.wss

Kuner, C., Cate, F., Millard, C., Svantesson, D. (2012). The challenge of 'big data' for data protection. *International Data Privacy Law, 2* (2), 47-49

Münzel, R. (2012). Protest im Netz. Bilderdienst Instagram rudert zurück. Retrieved April, 30th, 2013 from http://www.br.de/themen/ratgeber/inhalt/computer/instagram-bilderdienst-datenschutz-100.html

Rath, J. (2012). *Gartner, IBM See Big Market for Big Data*. Retrieved March, 9th, 2013 from https://www.datacenterknowledge.com/archives/2012/10/19/big-data-news-gartner-ibm-teradata/

Schectman, J. (2013). *IBM Security Tool Can Flag 'Disgruntled Employees'*. Retrieved March, 9th, 2013 from http://blogs.wsj.com/cio/2013/01/29/ibm-security-tool-can-flag-disgruntled-employees/

AUTOMATED JOURNALISM: ARTIFICIAL INTELLIGENCE TRANSFORMS DATA INTO STORIES

When data protection principles and privacy protect the right to express opinions freely and to receive accurate information

Cédric Goblet
Lawyer at the Brussels Bar

ABSTRACT: Narrative Science Inc., a company based in Chicago, has developed an artificial intelligence engine called Quill that *«transforms data into stories that are indistinguishable from those authored by people»*. This technology provides us a good opportunity to explore the complex relationship between privacy, data protection and freedom of expression, in the age of the Internet and of Big Data. Furthermore, Narrative Science's project raises questions on the relationship between human and the machine. Paradoxically, the use of a robot writer will not result in greater rationality, but will increase the tendency towards infotainment. More than ever before, the Internet has made the role of journalism a crucial one. Independence, the verification of sources and the search for truth, which are the foundation of journalism, are essential to make sense of the deluge of information we are now exposed to. Protecting journalists' right to freedom of speech, citizens' right to receive quality information, and the right to privacy of readers and users of social networks requires that a distinction be made between journalism and other types of activities. For each of these, specific data processing activities are performed with distinct purposes. The paper will focus on defining these purposes and on identifying the impact their pursuit entails on fundamental rights. The data protection regulation currently in force at both European Union and Council of Europe levels will be examined to determine whether it sufficiently protects these rights. This research will finally lead us to consider how this regulation may be improved.

KEYWORDS: Automated journalism; Artificial Intelligence; Freedom of expression; Right to information; Right to receive information; Privacy; Data protection; Article 9, Directive 95/46/EC; journalistic purposes.

1. AUTOMATED JOURNALISM: THE PROJECT

Narrative Science Inc., a company based in Chicago, has developed a platform called Quill that *«transforms data into stories that are indistinguishable from those authored by people»*[1]. This innovative technology incorporates the latest advances in Ar-

1 Narrative Science's website. Retrieved January, 29th, 2013 from http://www.narrativescience.com/technology (The content of this page has been updated).

tificial Intelligence and Big Data analytics. Initially, this robot writer was only capable to generate content in specific domains where the vocabulary is limited and the stories follow a predictable pattern, such as sport and real estate. Now, it is used by the business magazine *Forbes* to produce financial reports[2]. During the American presidential election, Quill has analyzed twitter traffic related to the Republican primary candidates to output daily articles about the campaign[3]. Progressively, computer intelligence is conquering the domain of political journalism. The massive amount of data available in social media constitutes a particularly interesting information source to achieve this goal.

This powerful technology provides us a good opportunity to explore the complex relationship between privacy, data protection and freedom of expression, in the age of the Internet and of Big Data. Furthermore, Narrative Science's project raises questions on the relationship between human and the machine. Paradoxically, the use of a robot writer will not result in greater rationality, but will increase the tendency towards infotainment. More than ever before, the Internet has made the role of journalism a crucial one. Independence, the verification of sources and the search for truth, which are the foundation of journalism, are essential to make sense of the deluge of information we are now exposed to.

Protecting journalists' right to freedom of speech, citizens' right to receive quality information, and the right to privacy of readers and users of social networks requires that a distinction be made between journalism and other types of activities. For each of these, specific data processing activities are performed with distinct purposes. The paper will focus on defining these purposes and on identifying the impact their pursuit entails on fundamental rights. The data protection regulation currently in force at both European Union and Council of Europe levels will be examined to determine whether it sufficiently protects these rights. This research will finally lead us to consider how this regulation may be improved.

---

2 Bell, E. (2012). The robot journalist: an apocalypse for the news industry? *The Guardian* (May 13). Retrieved January, 29th, 2013 from http://www.guardian.co.uk/media/2012/may/13/robot-journalist-apocalypse-news-industry/print. See also Morozov, E. (2012). A robot Stole My Pulitzer! How automated journalism and loss of reading privacy hurt civil discourse. *Slate Magazine* (March 19). Retrieved February, 11th, 2013 from http://www.slate.com/Articles/technology/future_tense/2012/03/narrat...ists_customized_news_and_the_danger_to_civil_discourse_.single.html.

3 Templon, J. (2012). *Quill Analyzes Presidential Campaign Funding*. Retrieved January, 29th, 2013 from http://www.narrativescience.com/blog/quill-analyzes-presidential-campaign-funding. See also Hammond, K. (2012). *Just to Clarify - Generating stories from social media: Getting to the meat of the tweets*. Retrieved January, 28th, 2013 from http://khammond.blogspot.be/2012/02/generating-stories-from-social-media.html.

2. RELATIONSHIP BETWEEN FREEDOM OF EXPRESSION AND PRIVACY IN THE AGE OF THE INTERNET AND BIG DATA

2.1. Freedom of expression

Ensuring access to a maximum of information to the largest number of people has long been a priority and a condition of democratic development. Technology has made a great contribution to achieve this goal. It is not mere chance that the 19th century represented the golden age of the press. Techniques for the communication and reproduction of information have undergone great developments during this era. The electric telegraph (1837), photography (1839), the telephone (1871) have brought profound changes to social relations and have provided a wider circulation of information[4]. In addition, developments in means of transportation, such as the railways, have played a role in speeding up the distribution of newspapers and information.

Yet this development would have been impossible under Western democracies without a supporting legal framework; and more specifically without enshrining freedom of expression and of press as a fundamental right. Sweden is believed to be the first country to have adopted a law protecting the freedom of the press in 1766[5].

In the Member States of the Council of Europe, article 10 of the European Convention on Human Rights[6] (hereinafter «ECHR»), has played a decisive role in protecting this right for over fifty years. According to this provision, *«everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas»*.

The wording taken from article 10 of the ECHR mentions the right to communicate and receive information as two indissociable facets of the same freedom. Many times over, the European Court of Human Rights tells us that *«not only does the press have the task of imparting such information and ideas: the public also has a right to receive them»*[7]. The reference to this part of freedom of expression denotes a greater inclusion of the role of the recipient of the information. This trend continues with the Internet, where the recipient now acts as an information provider.

---

4 Albert, P. (1970). *Histoire de la presse* (Collection «Que sais-je ?» n°414). Paris: Presses Universitaires de France, pp. 34-35.

5 OECD (2010). *News in the Internet Age: New Trends in News Publishing*. Paris: OECD Publishing, p. 26.

6 Signed in Rome by the Member States of the Council of Europe on 4 November 1950.

7 ECHR, *Sunday Times (No. 1) v. the United Kingdom*, judgment of 26 April 1979, §65. See also case of *Lingens v. Austria,* judgement of 8 July 1986, §41 (All the case-law is available at the Court website, at *http://cmiskp.echr.coe.int*).

The right to receive information essentially places a negative obligation on the State not to infringe on the freedom of receiving information[8]. It is presented as a particular aspect of the right to information, or to be more accurate, as one of the rights to information. The Court does not recognise the guarantee to absolute right to information in article 10. Such an interpretation would enshrine the existence of a general right of access to administrative data and documents[9], and even the unlimited right to know, as is so often claimed by the tabloid press. To avoid any inaccuracy or confusion, I will exclusively use the concept of the right to receive information in the continuation of this study.

The Court has had the chance to apply the principles it has set out in terms of freedom of expression in cases related to Internet. Among these rulings, we can pinpoint the case of *Times Newspapers Ltd v. the United Kingdom.* It stated that: *«In light of its accessibility and its capacity to store and communicate vast amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally. The maintenance of Internet archives is a critical aspect of this role and the Court therefore considers that such archives fall within the ambit of the protection afforded by Article 10»*[10].

2.2. Privacy and data protection

In the second half of the 19th century, legal constructs gradually appeared in Western countries to accompany the swift rise in communication techniques. This progress enabled the distribution of information to such a degree that the intimacy, honour and reputation of individuals could be affected[11]. Excesses of the press at the time were taken into account in the drafting of these new rights.

In Germany, the legal doctrine developed the right of personality (Persönlichkeitsrecht) which can be defined as *«the right of the individual to be an end in itself, to assert itself and to flourish as an end in itself»*[12] and which protects many aspects of human be-

8 Council of Europe, ECHR, Research Division (2011). *Internet: Case-law of the European Court of Human Rights*, 2011, p.20-23. Retrieved February, 5th, 2012 from http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_EN.pdf.

9 *Ibid.*

10 ECHR, *Times Newspapers Ltd v. the United Kingdom (nos. 1 & 2)*, Judgement of 10 March 2009, §27.

11 Rigaux, F. (2004). Protection de la vie privée. In *Répertoire pratique de droit belge* (Tome IX complément). Bruxelles: Bruylant, p.825.

12 Neuner, C. (1866). *Wesen und Arten der Privatrechtsverhältnisse*. Kiel, Schwers'sche Buchhandlung, p.16.

ings, such as image, reputation, honour, health and family issues[13]. In the United States, S. Warren and L. D. Brandeis[14] evoked the concept of *privacy* through not only American, but also English case law. They defined this new right as *«the right to be let alone»*. At the same time, French and Belgian case law witnessed decisions which show certain close similarities with the rulings commented on by Warren and Brandeis[15]. We already see the expression private life (vie privée) in a lecture given by B. Constant before the Athénée Royal in 1819. He said that *«our liberty has to consist of the peaceful enjoyment of private independence»*[16].

The right to intimacy shines through these legal constructs as a common feature, as the heart of Privacy. It is also this aspect that comes from the wording of article 8 of the ECHR, according to which *«everyone has the right to respect for his private and family life, his home and his correspondence»*. For over fifty years, the European Court of Human Rights has played a decisive role in the development of the concept of privacy. It has adopted an extensive and dynamic interpretation[17] of this provision, which has enabled it to move far beyond the strict framework of the right to intimacy. The Court appears to have definitively moved beyond this threshold in the case of *Niemietz v. Germany,* by enshrining *«the right for individuals to establish and develop relationships with other human beings»*[18].

Over the course of cases submitted before the Court, the direction of the right to (informational) self-determination[19], or in other words the right to control over information, is gradually taking shape. The emergence of this new facet of privacy is directly linked to the emergence of information and communications technologies.

Developments in ICT gradually have led to reflection from the 70s onwards[20], and then to the adoption of regulations with regard to the processing of personal data. *Convention n° 108 of 28 January 1981 of the Council of Europe* (hereinafter «Convention n°

13 See references cited by Rigaux, F., *op. cit.*, p. 825.

14 Warren, S.D., Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review*, pp. 193-220.

15 See references cited by Rigaux, F., *op. cit.,* p. 824;

16 Constant, B. (1819). *De la liberté des anciens comparée à celle des Modernes, lecture to the Athénée Royal of Paris in 1819* (Paris: éd. Mille et une nuits - 2010).

17 Sudre, F. (2005). La construction par le juge européen du droit au respect de la vie privée (Rapport introductif). In Sudre, F. (dir.) *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'Homme* (Collection «Droit et Justice» n° 63). Bruxelles: Bruylant - Nemesis, p.11.

18 ECHR, *Niemietz v. Germany*, judgement of 16 December 1992, §29.

19 ECHR, *Pretty v. United Kingdom*, judgement of 29 April 2002, § 61.

20 Council of Europe, Committee of Ministers. *Resolution 74(29) of 30 September 1974 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*. Retrieved

108»)[21] is the first notable text, as it lays out all the basic principles applicable in this area. These principles would later resurface in *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (hereinafter «Directive 95/46/EC»). This text was transposed to all European Union Member States, ensuring a high standard of protection.

The appearance of the Internet and the mass processing of personal data that we see today confirm the need for a specific body of rules enabling individuals to control personal data which is held by companies and public authorities. The European Court of Human Rights itself considers that Article 8 ECHR applies to the processing of personal data[22].

2.3. Reconciling the irreconcilable?

Freedom of expression and privacy are generally presented as only conflicting rights. This is surely the case in most disputes over media and press law, where the appellants invoke image rights, complain of the infringement of their honour, or claim to be the victims of defamatory statements. According to a group of experts for the Council of Europe over data protection, *«the potential for conflict is rendered more acute with the increasing recourse to automation by the various organs of the media».* [23]

The conflicting aspect of this relationship is highly evident if we put the freedom of the individual to express an opinion on one side, and the right to intimacy on the other. However, the nature of the relationship is much less clearly identified if we include the right to receive information and the right to (informational) self-determination. As already seen by the members of the *Article 29 Data Protection Working Party* in 1997, these «*two fundamental rights must not be seen as inherently conflicting. In the absence of adequate safeguards for privacy individuals may be reluctant to freely express their ideas. Similarly identification and profiling of readers and users of information services is likely to reduce the willingness of individuals to receive and impart information»*[24].

---

from https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2.

21 Convention n° 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

22 ECHR, *Rotaru v. Romania,* judgement of 4 May 2000, §43.

23 Council of Europe (1990). *Data Protection and Media, Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ).* Retrieved from: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Media_1990.pdf.

24 Article 29 Working Party 1/97 of 25 February 1997. Data protection and the media. Retrieved from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp1_en.pdf.

All of these fundamental rights form part of a single train of logic which aims to enable individuals to be free, to build their own identity and at the same time interact freely with other people in society. All things considered, the social and individual dimensions of these freedoms seem to be intertwined.

Studying the link between identity and privacy, A. Roosendaal[25] writes: *«Making choices and defining wishes and desires is closely related to identity. Identity is who you are as an individual and how you want to be seen by others, so it has an internal and an external element. The internal element can be described as how human beings acquire a sense of self[26]. The external element relates to social interaction with others».* These two elements appear to correspond to the two parts of privacy we looked at above: the internal element coincides with the right to intimacy; and the external element, with the right to self-determination.

The aim of the concept of right to self-determination is to provide a response to the following issue: ICT has improved our ability to process data which may relate to identified or identifiable people. This greater control over information considerably increases the powers of control held by public authorities and private entities over the people whose data they are processing. This development brings with it a risk of subservience of individuals to omniscient –and therefore all-powerful– authorities and companies. It has also awakened fears that these individuals may be subject to decisions taken against them based on entirely automated processing. In such a situation, the right to self-determination regarding information enables individuals to maintain control over their data and therefore over their individual destiny, while upholding a relationship with companies, the public authorities and other citizens.

Let us now return to freedom of expression. Case law from the European Court of Human Rights has precisely defined the role of this right in terms of both the personal development of individuals and in the community at large. The participation of citizens in public affairs –which translates as their ability to form an opinion, criticise the powers-that-be and to enter into debate– presuppose access to information. The Court regularly reaffirms that *«freedom of expression is one of the basic conditions for the progress of democratic societies and for the development of each individual»[27].* It continues to insist on the importance of this freedom in terms of the press: *«Freedom of the press affords the public one of the best means of discovering and forming an opinion of the ideas and attitudes*

25 Roosendaal, A. (2012). We Are All Connected to Facebook…by Facebook! In Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y. (ed.), *European Data Protection: In Good Health?* Dordrecht, Heidelberg, London, New-York: Springer, p.11.

26 Hekman, S. J. (2004). *Private selves, public identities: Reconsidering identity politics.* University Park: The Pennsylvania State Univ. Press, p22.

27 ECHR, *Handyside v. the United Kingdom*, Judgement of 7 December 1976, § 49.

of their political leaders. In particular, it gives politicians the opportunity to reflect and comment on the preoccupations of public opinion; it thus enables everyone to participate in the free political debate which is at the very core of the concept of a democratic society»[28].

In the age of the Internet and of Big Data, it is interesting to note that freedom of expression and privacy have an impact on the quantity and on the nature of information circulating in society. The issue is indeed specifically how to manage what has become a limitless amount of information.

Some may say *«too much information kills information»*[29]. This statement posits that there is a threshold, beyond which the amount of data is so large that it is no longer possible to process it and produce news articles and information of quality. Beyond this threshold, the objectives of quantity and quality would separate. With this in mind, the Internet and new technology may be a source of hardship...

In this study, we attempt to put some distance from these pessimistic ideas. Access to a growing source of information is incredible good fortune. It helps to free us as individuals and assists with democratic development, under two conditions. The first is that new technology must work for Man and not be used as a tool for enslavement. New technologies have to provide us with tools enabling us to cope with this flood of information. Partially, we already have this. Think of search engines, for example. The second is to consider that this growth in the amount of information available must bring with it an increase in work, which consists of checking that the processed information is true and reliable, and also of putting this information into context. This is precisely the job of journalists. Privacy and data protection rules can enable the fulfilment of these two conditions.

3. CAN DEMOCRACY SURVIVE WITHOUT JOURNALISM? CAN A ROBOT REPLACE A JOURNALIST?

The access to reliable and accurate news is a prerequisite to the empowerment of individuals and for citizen participation in public affairs. This is why journalism plays a central role in a democracy. Independence[30], the search for truth and the verification of sources lie at the base of this profession and guarantee access to reliable information.

---

28 ECHR, *Lingens v. Austria*, Judgement of 8 July 1986, Series A no. 103, p. 26, §42.

29 This fairly well known expression is attributed to a French politician Mamère, N. (1988) *La Dictature de l'audimat*. Paris: La découverte.

30 Independence is not a synonym for neutrality. See Kovach, B. and Rosenstiel, T. (2001). *The Elements of Journalism: What Newspeople Should Know and the Public Should Expect*. New-York: Three Rivers Press (experts on http://www.nieman.harvard.edu/reports/article/102544/Journalists-Must-Maintain-an-Independence-From-Those-They-Cover.aspx).

The Internet has revolutionized the manner in which information is produced and processed. A first factor of change concerns the relationship between the public and journalists. With traditional mass media, the information receiver played a more passive role in the communication process. On today's Internet, the information receiver acts properly as an information provider. Blogs, social media and chats have emerged as dynamic tools to publish fresh contents and to express comments about a variety of topics and events. Cyberspace more widely reflects the large spectrum of opinions and views that characterize our society.

However, this very proximity of journalists with the public may undermine the principle of independence. It entails the risk of seeing journalists adapt their positions to what their readers think, or with the dominating perceptions and norms of society. This lack of distance may in turn entail greater conformism.

With the Internet, the daily newspaper is replaced by continually renewed information, available around the clock. A first glance might lead one to think this information flow contributes to the production of a varied range of opinions and contents. Unfortunately, such is not the case. For many journalists, this rhythm is a source of pressure that results in a race to produce contents, sacrificing the time dedicated to on-site research, to background work, and to reflection. Many specialists have noted a trend on the web towards the homogenization of contents and stressed the dangers of churnalism, a practice which consists on producing articles on the basis of previously available content without any information check and without the least critical look[31].

Speed and interactivity are inherent characteristics of the Internet. Considerable progress can be made for democracy with this powerful tool. However, it all depends on how it is used. Now, automatic content production is a response to a demand by companies, including press publishers, who must labour with ever-increasing speed to create contents that will bring traffic to their website. The generation of advertising income depends on the audience reached. However, website traffic depends largely on search engines such as Google, which select pages on the basis of keywords corresponding to web users' searches.

From the rise of internet, we assist to the decline of this traditional medium, of the paper press. This downward trend has been amplified with the economic crisis[32]. The newspaper industry has to face an increased competition, a drop in advertising revenues and a decrease of the readership[33].

31 Katrandjian, O. (2012). *Churnalism and Its Discontents*. Retrieved February, 11th, 2013 from http://www.policymic.com/articles/1400/churnalism-and-its-discontents.

32 See OECD (2010), *op. cit.,* p. 3.

33 OECD (2010), *op. cit.,* pp. 17, 36, 60.

Narrative Science's project flourishes in this context characterized by cuts in editorial resources and budgets for investigation journalism, overworked journalists, understaffed newsrooms and closure of newspapers[34]. A client of Narrative Science, declared that he was *«impressed by the cost»* and explained that he pays *«less than $10 for each article of about 500 words –and the price will very likely decline over time»*[35]. Kris Hammond, a cofounder of Narrative Science, predict that *«in five years, a computer program will win a Pulitzer Prize».* [36] He estimates that 90 percent of news would be written by computers in 15 years[37].

Nevertheless, the contents generated by a platform like Quill cannot be classified as journalistic for a number of reasons. Getting rid of the journalist in the process of content creation leads to the loss of all editorial autonomy whose purpose it is to shield the decision-making process from economic pressures when it comes to which topics are to be covered, and how they are to be treated. The result is the risk that a goodly number of news themes that are of no interest to the masses yet are significant in terms of democracy might no longer be covered. The journalist's role as the watchdog of democracy seems to be in jeopardy.

A robot –however efficient it might be– does not allow sources to be verified, nor does it deal with information with a critical eye and with the required remoteness. Indeed, the journalist's task is not limited to gathering, connecting and correlating data. One might be lead to believe that the intervention of a machine would allow the transmission of information which would be neutral, perfectly objective, and would no longer depend on the subjective interpretations and impressions of those who produce it. But that would lose sight of the fact that machines process information according to parameters and algorithms previously defined by their creators. Furthermore, one may seriously question whether there is not in fact a risk of arbitrariness that ensues from the analysis of a variable and changing reality through a predetermined interpretation chart and predefined criteria.

Furthermore, whereas journalists draw most of their information from the real world, a Quill-like robot is fed solely with data drawn from the Internet, *i.e.* mostly user-produced contents found in social networks, in the chat rooms and forums of newspaper

34 OECD (2010), *op. cit.,* pp. 10, 18, 120.

35 Lohr, S. (2011). In Case You Wondered, a Real Human Wrote This Column. *New York Times* (September 10). Retrieved February, 11th, 2013 from http://www.nytimes.com/2011/09/11/business/computer-generated-articles-are-gaining-traction.html?_r=0&pagewanted=print.

36 *Ibid.*

37 Levy, S. (2012). Can an Algorithm Write a Better News Story Than a Human Reporter? *Wired* (April 4). Retrieved February, 11th, 2013 from http://www.wired.com/gadgetlab/2012/04/can-an-algorithm-write-a-better-news-story-than-a-human-reporter.

sites. But most of the information found through these means represent the expression of comments, impressions, feelings on sundry topics. This therefore leads to a paradox: the use of a machine will not result in greater rationality; on the contrary, it will increase the tendency towards infotainment throughout an Internet which already devotes considerable space to comments and the expression of personal impressions and feelings.

The production of contents from previously published data presents a danger E. Morozov described very well: «*some people might get stuck in a vicious news circle, consuming nothing but information junk food and having little clue that there is a different, more intelligent world out there*».[38]

There are those who predict that the Internet will lead to the disappearance of traditional journalism in favour of citizen journalism. On the contrary, the Internet has made the role of journalism a crucial one.

«*The main belief is that better technology equals better communication, and that's not true*»[39], explains D. Wolton who underlines the need to take into account the human dimension of communication[40]. He said that «*the problem is not to send information quickly but to have common understanding. The challenge of democracy is to help people live together in peace, and communication isn't always successful…If you put 500,000 computers between Israël and Palestine, you won't get peace*».

4. DATA PROTECTION RULES TO JOURNALISM'S RESCUE

The protection of quality journalism, and more particularly journalists' right to freedom of speech, citizens' right to receive quality information, and the right to privacy of readers and users of social networks requires that a distinction be made between three types of activities: 1. journalism; 2. the study for statistical purposes of data drawn from net user-produced contents; 3. the production of personalized contents according to profiles assigned to readers.

For each of these activities, specific data processing (mostly of personal data) is performed in the context of distinct purposes. Undoubtedly, the purpose principle constitutes one of the most crucial data protection mechanisms. Directive 95/46/EC puts it as follows: «*personal data must be collected for specified, explicit and legitimate purposes*»[41]. The corollary to this provision is that personal data cannot be processed later on a man-

38 Morozov, E. (2012), *op. cit., supra.*

39 Public lecture of D. Wolton in the Alliance française du Macao, 28th September 2010. Retrieved from http://www.alliancefrancaise.org.mo/spip.php?article222&lang=en.

40 See Wolton, D. (2009). *Informer n'est pas communiquer*. Paris: CNRS éditions.

41 Article 6, 1°, b).

ner which is incompatible with the purpose for which they were collected. The purpose principle permits us to define –and thereby delimit– the power of the person responsible for the processing: the various operations performed on the data must fit within the framework of the purposes defined.

In the following points, we will focus on defining these purposes, identifying the impact their pursuit entails on fundamental rights, and understanding how data protection rules may be applied to each one of them.

Let us remember that, for the most part, the obligations that ensue from Directive 95/46/EC fall on the controller, *i.e.* on «*the natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data*»[42]. Journalists and press publishers must be deemed jointly controller for the processing performed for journalistic purposes. Generally, press publishers will be held controller for the processing corresponding to the purposes mentioned in the points 2 and 3.

Note that the purpose principle and the notion of controller are to be found in Convention n° 108. [43]

4.1. Journalistic purposes

Both Convention n° 108 and Directive 95/46/EC contain a provision that manage the conflicts which might arise between the data protection rules they contain and freedom of speech.

Under article 9, 2° of Convention n° 108, «*derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of (…) b. protecting (…) the rights and freedoms of others*». As part of the current modernization of the Convention, the Convention's Consultative Committee recommends adding, at the end of the previous text, *«notably freedom of expression»*.[44]

Article 9 of Directive 95/46/EC states that: «*Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression*». Recital 17 of the Directive permits a better interpretation of this provision by specifying that: «*the processing of personal data for purposes of*

42 Article 2, d).

43 Articles 2, d) and 5, b).

44 Modernisation proposals adopted by the 29th Plenary meeting, 27-30 November 2012 (T-PD(2012)4Rev3). Retrieved February, 4th, 2013 from http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp.

journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 ECHR».

On 25 January 2012, the European Commission established rule proposal 2012/11[45], the purpose of which is to reform Directive 95/46/EC. This text, currently under discussion in the European Parliament, contains an article 80 which repeats the statement of the aforementioned article 9.

The aforementioned provisions of the Directive and Convention n° 108 both permit a near-complete derogation of data protection rules. When freedom of speech and data protection clash, the interests at stake must be weighed and a balance found on the basis of the proportionality criterion.[46]

Both texts do differ in scope, however. Article 9 of Convention n° 108 addresses, in general terms, all situations where freedom of speech and data protection clash. The text of the Directive, however, concerns *«journalistic purposes or the purpose of artistic or literary expression»*. The use of the term *«solely»* demonstrates the restricted nature of this exceptional regime.[47] Therefore, all the data processing the purpose of which might jeopardize freedom of speech is not necessary covered by the hypothesis of article 9 of the Directive. Nevertheless, even where the data processing is not protected by the regime of this provision, specific derogations to the Directive's obligations may be allowed if they are necessary to reconcile the opposing fundamental rights.

Whether on the basis of the text of the Directive or of that of Convention n° 108, it is accepted that data processing for journalistic purposes (editorial including electronic publishing) almost requires a derogation to nearly all applicable rules concerning data protection. The journalist's task would become difficult –if not impossible– to perform if the consent of individuals whose data was being processed had to be obtained every time, or if information, especially regarding processing purposes, had to be provided to them.

In order to differentiate which types of data processing do qualify under the Directive's derogation system from those which do not, we should define what must be understood by *«journalistic purposes»*.

---

45 Proposal for a regulation 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). Retrieved February, 1st, 2012 from http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

46 See ECJ, Case C-101/01, *Bodil Lindqvist*, judgment of 6 November 2003 (All the case law is available at the Court website, at http://curia.europa.eu).

47 Article 29 Working Party 1/97, *op. cit.,* p. 8.

The Court of Justice of the European Union (hereinafter «ECJ») has considered this concept in a judgment dated 16 December 2008. It decided that activities «*relating to data from documents which are in the public domain under national legislation, may be classified as 'journalistic activities' if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit-making purposes*»[48]. It determined that any activity had to be considered as a journalistic one, if it was one *«in which data relating to the earned and unearned income and assets of natural persons are: collected from documents in the public domain held by the tax authorities and processed for publication; published alphabetically in printed form by income bracket and municipality in the form of comprehensive lists; transferred onward on CD-ROM to be used for commercial purposes; and processed for the purposes of a text-messaging service whereby mobile telephone users can, by sending a text message containing details of an individual's name and municipality of residence to a given number, receive in reply information concerning the earned and unearned income and assets of that person»*[49].

This decision warrants a number of criticisms. The interpretation given by the ECJ to journalistic activities far exceeds the manner in which they are usually understood. The ECJ even includes in this notion those activities which are intended solely to market the data, without any journalistic treatment of the information. Such activities often include significant risks of invasion of privacy and are unrelated to the mission conferred unto journalism in a democracy. While the practice of journalism may also include the search for financial returns, the danger lies in confusing data processing for journalistic purposes with data processing for marketing purposes. And that is all the more worrisome now that, with the Internet, the lines between marketing and journalistic contents tend to get blurred, *«causing problems for people in search of objective information»*. [50]

It is essential to incorporate into the notion of journalistic purposes the ethical norms and the values that are the foundation of journalism. Working Party experts were already moving in this direction in a recommendation adopted in 1997. Furthermore, the role of the media in a democratic society «*to impart information and ideas on all matters of public interest*» –as stressed in the jurisprudence of the European Court of Human Rights[51]– should be taken into consideration. Advocate General Kokott had adopted this position in her opinion in the aforementioned case. However, the ECJ did not agree.

48 ECJ (Grand Chamber), *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia*, judgment of 16 December 2008.

49 *Ibid.,* §34.

50 Custom Content Blog (2012). *Is Content Marketing Invading Traditional Journalism's Turf?* Retrieved January, 29th, 2013 from http://blog.customcontentcouncil.com/?p=1898.

51 ECHR, *Lingens v. Austria*, *op. cit.*, § 44.

Therefore, I propose journalistic purposes be defined as: the production of information on topics of general interest, in accordance with ethical and professional obligations that are the foundation of journalism, to wit independence, the verification of sources and the search for truth.

The distribution of information without any commentary falls within the scope of this purpose, whether in publishing a photograph or simply reproducing a document, figures or a set of raw data. Indeed, the distribution of such information presupposes a decision on the part of the journalist and efforts to contextualize the information: he will have come to the conclusion that this information was relevant as part of a debate on a topic of general interest. Let us consider, for example, the publication of a photograph. Its very contents may bring to the public's attention facts of great importance. Yet no journalist who exercises his profession correctly would publish it without first verifying its authenticity, duly stepping back and expressing, if necessary, reservations.

Furthermore, the reuse of personal data previously made available to the public comes under journalistic purposes so long as the aforementioned ethical rules have been respected, which requires the intervention of a flesh-and-blood journalist. The same applies to data obtained from social networks or those published over the Internet. *A contrario*, merely providing personal data out of context, or subject to criteria or purposes which are left entirely to the recipient of the information, does not come under this hypothesis. Thus, the fact of granting access to the fiscal data of various people to users who may consult them out of idle curiosity does not fall within the scope of journalistic activities. Which is not to say that a person's fiscal data cannot be published by the press in certain cases. An excellent illustration of this is the *Fressoz and Roire c. France* case. In that instance, «*the article was published during an industrial dispute at one of the major French car manufacturers. The workers were seeking a pay rise which the management were refusing. The article showed that the company chairman had received large pay increases during the period under consideration while at the same time opposing his employees' claims for a rise*»[52].

4.2. Identification of the purposes of data processing performed as part of automated «journalism»

The automatic production of contents through the reuse of data drawn from contents uploaded by Internet users has serious consequences regarding fundamental rights. As previously demonstrated, the right of citizens to receive quality information is seriously jeopardized. The same applies to the right to privacy and data protection of users of social networks, chat rooms and forums. Data published on line by a user, to which

52 ECHR, *Fressoz and Roire c. France*, judgement 21 January 1999, §50.

must be added the data resulting from interactions with other people, reveal many personality aspects, ranging from political opinions to consumption habits, and including health, philosophical convictions, sexual life, profession…. Such information allows the creation of highly detailed profiles of individuals.

Here, rules applicable to data protection must be applied fully, as this does not remotely enter into our previous definition of journalistic purposes. Concretely, users of social networks, chat rooms and forums communicated their data to express an opinion, contact other users, and share experiences and contents with them. The robot journalist reuses the data for a purpose which may be defined as follows: to perform statistical studies and research on opinion trends on the web and in social networks. The published results are no longer personal data, but general data that provide a global overview.

The robot's processing is incompatible with the purpose of the initial collection. Therefore, reuse of the data implies in this case the birth of a new process, one which must meet all the requirements of Directive 95/46/EC. It bears noting that the Directive allows Member States to provide for a favourable regime where the data are reused for historical, statistical or scientific purposes, so long as appropriate safeguards are included. In most Member States, these guarantees include the anonymization of the data. This statistical-research purpose, as we have defined it, excludes any profiling of individuals and any marketing purpose. Traffic data may be processed in this case, only if the sole objective is to understand the audience in a global manner. Under no circumstance may such a process exercise any influence over the contents of the articles made available to readers. That would then constitute a marketing purpose.

Statistical purposes must be carefully distinguished from profiling ones. «*Statistics aim at analysing mass phenomena. Statistics allow (…) the drawing of a general affirmation from a series of systematic individual observations (…) In this way, although statistics are based on individual observations, their objective is not to acquire knowledge of the individuals as such (…) Statistical activities (…) are not directed at taking decisions or individual measures, but rather (…) collective judgments or decisions*»[53].

Directive 95/46/EC calls for other safeguards, some of which are: the protection of people requires compliance with article 6, 1°, (e), which stipulates that the data must be «*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed*». Readership studies that are conducted do not require the use of data which permits those involved to be identified. Such data should therefore always be anonym-

53 Council of Europe (1997). *Explanatory Memorandum of Recommendation No.R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes*. Retrieved from http://www.coe.int/t/dghl/standardsetting/dataprotection/EM/EM_R(97)18_EN.pdf.

ized, keeping in mind the fact that the simple interconnection of data may easily allow the identification of the individuals concerned. This is especially so given the quantity and nature of the data collected.

The processing of sensitive data, such as medical data or data revealing ethnic origin, political opinions, philosophical beliefs, requires obtaining the prior consent of those persons involved. They must be provided with complete information on the intended purposes, the identity of whoever will receive the data. The persons involved must also be able to exercise effectively their rights, including those to access and correction.

It bears noting that publication of the result of the research is protected by freedom of speech.

4.3. From targeted advertisement to customized «journalistic» contents

«Imagine creating multiple versions of the same story, with each story's content customized for different audiences and tailored to fit a particular voice, style and tone.» [54] This is what we could read until very recently on Narrative Science's website in a section regarding the services Quill could provide in the field of *«Publishing and Media».*

Data processing as it is viewed here is not intended to consider the contents of blogs and social networks as a source of information that allows us to gain better knowledge of the world that surrounds us and the debates on ideas that are going on in our societies. The intent here is purely a commercial one. Data on newspaper readers are analyzed to produce non-objective but personalized information. Topics of general interest are treated in a non-journalistic manner.

This type of approach is not specific to the Narrative Science project. A. Altert warns us, in an article published in the Wall Street Journal, that «*your E-book is reading you*»[55]. *«The major new players in e-book publishing - Amazon, Apple and Google - can easily track how far readers are getting in books, how long they spend reading them and which search terms they use to find books. Book apps for tablets like the iPad, Kindle Fire and Nook record how many times readers open the app and how much time they spend reading. Retailers and some publishers are beginning to sift through the data, gaining unprecedented insight into how people engage with books*».

This type of treatment constitutes a serious attack on the right to receive objective information, as well as on the right to privacy of the readers and Internet users. Let us apply the provisions of Directive 95/46/EC. First of all, the consent of those people

54 Retrieved January, 29th, 2013 from http://www.narrativescience.com/services.

55 Alter, A. (2012). Your E-Book Is Reading You. *Wall Street Journal* (July 19). Retrieved January, 29th, 2013 from http://online.wsj.com/article/SB10001424052702304870304577490950051438304.html.

involved should always be obtained prior to this type of processing. As the purpose is a marketing one, those involved have the right to oppose, without cost, such a process. Furthermore, the processing of sensitive data should be forbidden even should the consent of those persons involved be obtained. The processing of such data is disproportionate in the context of marketing purposes, which constitutes a violation of Article 6, c) of Directive 95/46/EC, according to which the processed data must be «*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*».

5. CONCLUSION

The context applicable to data protection is currently being reviewed both by the Council of Europe and the European Union. This therefore provides an opportunity to add to the current text of Directive 95/46/EC a more general provision, such as Article 9 of Convention n° 108, to the derogation applicable to «*journalistic purposes or the purpose of artistic or literary expression*». This also would be the right time to insert in Convention n° 108 a derogation which would be applicable specifically to these purposes, such as the one mentioned in the Directive. The purpose of journalism should clearly be defined in each of these instruments. Moreover, the exact object of the derogations allowed in this matter should be clearly specified. The same needs be done as regards artistic and literary expression. Generally speaking, the derogations applicable to all of these activities should be allowed only if the data processing is performed by human beings, not solely by machines.

BIBLIOGRAPHY

Albert, P. (1970). *Histoire de la presse* (Collection «Que sais-je ?» n° 414). Paris: Presses Universitaires de France, pp. 34-35

Alter, A. (2012). Your E-Book Is Reading You, *Wall Street Journal* (July 19). Retrieved January, 29th, 2013 from http://online.wsj.com/article/SB10001424052702304870304577490950051438304.html

Bell, E. (2012). The robot journalist: an apocalypse for the news industry? *The Guardian* (May 13). Retrieved January, 29th, 2013 from http://www.guardian.co.uk/media/2012/may/13/robot-journalist-apocalypse-news-industry/print

Constant, B. (1819). *De la liberté des anciens comparée à celle des Modernes, lecture to the Athénée Royal of Paris in 1819* (Paris: Mille et une nuits – 2010)

Council of Europe, Committee of Ministers. *Resolution 74(29) of 30 September 1974 on the protection of the privacy of individuals vis-à-vis electronic data*

banks in the public sector. Retrieved from https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=590512&SecMode=1&DocId=649498&Usage=2

Council of Europe (1990). *Data Protection and Media, Study prepared by the Committee of experts on data protection (CJ-PD) under the authority of the European Committee on Legal Co-operation (CDCJ).* Retrieved from: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Media_1990.pdf

Council of Europe, ECHR, Research Division (2011). *Internet: Case-law of the European Court of Human Rights*, 2011. Retrieved February, 5th, 2012 from http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_EN.pdf

Custom Content Blog (2012). *Is Content Marketing Invading Traditional Journalism's Turf?* Retrieved January, 29th , 2013 from http://blog.customcontentcouncil.com/?p=1898

Hammond, K. (2012) *Just to Clarify - Generating stories from social media: Getting to the meat of the tweets*. Retrieved January, 28th, 2013 from http://khammond.blogspot.be/2012/02/generating-stories-from-social-media.html

Hekman, S. J. (2004). *Private selves, public identities: Reconsidering identity politics.* University Park: The Pennsylvania State Univ. Press, p.22

Katrandjian, O. (2012). *Churnalism and Its Discontents*. Retrieved February, 11th, 2013 from http://www.policymic.com/articles/1400/churnalism-and-its-discontents

Kovach, B. & Rosenstiel, T.(2001). *The Elements of Journalism: What Newspeople Should Know and the Public Should Expect*. New-York: Three Rivers Press

Levy, S. (2012). Can an Algorithm Write a Better News Story Than a Human Reporter? *Wired*, (April 4). Retrieved February, 11th, 2013 from http://www.wired.com/gadgetlab/2012/04/can-an-algorithm-write-a-better-news-story-than-a-human-reporter

Lohr, S. (2011). In Case You Wondered, a Real Human Wrote This Column. *New York Times* (September 10). Retrieved February, 11th, 2013 from http://www.nytimes.com/2011/09/11/business/computer-generated-articles-are-gaining-traction.html?_r=0&pagewanted=print

Morozov, E. (2012). A robot Stole My Pulitzer! How automated journalism and loss of reading privacy hurt civil discourse. *Slate Magazine* (March 19). Retrieved February, 11th, 2013 from http://www.slate.com/Articles/technology/future_tense/2012/03/narrat...ists_customized_news_and_the_danger_to_civil_discourse_.single.html

Neuner, C. (1866). *Wesen und Arten der Privatrechtsverhältnisse*. Kiel, Schwers'sche Buchhandlung, p.16

OECD (2010). *News in the Internet Age: New Trends in News Publishing*. Paris: OECD Publishing

Rigaux, F. (2004), Protection de la vie privée. In *Répertoire pratique de droit belge* (Tome IX complément). Bruxelles: Bruylant, p.825

Roosendaal, A. (2012). We Are All Connected to Facebook…by Facebook! In Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y. (ed.), *European Data Protection: In Good Health?* Dordrecht, Heidelberg, London, New-York: Springer, p.11

Sudre, F. (2005). La construction par le juge européen du droit au respect de la vie privée (Rapport introductif). In Sudre, F. (dir.) *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'Homme* (Collection «Droit et Justice» n°63). Bruxelles : Bruylant - Nemesis, p.11

Templon, J. (2012). *Quill Analyzes Presidential Campaign Funding*. Retrieved January, 29th, 2013 from http://www.narrativescience.com/blog/quill-analyzes-presidential-campaign-funding

Warren, S.D., Brandeis, L.D. (1890). The Right to Privacy. *Harvard Law Review*, pp. 193-220

Wolton, D. (2009). *Informer n'est pas communiquer*. Paris: CNRS éditions

12

E-HEALTH IN THE AGE OF BIG DATA: THE EU PROPOSED REGULATION ON HEALTH DATA PROTECTION

Panagiotis Kitsos, LLM, PhD
ITLaw Team, Dept. of Applied Informatics
University of Macedonia, Researcher

Aikaterini Yannoukakou, Librarian MSc
ITLaw Team, Dept. of Applied Informatics
University of Macedonia, PhD candidate

ABSTRACT: The amount of medical data is growing rapidly in the current technological and social environment. Big data analytics are being developed to assist health service providers, doctors and researchers to accelerate scientific discovery, enable personalized medicine and improve the quality of health care. It is being underpinned that in order to achieve these objectives an open data strategy should be followed by public authorities allowing third parties to access medical data.

This process though raises severe concerns over privacy issues relating to the use of medical information by both private and public entities. Against this complex network of technology threats, European citizens are currently protected by a rather outdated regulatory framework, namely the Directive 95/46/EC, which however is under revision and hopefully is about to be replaced by a new, updated and more comprehensive Regulation.

This paper conglomerates the presentation of research on privacy problems arising from the emergence of big data sets in medical sector by attempting to re-address the privacy problems in the environment of big data and open data policies in health sector and tries to examine to what extent the proposed data protection regulation can address these issues so as to create a modern and updated legal framework by introducing new rules that will provide greater legal certainty, enhance citizens' trust in the use of their medical data, and ultimately achieve the goal of delivering efficient health services.

KEYWORDS: e-health, big data, open data, General Data Protection Regulation.

1. INTRODUCTION

During the decades of the 1950s and 1960s governments embraced the new emerging computer technologies, which primarily integrated data processing into management systems enabling their fast interlinking and processing to respond to the continuously increased demands of modern States. Accordingly, in the 1980s the rise of network technology made it possible for computers to be linked together, and further the emergence of telecommunication networks and, especially Internet, provided with the opportunity to establish of digital networks with immense capacities for accessing, processing and sharing large amount of data held by government, hospital, university

and/or private entities. By the end of 1990s all the «e-terms» were broadly introduced –e-government, e-crime, e-learning, e-justice, e-health– and have now dominated the policy orientation of governments and public administrations worldwide trying to exploit the advances of the Information and Communication Technologies (ICTs) to increase information access and availability as well as transparency and the accountability of the public sector.

Within this scope e-health:

> is the use of ICTs in health products, services and processes combined with organisational change in healthcare systems and new skills, in order to improve health of citizens, efficiency and productivity in healthcare delivery, and the economic and social value of health. E-health covers the interaction between patients and health-service providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and/or health professionals. (European Commission, 2012a, p. 3).

Thus, the amount of medical data is growing rapidly in the current technological and social environment. Moreover, the current formated informational environment consisting of the use and usage of big data and open data policies can be proven extremely expedient when it comes to assisting health service providers, doctors and researchers to accelerate scientific discovery, enable personalized medicine and improve the quality of healthcare. However, a number of privacy and data protection issues such as the prevention of unauthorized disclosure to all health related information, the anonymisation, re-identification and de-identification procedures, the reinforcement of consent, the right of the citizen to erase personal data must be considered beforehand when designing e-health policies so as to provide Europeans with a better quality of life through better designed healthcare systems.

The main objective of the paper is to examine the current technological environment of e-health in the era of big and open data as well as whether and under which circumstances the implementation and blanket introduction of such techniques should be considered and adopted giving emphasis on privacy and data protection. Further, we intend to demonstrate the legislative framework on e-health as formulated within European Union (EU) the e-Health Action Plan 2012-2020 and primarily the General Data Protection Regulation, and how is being related to the deployment of e-health initiatives.

Our starting point is the review of the several European initiatives on e-health in order to evidence the importance that EU has assigned to the development of electronic healthcare systems, whereas further we examine the core essence of what big data and open data are and how they apply and beseem within the e-health spectrum. Finally, we review how the Proposed Regulation can accommodate both the development and wide implementation of e-health systems and the protection of the data subjects –the patients in this case– from unlawful and illegal processing of their health data at the same time.

2. E-HEALTH

The automation of procedures in the e-health sector has been among the priorities of governments worldwide during the last decade –being one of the pillars of the e-government vision– considering that the introduction of ICTs to the healthcare systems can revolutionize the way medicine is being applied bearing benefits for all stakeholders –patients, health physicians and the State itself. Healthcare systems are part of a wider network of social and welfare services (Callens, 2010), which were among the first to benefit from the introduction of computers and networking long before from the advent of e-government. One of the most successful examples is the program «Families First» implemented in Camden, New Jersey in February 1994 with the distribution of cash and food stamps in the format of ATM cards which were charged as appropriate via an electronic system (Milward & Snyder, 1996, p. 267).

Since then the generalized implementation of electronic services to the health sector has become an undeniable realization shaping the scenery of e-health. As e-health is defined:

> the application of ICTs across the whole range of functions that affect the healthcare sector consisting of four interrelated categories of applications a) clinical information systems, b) telemedicine and home care, namely personalized health systems and services for remote patient monitoring, c) integrated regional/national health information networks (i.e. e-prescription), and d) secondary usage of non-clinical systems (i.e. specialized systems for researchers or support systems such as billing systems). (Callens, 2010, p. 561).

EU realizing the immense inherent power and the great impact that e-health applications would have in a pan-European level hastened into adopting a statutory framework early including provisions for promoting the implementation of e-health services. More specifically, eEurope 2002 Action Plan provided for Health Online «to develop an infrastructure of user-friendly, validated and interoperable systems for health education, disease prevention and medical care» (2000, p. 23).

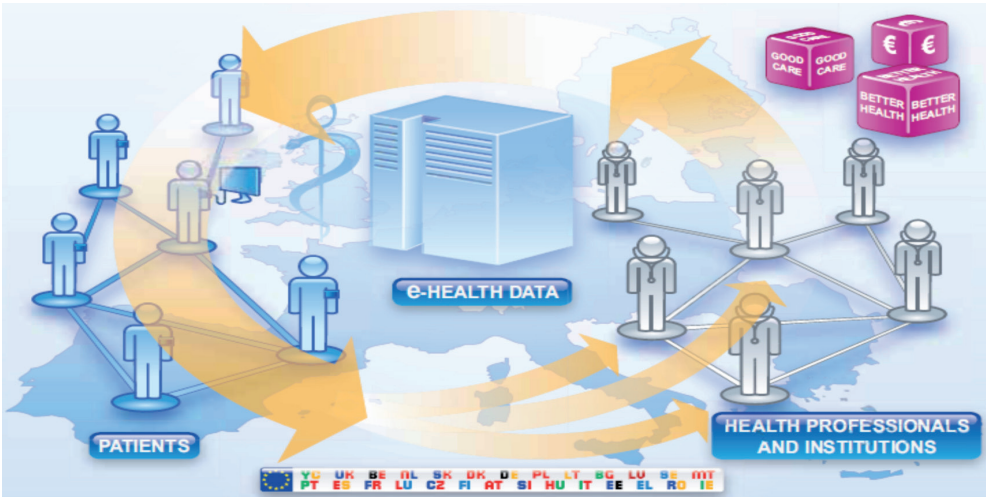
The term «e-health» is officially used in the eEurope 2005 Action Plan (2002) as a means:

> to reduce administrative costs, to deliver health care services at a distance, to avoid unnecessary duplicate examinations via three (3) proposed actions a) electronic health cards, b) health information networks with broadband connectivity, and c) online health services (e.g. information on healthy living and illness prevention, electronic health records, tele-consultation, e-reimbursement). (p. 13).

Alongside, the i2010 Communication promotes the introduction of ICTs to public sector, including healthcare, aiming for better, more accessible and more cost effective

public services by employing technologies for wellbeing, independent living and health (European Commission, 2005, p. 10-11). Finally, Point 2.7.2 of Digital Agenda for Europe[1] states that the deployment of e-health technologies are a key action in improving the quality of care, reducing medical costs and fostering independent living, including in remote places. In parallel, the eHealth Task Force has issued the report «Redesigning health in Europe for 2020» which designates five (5) levels of change for a shift towards an integrated e-health environment for the 21st century:

1. **My data, my decisions**, designating individuals as owners and controllers of their own health data with the right to make decisions over access to the data and to be informed about how it will be used.
2. **Liberate the data**, introducing open practices to health data so as to transform the way that care is provided and generate cost savings.
3. **Connect up everything**, exploiting the personal digital life streams published by individuals to geo-tag them and use them for public health surveillance and epidemiology.
4. **Revolutionise health**, publishing the efficiency of health institutions and professionals enables the public to make informed decisions on their course of treatment.
5. **Include everyone**, employment of ICTs to reduce inequalities by designing services that promote and enhance equity.



Source: Redesigning health in Europe for 2020, eHealth Task Force Report

1 The European Commission launched in March 2010 the Europe 2020 Strategy to exit the crisis and prepare the EU economy for the challenges of the next decade. More information available at http://ec.europa.eu/europe2020/index_en.htm.

The first e-Health Action Plan, issued on April 2004, vividly delineated the framework of European policies and initiatives providing tomorrow's instrument for substantial productivity gains, restructured, citizen-centered health systems and, at the same time, respecting the diversity of Europe's multi-cultural, multi-lingual health care traditions (p. 4). The consecutive e-Health Action Plan 2012-2020 was issued in December 2012 setting out a road map to address barriers to the use of ICTs in Europe's healthcare systems by recognizing the right of individuals to have their personal health information safely stored within a healthcare system accessible online as an essential condition for success of these initiatives and focusing especially to the cross-border transmission of health data.

Especially considering the cross-border transmission of health data, EU adopted in March 2011 the Directive 2011/24/EU on the application of patients' rights in cross-border healthcare. The purpose of the Directive (Article (1)) is to

> provide rules for facilitating the access to safe and high-quality cross-border healthcare and promotes cooperation on healthcare between Member States, in full respect of national competencies in organising and delivering healthcare. (p. 53).

According to Recital (2) the legal basis is Article 114 of TFEU[2] concerning the improvement of functioning of the internal market and the free movement of goods, persons and services, whereas Recital 25 specifies that the transfer should depend on the protection of personal data as indicated to Directive 95/45/EC, and establishes the right for individuals to have access to their personal medical data containing information as diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided. Finally, Article 14 refers specifically on the provision for the establishment of a voluntary e-health network which should exploit the capabilities of European e-health systems and draw up guidelines on which data can be shared and the effective methods of use of medical information, whilst in parallel Recital 57 provides for the interoperability of e-health solutions. Unfortunately, there is no direct mentioning either to big data or to open data and the way that can be implemented within the health sector, but elements the reference to e-health solutions could be perceived as an indirect mention, and also elements from the Open Strategy for Europe can be incorporated and used in order to facilitate their use.

Still the goal to promote the use of ICTs in healthcare sector without compromising citizens' privacy might be proven a quite challenging task in the age of big data,[3] where the added value of information has led to unprecedented collection, aggregation

2 Treaty on the Functioning of the European Union (TFEU) is the Treaty which organises the functioning of European Union and determines the areas of, delimination of, and arrangements for exercising its competences. It forms the basis for the introduction of new policies and legislation in EU.

3 As the term was used by Steve Lohr.

and storage of data. In the case of health sector, where new technologies are virtually used in all levels of healthcare, the production and exploitation of health related data is becoming the main goal of private companies, marketers, research centers and government initiatives as a means to improve profit and healthcare services.

3. BIG DATA

Big data has been characterized as planet nervous system[4] (Hernadez, 2012), but basically is a buzz word affixed by software engineers, computer scientists, and social scientists describing of the revolutionary ability to detect, corral and compare data on scales few even dreamed possible even some years ago (Raash, 2012). It mainly refers to datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze (McKinsey Global Institute, 2011), or simply

> high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making. («Big Data,» n.d.).

It is estimated that approximately 2.5 quintillion bytes of data is created daily in any structured and unstructured format of text, sensor data, audio, video, click streams, log files and many more emerging from various and diverse sources such as sensors used to gather climate information, posts to social media sites, digital pictures and videos, purchase transaction records, and cell phone GPS signals (International Business Machines [IBM], n.d.).

The World Economic Forum's 2012 report states that big data can be actionable information used to identify needs, provide services, and to predict and prevent crises for the benefit of low income populations. In March 2012, the U.S government announced $200 million in research programs for big data computing (United States, 2012) and the trend for the future is that big data analytics will provide a series of tailored made information to a variety of demands. Only recently the Obama 2012 campaign used data analytics and the experimental method to creating a system that collected information from smartphones, social-media contacts overturning the dominance of TV advertising in U.S. politics and creating a national campaign run like a local ward election, where the interests of individual voters were known and addressed (Scherer, 2012).

In parallel the development of open data and their rapid adoption to public sector pose additional issues on the handling of health data, especially considering that health data fall under special category of data processing as specified to Article 8 of the Direc-

4 According to Rick Smolan, Yahoo CEO, Marissa Mayer, on a Twitter discussion, described big data as «the world is developing a nervous system.»

tive 95/46/EC. Broadly speaking open data is defined as «*data that can be freely used, reused and redistributed by anyone - subject only, at most, to the requirement to attribute and sharealike» (Open Knowledge Foundation [OKF]), or otherwise open data «can be in any content format (text, image, sound, numbers) or software and available to the public without copyright or other licensing restrictions for copying, further use and dissemination» (Tsiavos, 2011)*. Summarising this, open data refers to availability and access, reuse and redistribution, universal participation and interoperability.

Incorporating open practices into healthcare sector is a challenge mainly due to the sensitive and confidential nature of health data on one hand, and the inherent openness of procedures on the other hand. However, in order to implement an e-health environment this incorporation seems obligatory, and it is among the objectives set by the eHealth Task Force when referring to the liberation and connection of data with open practices and the eHealth Action Plan, which consistently supports and promotes the interoperability and cross-border transmission of health data.

3.1. Big data in Health Sector

Acquiring medical data is not an easy task since 80 percent of all information is unstructured, and as Cohn (2013) signifies namely it consists of «physician's notes dictated into medical records, long-winded sentences published in academic journals, and raw numbers stored online by public-health departments». So given the self-evident importance of big data in every sector, the healthcare systems worldwide are the next frontier since big data sets are considered to be the biggest potential areas of application for society is healthcare (Rooney, 2012).

Health related data, collected in versatile modes such as via mobile devices by health workers and individuals, or analysed in the form of data exhaust, can constitute a useful tool for understanding population health trends or stopping outbreaks, and further data from electronic health records can be used to create massive datasets with which treatments and outcomes can be compared in an efficient and cost effective manner (World Economic Forum [WEF], 2012, p. 2). Grant (2012) stresses that big data permits to epidemiologists to gather information on social and sexual networks to better pinpoint the spread of disease and create early warning systems. Comparative-effectiveness researchers are combing government and clinical databases for proof of the best, most cost-effective treatments for hundreds of conditions, information that could transform healthcare policy. Disease researchers having access to human genetic data and genomic databases of millions of bacteria data they can combine to study treatment outcomes.

When describing big data in the health sector, we mainly see certain healthcare data pools that function as sources of information with the scope to improving healthcare such as:

1. Drug data extracted from prescription records reveal the prescribing practices of individual doctors (Lewis, 2011),

2. Device data collected from implantable cardiac devices that record and store data onboard, while patient's wireless monitors, download the files and send them to the developer and manufacturer of the device website accessible by doctors (Dockser-Marcus & Weaver, 2012),
3. Clinical data collected from medical records and medical images assist the production of pharmaceuticals and of improvement clinical research and healthcare (Vu & Slavkovic, 2009),
4. Claims and financial data, where information is extracted on total healthcare costs as well as patient burden and insurance claims,
5. Patient behavior and sentiment data is very important for predictive analytics since it can be easily extracted from consumers/patients online behaviour, while purchasing pharmaceutical products, searching and visiting certain health related websites, posting on social media, data pulled from RFID chips embedded in drug packaging and connected by networks to computing resources (McKinsey Global Institute, 2011, p. 42). Patients can also seek for advice, learn from each other, discuss test results, and compare medications, treatments or combinations of drugs (Al-Ubaydli, 2012) via the online support networks as for example «Health Unlocked» or the «Patients Like Me».

Concluding big data harbors tremendous possibilities to healthcare and well-being providing enormous advantages to all stakeholders when properly implemented and applied on every aspect, because they present the unique opportunity of connecting people with their own data and offer them with the change to chance their life.

3.2. Open Data in the Health Sector

The problem of health related data is that it forms a kaleidoscope of imaging from X-rays, MRI's and other scanners, genetics, pathology, sensors and research data stored in a vendor specific manner so that it cannot be shared or used in a smart way such as for research or educational purposes (Wijsman, 2012).

The release of the health data in an unrestricted, free of charge, 24/7 accessible and available manner is the core of the synergy among open data practices and healthcare sector. This collaboration is made even more compulsive considering that the greatest percent of health data comes under the label of government data as for which there is a shift towards employing open practices of management. As Groen (n.d.) mentions this prospect is translated into:

> finding ways to add value and generating useful new reports of products for commercial or non commercial purposes, and improving the populations health, well-being and mortality rate in the case of health sector.

There are many initiatives worldwide supporting and promoting the synergy among open data and health data such as the World Bank Health Data, where data is collected from national health systems, disease prevention, reproductive health, nutrition and population dynamics (Groenpj, n.d.). Also, UK National Health System has developed an open policy on health data in order to reduce the expenditures on medicine and health consultations, and improving the health related services at the same time. At the same pace, the US Department of Health & Human Services has introduced the Health Data Initiative (HDI):

> aiming to help US citizens understand health and healthcare performance in their communities and to help spark and facilitate action to improve performance by the creation and use of an ever-growing array of new applications.

Analogous efforts have been tested in regional and community basis such as the Open Data Initiative taken place by the city of Almere in Netheralnds, where health providers, government and knowledge institutions and several ICTs companies collaborated to develop a vendor-neutral big data platform (Boermeester, 2012), whereas Kenya's «Open Data Portal» launched in 2011 is considered an excellent example of open data practice to be used as a guide to adopt open data in the health sector (WEF, 2012, p. 6).

Opening up health data both to the public and the private sector should not come without any obligation regarding privacy and data protection issues, and it is directly associated with the adopted legislative and policy frameworks in national, regional, local level and global as well. Therefore, the introduction and the employment must be fully planned and thoroughly examining all implicated components well beforehand. The importance of health and medical related data cannot be better overemphasized to the decision of US Supreme Court some days ago that ruled against Myriad Genetics on the patent of human genes and cleared the way for patients, physicians and scientists to benefit from the findings of medical research and the advances of medical technology (Wolf, 2013).

4. PRIVACY CONCERNS

Big data in healthcare poses a number of privacy concerns, which are raised by its inherent characteristics as a combination of powerful data mining tools. Big data is characterized by certain features that create a pervasive environment for privacy and personal data protection (Rubinstein, 2013). Firstly, the unprecedented and massive collection of data that generate more than 900 million web pages and upload more than 250 million photos every day on social networks alone. Google sites had more than 1 billion unique visitors, whilst YouTube passed 1 trillion video playbacks in 2011. Accordingly, email, instant messaging, VOIP calls, and other communications generate tens of trillions of recorded messages every year. The same goes for credit and debit

cards, checks, and other financial activities that provide a stream of billions of recorded financial transactions (Kuner, Cate, Millard, & Svantesson, 2012). Mobile phones, surveillance cameras, apps, and tweets create and share vast amounts of personal data that can be stored, shared, searched, combined, and duplicated with extraordinary speed and at very little cost creating an environment of ubiquitous data collection, where our everyday life activities result in data being captured and stored by third parties.

Secondly, «the use of high speed, high-transfer rate computers, coupled with petabytes of storage capacity, resulting in cheap and efficient data processing» (Rubinstein, 2013, p. 4) based on the emerging of cloud computing technologies and models. Thirdly, the use of new computational frameworks such as Apache Hadoop[5] facilitate the handling (storage, analysis and access) of massive amounts of structured and complex unstructured data quickly and cost effectively.

The result of these features is the ever increasing dangers for individual right to data protection and privacy. Rubinstein (2013) identifies the capability of big data analytics to re-identify data subjects the major privacy concern raised by their use. Eventhough organizations used various methods of de-identification –i.e. anonymisation, pseudonymisation, encryption, key-coding, data sharing– to distance data from real identities and allow analysis (Tene & Polonetsky, 2012a), still Ohm argues that re-identification science disrupts the privacy policy landscape by undermining the faith placed in anonymization (as cited in Tene & Polonetsky, 2012a, p. 65). Re-identification has been a controversial subject likewise encryption at the early 00s, but we still use encryption methods and secure web sites (Oram, 2012). In the context of health related information the tracking and profiling of patients' medical records is a great concern, and somewhat blurring the thin line between personal and non personal data since it will permit the linking of pieces of data to a person's real identity. Essers (2012) argues that «by querying a database often and asking it different questions it is possible to find out where someone lives, or to find the medical record of a colleague or friend», whereas:

> the entire premise of big data is that the collection of more and more terabytes of the most deeply personal, intimate information about each individual's mind and body, geolocations, exercise, eating habits, etc will be used for research or data analytics. (Roop, 2012, p. 10).

However, a breakthrough article by Daniel Barth-Jones attempts to substantiate that the risks of re-identification to privacy are being exaggerated by analysing the re-identification case of Governor William Weld's medical information, Governor of Cambridge, MA. He ultimately concludes that the re-identification of his medical data made possible due to the publicity of his hospitalisation, and not because of the re-identification methods used. He argues that:

5 For more information on Apache Hadoop see http://hadoop.apache.org.

> the logic underlying re-identification depends critically on being able to demonstrate that a person within a health data set is the only person in the larger population who has a set of combined characteristics (known as «quasi-identifiers») that could potentially re-identify them, most re-identification attempts face a strong challenge in being able to create a complete and accurate population register. (Barth-Jones, 2012).

At that extend, he recommends that policymakers should focus on establishing a safe harbour for proper de-identification methods based on a rigourous statistical analysis of re-identification risks. This approach coupled with legal limitations on re-identification could protect consumers against real privacy harms, while still allowing the free flow of data that drives research and innovation throughout the economy (Szoka, 2012).

5. SELECTED ISSUES OF GENERAL DATA PROTECTION REGULATION

Eventhough, EU recognizes the protection of personal data as a fundamental right,[6] the non uniform application of Directive 95/46/EC on data protection across the Member States causes legal uncertainty and obstacles in the flow of information in EU. For that reason European Commission introduced on January 2012 new rules in the form of Regulation, since Regulation is directly applicable to all Members States without a need for implementation by the national legislation.[7] The proposal is based on Article 16 of the Treaty on the Functioning of the European Union (TFEU), which is the new legal basis for the adoption of data protection rules introduced by the Lisbon Treaty. The provision allows the adoption of rules relating to the protection of individuals with regard to the processing of personal data by Member States when carrying out activities which fall within the scope of Union's law. It also allows the adoption of rules relating to the free movement of personal data, including personal data processed by Member States or private parties, as determined in Explanation 3.1.

Generally the Proposed Regulation aims to modernize the principles enshrined in the Directive 95/46/EC to guarantee privacy rights and to apply the principles of data protection to any information concerning an identified or identifiable person, no matter where it is sent, processed or stored. In particular the main provisions of the Proposed Regulation of particular interest to e-health initiatives are (European Commission, 2012b):

---

6 As determined to Article 8 of the Charter of Fundamental Rights and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).

7 See Article 288 of TFEU.

a. New general principles governing personal data processing as transparency principle, comprehensive responsibility and liability of the controller, and clarification of the data minimization principle;
b. The special categories of processing, found in Articles 80 to 85, which include processing of personal data for journalistic purposes, health purposes, use in the employment context, historical, statistical or scientific purposes, use by individuals bound by a duty of professional secrecy, public interest;
c. The consent requirement which provides that consent will have to be given explicitly, rather than assumed;
d. The right to object to the processing of personal data would be supplemented by a right not to be subject to measures based on profiling;
e. The introduction of the controversial «right to be forgotten» that will allow people will be able to delete their data if there are no legitimate reasons for retaining it.

5.1. Health Data as Personal Data

According to Article 4(1) data subject is defined «any identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person», whilst Article 4(2) defines personal data as any information relating to a data subject.

In an effort to sustain a clear definition of health related data, Recital 12 determines that data concerning health means «any information which relates to the physical or mental health of an individual or to the provision of health services to the individual». Further, as pointed to Recital 26 personal data relating to health should include:

> all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples. Identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test.

When data concerning health is rendered anonymous, Recital 23 explicit mentions that the principles of protection should not apply since the data subject is no longer identifiable. However because re-identifying a person it is possible when using online services, since individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers, Recital 24 points out that account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual.

As a result the Proposed Regulation introduces the obligation of the controllers to implement:

> mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage …providing that those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals. (Article 23(2).

Accordingly, Article 33(1) requires from controllers or processors to carry out an impact assessment to assess re-identifiability on the protection of personal data when processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. However, re-identification is hard in most real-life situations because the lists of the people being searched are almost always incomplete –for instance, voter registration rolls usually miss 30% of the people in their region– and the best approach to minimise re-identification is to designate very precise de-identification rules (Omar, 2012). Maybe there is a potential risk from re-identification if the techniques and methods used for recording health realted data –and personal data in general– will become more complete and enhanced allowing through correlations the re-identification of a data subject, and this is the point needing legal protection.

5.2. Processing Health Data

The basic personal data processing principles are being retained and reinforced by the new ones of transparency, the clarification of the data, minimisation principle and the establishment of a comprehensive responsibility and liability of the controller as determined to Article 5:

a. processed lawfully, fairly and in a transparent manner in relation to the data subject;
b. collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
c. adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as,

the purposes could not be fulfilled by processing information that does not involve personal data;

d. accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research purposes in accordance with the rules and conditions of Article 83 and if a periodic review is carried out to assess the necessity to continue the storage;

f. processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation.

Further Recital 122 denotes that personal data related to health is a special category of data, the processing of which deserves higher protection, and often is justified by a number of legitimate reasons for the benefit of individuals and society as a whole in the context of ensuring continuity of cross-border healthcare, and, thus, should be subjected to specific and suitable safeguards so as to protect the fundamental rights and the personal data of individuals including the right for individuals to have access to their personal data concerning their health as for instance their medical records containing diagnosis, examination results, assessments by treating physicians and any treatment or interventions provided. Still personal data concerning health may be processed for reasons of public interest in the areas of public health, without consent of the data subject.[8] In such case Recital 123 specifies that the processing of personal data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers, insurance and banking companies.

Moreover, Article 9 sets out the general prohibition for processing special categories of personal data and the exceptions from this general rule. The processing of genetic data or data concerning health shall be prohibited with the exception the data subject has given consent to the processing of those personal data. Also when the processing

8 In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, meaning all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, healthcare needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality.

of data related health is necessary for health purposes, then the processing is subject to the conditions and safeguards referred to in Article 81, which provides that within the limits of the Proposed Regulation and in accordance with point (h) of Article 9(2), processing is only allowed if is necessary for:

a. the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies; or
b. reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety, inter alia for medicinal products or medical devices; or
c. other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.

The processing of personal data concerning health which is necessary for statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83; according to which personal data may be processed for, scientific research purposes only if these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject. It is also stated that any identifying information should be kept separately from the other information as long as these purposes can be fulfilled in this manner.

5.3. Consent Requirements

Articles 4(8) and 7(1) propose a reinforced definition of consent which is the very basis for the legitimacy of the processing (Gilbert, 2012). According to Article 4(8) the data subject's consent which shall mean any freely given specific, should also be informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed. In Explanation 3.4.1 is clarified that the criterion explicit is added to the consent definition in order to avoid confusing parallelism with unambiguous consent, and to have one single and consistent definition of consent, ensuring the awareness of the data subject that, and to what, he or she gives consent.

The controller shall bear the burden of proof for the data subject's consent to the processing of its personal data for specified purposes. Still for a data controller whether this could be a researcher or a doctor instead of obtaining patient consent would be

better to find other legitimate reasons to justify the processing of personal data (Long, Pavlou, & Walsch, 2012).

5.4. The Right to be Forgotten

Article 17 provides the data subject's right to be forgotten by elaborating on the right of erasure provided for in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten, including the obligation of the controller, which has made the personal data public, to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. In conjuction to Article 17, Recital 54 indicates that the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible to ensure this information. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.

Considering that a continually increasing number of patients and doctors communicate, interact and share information through social media using pcs, tablets and smatphones, it is obvious that the right to be forgotten, if applied, will create a number of issues since in case of the personal data been accessed by others there is no means of knowing who accessed it, when and what did he/she do with that data. Still the exemption for retaining personal data for a number of reasons relating to historical, statistical scientific research purposes is well-established in Article 83, as analysed above.

6. CONCLUSIONS

It is argued that «although health data is highly sensitive and thus require protection, they is also a public good» (Litan, 2012). Also, the more data analyzed the better chances to detect patterns that can lead to fewer wasteful procedures and tests, and «finding new causes, treatments, and even cures for diseases» (Litan, 2012). Big data in healthcare is very important for a number of reasons, most of them directly related to the immense capabilities of big data to combine patient level information with large existing data sets, which:

> will generate far more accurate predictive modeling, personalization of care, assessment of quality and value for many more conditions, and help providers better manage population health and risk-based reimbursement approaches. (Kocher & Roberts, 2012).

The right to privacy and the need to ensure the protection of patients' data is the key for the successful deployment of big data and open data policies. Citizens need to be able to trust that the use of their health data will be treated as confidential by all parties

involved in the delivery of health care services. The element of the traditional patient-doctor confidence should be built in solid base in order to boost the big data and open data initiatives.

The Proposed Regulation aims to reinforce the rights of citizens by introducing stricter rules on access, storage, processing and deletion of personal data. Therefore, the problem in question is to protect patients' personal data without impeding the effective delivery of health services. As noted above the delivery of healthcare relies upon data extracted from patient records and clinical records. Moreover, health and social insurance systems also need this kind of information for the purposes of planning, reimbursement, auditing and statistics (eHealth Governance Initiative, 2012). Health information may therefore be shared between the parties involved, as long as the specific conditions and safeguards provided by the Proposed Regulation are respected.

Anonymization should be the rule when processing patient-identifiable information for secondary use. Further, rights such as the right to be forgotten should be carefully examined since it might cause implications on useful information of clinical and financial data and research perspective, because the contingent deletion of data from electronic records, rendering them that way incomplete, can result in potential harm on a patient healthcare. For those involved in health research and health services is essential that the Proposed Regulation should ensure that health information will be available as a means to facilitate research and deliver of health care services, while striking the right balance with personal data protection.

7. REFERENCES

Al-Ubaydli, M. (2012, April 17). How social networks enable patients to be more involved in their healthcare. *Guardian Professional*. Retrieved February 15th, 2013 from http://www.guardian.co.uk/healthcare-network/2012/apr/17/patients-social-networks-new-technologies.

Barth-Jones, D. C. (2012, July 24). The «re-identification» of Governor William Weld's medical information: A critical re-examination of health data identification risks and privacy protections, then and now. *SSRN Library*. Retrieved April 22nd, 2013 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397.

Big data. (n.d.). In *Gartner IT glossary*. Retrieved February 3rd, 2013 from http://www.gartner.com/it-glossary/big-data/.

Boermeester, F. (2012, May 23). Top big data opportunities for health startups [Web log comment]. Retrieved February 9th, 2013 from http://healthstartup.eu/2012/05/top-big-data-opportunities-for-health-startups/.

Callens, S. (2010). The EU legal framework on e-health. In E. Mossialos, G. Permanand, R. Baeten & T. K. Hervey (Eds.), *Health Systems Governance in Europe* (pp. 561-588). Cambridge : Cambridge University Press.

Cohn, J. (2013). The robot will see you now. *The Atlantic, March 2013*. Retrieved March 3rd, 2013 from http://www.theatlantic.com/magazine/archive/2013/03/the-robot-will-see-you-now/309216/.

Commission of the European Communities (2002, May 28). *eEurope 2005: An information society for all action plan* (COM(2002) 263 final). Retrieved July 23rd, 2009 from http://ec.europa.eu/information_society/eeurope/2002/news_library/documents/eeurope2005_en.pdf.

Council of the European Union (2011, March 9). *Directive 2011/24/EU on the application of patients' rights in cross-border healthcare* (L88). Retrieved June 15th, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF.

Council of the European Union & Commission of the European Communities (2000, June 14). *eEurope 2002: An information society for all action plan*. Retrieved July 23rd, 2009 from http://ec.europa.eu/information_society/eeurope/2002/documents/archiv_eEurope2002/actionplan_en.pdf.

Dockser-Marcu, A., & Weaver, C. (2012, November 28). Heart gadgets test privacy-law limits. *The Wall Street Journal*. Retrieved February 8th, 2013 from http://online.wsj.com/article/SB10001424052970203937004578078820874744076.html.

eHealth Governance Initiative. (2012, October 22). *Discussion paper on implications of the proposed general regulation on data protection for health and e-health*. Retrieved February 11th, 2013 from http://cpme.dyndns.org:591/database/2012/Info.2012-122.Data.Protection.paper.for.eHN.final.pdf.

Essers, L. (2012, October 8). Medical privacy threatened by loophole in draft EU data protection law, professor warns. *Computerworld*. Retrieved February 12th, 2013 from http://news.idg.no/cw/art.cfm?id=905E03DE-D151-A1BC-F4FBA421C54FE418.

European Commission. (2004, April 30). *eHealth: Making healthcare better for European citizens* (COM(2004) 356 final). Retrieved January 15th, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0356:FIN:EN:PDF.

European Commission. (2005, June 1). *i2010: An information society for growth and employment* (COM(2005 229 final). Retrieved July 23rd, 2009 from http://eur-lex.europa.eu/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF.

European Commission. (2010, May 19). *A digital agenda for Europe* (COM(2010) 245 final/2). Retrieved January 18th, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

European Commission. (2012, January 25). *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)* (COM(2012) 11 final). Retrieved January 5th, 2013 from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

European Commission. (2012, January 25). *Data protection reform: Frequently asked questions* (MEMO/12/41). Retrieved January 5th, 2013 from http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=en.

European Commission. (2012, December 6). *eHealth Action Plan 2012-2020: Innovative healthcare for the 21st century* (COM(2012) 736 final). Retrieved January 15th, 2013 from http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=1252.

European Union, e-Health Task Force. (2012). *Redesigning health in Europe for 2020* (Report). Luxembourg : Publications Office of the European Union. Retrieved January 28th, 2013 from http://epractice.eu/en/library/5362646.

Hernandez, D. (2012, October 10). Big data is transforming healthcare. *Wired Magazine*. Retrieved February 1st, 2013 from http://www.wired.com/wiredscience/2012/10/big-data-is-transforming-healthcare/.

Gilbert, F. (2012, October 9). European data protection 2.0: New compliance requirements insight. *Santa Clara Computer & High Technology Law Journal 28*, 815-863. Retrieved January 9th, 2013 from http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1550&context=chtlj.

Grant, E. (2012). The promise of big data. *HSPH News, Spring/Summer*. Retrieved February 5th, 2013 from http://www.hsph.harvard.edu/news/magazine/spr12-big-data-tb-health-costs/.

Groenpj. (n.d.). Open data & healthcare [Web log comment]. Retrieved February 15th, 2013 from openhealthnews.com/blogs/groenpj/2012-03-06/open-data-healthcare.

International Business Machines. (n.d.). What is big data?. Retrieved February 3rd, 2013 from http://www-01.ibm.com/software/data/bigdata/.

Kocher, R., & Roberts, B. (2012, March 15). Meaningful use of health IT stage 2: The broader meaning [Web log comment]. Retrieved February 5th, 2013 from http://healthaffairs.org/blog/2012/03/15/meaningful-use-of-health-it-stage-2-the-broader-meaning/.

Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. (2012, May). The challenge of 'big data' for data protection. *International Data Privacy Law 2*(2), 47-49. Retrieved February 11th, 2013 from doi:10.1093/idpl/ips036.

Lewis, N. (2011, June 24). Drug prescription data mining cleared by Supreme Court. *InformationWeek*. Retrieved February 8th, 2013 from http://www.informationweek.com/healthcare/security-privacy/drug-prescription-data-mining-cleared-by/231000397.

Litan, R. E. (2012, May). Big data can save health care: But at what cost to privacy?. *TheAtlantic*. Retrieved January 31st, 2013 from http://www.theatlantic.com/health/print/2012/05/big-data-can-save-health-care-0151-but-at-what-cost-to-privacy/257621/.

Long, W., Pavlou, A., & Walsch, J. (2012, February 24). The new EU data protection regulation: What will the impact be on the life sciences industry?. *Script Regulatory Affairs*. Retrieved January 20th, 2013 from http://www.rajpharma.com/productsector/medicaldevices/The-new-EU-Data-Protection-Regulation-what-will-the-impact-be-on-the-life-sciences-industry-327344?autnID=/contentstore/rajpharma/codex/8dcf9154-5ef3-11e1-97a6-3968679900bf.xml.

Lohr, S. (2011, February 11). The age of big data. *The New York Times*. Retrieved February 1st, 2013 from http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all.

McKinsey Global Institute. (2011). *Big data: The next frontier for innovation, competition, and productivity*. Retrieved February 3rd, 2013 from http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation.

Milward, B. H., & Snyder, L. O. (1996). Electronic government: Linking citizens to public organizations through technology. *Journal of Public Administration Research and Theory* 6, 261-275.

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review 57*, 1701-1777. Retrieved February 11th, 2013 from http://www.uclalawreview.org/pdf/57-6-3.pdf.

Open Knowledge Foundation. (n.d.). What is open data?. Retrieved February 10th, 2013 from http://opendatahandbook.org/en/what-is-open-data/index.html.

Oram, A. (2012, September 24). Assessing the real risks of re-identifying patient data. *O'Reilly Strata*. Retrieved April 22nd, 2013 from http://strata.oreilly.com/2012/09/assessing-the-real-risks-of-re-identifying-patient-data.html.

Raash, C. (2012, December 4). Explosion of «big data» collection and analysis is hopeful, yet worrisome, trend. *USA Today*. Retrieved February 1st, 2013 from http://www.usatoday.com/story/tech/2012/12/04/big-data-explosion/1729535/.

Rooney, B. (2012, January 19). Health care is next frontier for big data. *The Wall Street Journal, Tech Europe*. Retrieved January 31st, 2013 from http://blogs.wsj.com/tech-europe/2012/01/19/health-care-is-next-frontier-for-big-data/.

Roop, E. S. (2012, September 10). Big data creates big privacy concerns. *For the Record 24*(16), 10. Retrieved February 11th, 2013 from http://www.fortherecordmag.com/archives/091012p10.shtml.

Rubinstein, I. (2013, January 25). Big data: The end of privacy or a new beginning?. *International Data Privacy Law*. Retrieved February 18th, 2013 from doi:10.1093/idpl/ips036.

Scherer, M. (2012, November 7). Inside the secret world of the data crunchers who helped Obama win. *Time Swampland*. Retrieved February 3rd, 2013 from http://swampland.time.com/2012/11/07/inside-the-secret-world-of-quants-and-data-crunchers-who-helped-obama-win/.

Szoka, B. (2012, September 6). Let's not exaggerate privacy risks: Re-identification isn't so easy after all, says New Barth-Jones paper. *The Technology Liberation Front*. Retrieved April 22nd, 2013 from http://techliberation.com/2012/09/06/lets-not-exaggerate-privacy-risks-re-identification-isnt-so-easy-after-all-says-new-barth-jones-paper/.

Tene, O., & Polonetsky, J. (2012, February 2). Privacy in the age of big data: A time for big decisions. *Stanford Law Review Online 64*, 63-69. Retrieved February 6th, 2013 from http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-63_1.pdf.

Terry, N. P. (2012). Protecting patient privacy in the age of big data. *UMKC Law Review 81*(2), 1-31. Retrieved February 8th, 2013 from http://dx.doi.org/10.2139/ssrn.2153269.

Tsiavos, P. (2011, December 06). *Open data*. Retrieved February 10th, 2013 from http://conferences.ellak.gr/opendata2011/files/2011/12/ΕΛΛΑΚ_03_12_11PDF.pdf.

United States, Executive Office of the President, Office of Science and Technology Policy.(2012, March 29) *Obama administration unveils «big data» initiative: Announces $200 million in new r&d investments*. Retrieved February 5th, 2013 from http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release_final_2.pdf.

United States, Department of Health & Human Services. (n.d.). About the health data initiative. Retrieved February 15th, 2013 from http://www.hhs.gov/open/initiatives/hdi/about.html.

Vu, D., & Slavkovic, A. (2009). Differential privacy for clinical trial data: Preliminary evaluations. In Y. Saygin, J. Xu Yu, H. Kargupta, W. Wang, S. Ranka, P. S. Yu and X. Wu (Eds.), *IEEE international conference on data mining, 6 December 2009, Florida*. Retrieved February 8th, 2013 from http://doi.ieeecomputersociety.org/10.1109/ICDMW.2009.52.

Wijsman, O. (2012, April 20). Big data, open data and eHealth in an ecosystem. Retrieved February 15th, 2013 from http://daa.ec.europa.eu/content/big-data-open-data-and-ehealth-ecosystem.

Wolf, R. (2013, June 13). Justices rule human genes cannot be patented. *USA Today*. Retrieved June 15, 2013 from http://www.usatoday.com/story/news/nation/2013/06/13/supreme-court-gene-breast-ovarian-cancer-patent/2382053/.

World Economic Forum. (2012). *Big data, big impact: New possibilities for international development*. Retrieved January 31st, 2013 from http://www3.weforum.org/docs/WEF_TC_MFS_BigDataBigImpact_Briefing_2012.pdf.

BIG DATA AND SOCIAL CONTROL IN THE PERSPECTIVE OF PROPOSED EU REFORM ON DATA PROTECTION

Alessandro Mantelero
Polytechnic University of Turin
Author of paragraphs 1, 3.1

Giuseppe Vaciago
University of Insubria
Author of paragraphs 2, 3.2

ABSTRACT: The revolution in social analysis due to Big Data and their predictive capacities poses different questions related to risks of asymmetries in the control over information.

To have access to this technology and to exploit its power it is necessary to have the availability of large data sets and to invest heavily in equipment and research. Only big companies and governments have these resources and, consequently, are able to use this control over digital information both to increase their performances and to increase their control over individuals.

Information found online, via activities of analysis, monitoring, geolocation and facial recognition that are not always legal, provide a glimpse into the lives of suspects, victims, and witnesses that wouldn't be possible with a real-life investigation. It is suffice to recall that in 2012 the Los Angeles Police Department is using a software application that can combine Big Data for the purpose of predicting and preventing crimes that appears to have contributed to the sensitive fall in the crime rate in the city.

From this perspective, considering the role of government agencies and their increasing requests of information to the private sector for public security purposes, it is necessary to adopt specific rules in order to regulate the information flow, define the rights over data and ensure adequate enforcement. If it is true that information is often publicly available, it is also true that the line between the public and private sphere will become even more blurred in the Big Data era.

KEYWORDS: privacy, data protection, social control, Big Data, European Union Law, Comparative Law.

1. SOCIAL AND LEGAL CHALLENGES OF BIG DATA

New technologies are not good or bad, they are only a new means to manage some aspects of life. However their use can be described as positive or negative. These considerations also apply to ICT, as demonstrated by the evolution of this technology over the last seventy years. From mainframes to tablets and from telephone networks to hight speed global networks, new technologies have been used to plan wars, destroy computer systems, steal information, but also to connect people, carry out innovative research, increase global knowledge and much more.

The difference between a positive or negative use of technology comes from the user. A computer and Internet can be used to close down local energy distribution system or to connect people fighting for democracy. From this perspective, considering the relationship between technology and human behaviour, the legal system as become a key element in managing technologies and orientate them towards useful purposes.

Historically regulations have to define the border between actions with a positive social output, which are permitted and induced by laws, and antisocial behaviours, which are inhibit and punished. This role is also played by the law in an ICT context.

Regulations on data protection, computer frauds and computer crimes are just a few examples of the role assumed by the law in shaping the use of new technologies and technologies themselves. In doing so, the law can use traditional «behavioural» rules, which permit or prohibit some activities by using a three-phase model focused on prescription, ex post evaluation and sanction. This model is efficient in contexts where individual activities are traceable and the identity of the author of illicit activities can be discovered. However, these conditions are not always present in on-line dimensions or they involve excessive costs. For this reason, a different approach based on the embedding of legal prescription into the design of technological devices and processes represents a good alternative. Law-orientated technologies offer more advantages in terms of enforcement and application in super-national contexts. Thus, shaping technologies in order to create a «structural» barrier to possible illicit uses should consequently reduce unlawful behaviours. The implementation of technology-based solutions is also less conditioned by the local legal framework than the implementation of «behavioural» solutions and could easily be realized uniformly in different legal systems. For these reasons, in many cases this approach is more suitable than ordinary «behavioural» rules to address the transnational dimension and the continuous evolutionary aspects of ICT regulation.

All these considerations can be made with regard to the Big Data context and can help in addressing the challenges that it poses to the existing legal framework.

Big Data is not something new, but currently is at the final stage of a long evolution of the capability to analyse data using computer resources. Big Data represents the convergence of different existing technologies that permit enormous data-centres to be built, create high-speed electronic highways and have ubiquitous and on-demand network access to computing resources (cloud computing). These technologies offer substantially unlimited storage, allow the transfer of huge amounts of data from one place to another and allow the same data to be spread in different places and re-aggregated in a matter of seconds.

All these resources permit a large amount of information from different sources to be collected. The whole dataset can be continuously monitored in order to identify the emerging trends in the flows of data. This approach is revolutionary and differs from the traditional sampling method, which is based on the extraction of a representative

sample from the total statistical population. This statistical method was necessary due to the absence of instruments that could analyse the entire population.

However, in order to define the sample it is necessary to define in advance the purposes of the research and some working hypotheses. In this sense traditional sampling methods show their limits because they tend to infer or imagine the relevant aspects to be examined, so unexpected tendencies may not be considered. On the contrary, using Big Data analytics, new trends become self-explanatory and the purposes are not necessarily defined in advance but are a consequence of monitoring the flows of data. In this sense, unlike the traditional method, the Big Data approach focuses on the tendencies which emerge from collected information. It use an inductive method which requires the largest amount of information possible, as it is not possible to select a representative sample in an analysis that does not start out with a precise target of study. This method involves a degree of statistical error, but at the same time it is possible to draw inferences about unknown facts from statistical occurrence and correlation, with results that are relevant in socio-political, strategical and commercial terms. Despite the weakness of this approach, it is useful for the prediction and perception of the birth and evolution of macro-trends, that can be later analysed in a more traditional statistical way in order to identify their causes.

The availability of these new technologies give a competitive advantage to those who own them in terms of capability to predict new economic, social and political trends. The control over the information deriving from Big Data is not accessible to everyone, as it is based on the availability of large datasets, expensive technologies and specific human skills to develop sophisticated systems of analyses and interpretation. For these reasons big business and governments are in the best position to take advantage of Big Data: they have large amounts of information on citizens and consumers and enough human and computing resources to manage it.

Now in the Big Data era, the same thing happens as the beginning of the computer era when only a few entities could buy and use the first mainframes, with consequences in terms of economic advantage and social control. In a similar way to that period, Big Data generates an asymmetric control over information in society.

Another relevant aspect of the control deriving from Big Data is the amount of it. Analyses focused on profiling permit us to predict the attitudes and decisions of any single user and even to match similar profiles. In contrast, Big Data is not used to focus on individuals, but to analyse large groups and populations; Big Data analytics do not predict the next book that the man in the street will read, but the political sentiment of an entire country.

This control is more pervasive when it is realised by government agencies, in countries where legal provisions give them the power to require information about individual citizens from private companies in order to realise an invasive and generalized moni-

toring of the behaviour of thousands of people[1]. The results are rather peculiar as, in this way, governments obtain information with the indirect «co-operation» of the users, those who probably would not give the same information to public entities if requested. Service providers collect personal data on the base of private agreements (privacy policies) with the consent of the user and for their own purposes, but governments exploit this practice and use mandatory orders to obtain the disclosure of information. This double mechanism hides from citizens the risk and the dimension of the social control that can be realized by monitoring social networks or other services.

From this perspective, the central role of individual consent in data protection principles and regulations reveals its very weakness. The complexity of data processes and the power of modern analytics drastically limit the awareness of data subjects, their capability to evaluate the various consequences of their choices and the expression of a real free and informed consent. This lack of awareness is not avoided by giving adequate information to the data subjects or by privacy policies, due to the fact that these notices are read only by a very limited number of users which, in many cases, are not able to understand part of the legal terms usually used in these notices[2].

These aspects are even more present in a Big Data context, where it is even more evident that the traditional model of data protection is in crisis[3]. The traditional model is based on notice, consent[4] and the coherence of the data collection with the purposes defined at the moment in which the information is collected. However, nowadays much of the value of personal information is not apparent when the notice and consent are normally given[5] and the «transformative»[6] use of Big Data makes it difficult to explain the description of all its possible uses at the time of initial collection.

Various commentators consider that the privacy risks related to Big Data analytics are low, pointing out the large amount of data processed by analytics and the de-identi-

---

1 See DARPA (2002). *Total Information Awareness Program (TIA). System Description Document (SDD), Version 1.1*. Retrieved February 10th, 2013 from http://epic.org/privacy/profiling/tia/tiasystemdescription.pdf. See also National Research Council (2008), Appendix I and Appendix J; Congressional Research Service (2008). More sources on TIA are available at http://epic.org/privacy/profiling/tia/.

2 See Turow, J., Hoofnagle, C., Mulligan, D., Good, N., & Grossklags, J. (2007), 723-749. See also Brandimarte, L., Acquisti, A., & Loewenstein, G. (2010).

3 See Cate, F.H. (2006), 343-345. See also Cate, F.H., Mayer-Schönberger, V. (2012), 4; Rubinstein, I.S. (2013), 2.

4 With regard to personal information collected by public entities the Directive 95/45/EC permits the data collection without the consent of data subject in various cases; however, the notice to data subjects is necessary also in these cases. See Articles 7, 8 and 10, Directive 95/46/EC.

5 See Cate, F.H., Mayer-Schönberger, V. (2012), 3.

6 See Tene, O., Polonetsky, J. (2012), 64.

fied nature of most of this data. This conclusion is wrong. Anonymity by de-identification is a difficult goal to achieve, as demonstrated in a number of studies[7]. The power of Big Data analytics to draw unpredictable inference from information undermines many strategies based on de-identification[8]. In many cases a reverse process in order to identify people is possible; it is also possible to identify them using originally anonymous data. Here, it is closer to truth to affirm that each data is a piece of personal information than to assert that it is possible to manage data in a de-identified way.

For these reasons, the study of the existing interaction between public and private social control and the analysis of specific forms in which it is realised represent the first step in order to define how to deal with these social and legal challenges.

2. INTERACTION BETWEEN PUBLIC AND PRIVATE IN SOCIAL CONTROL

The interaction between public and private in social control could be divided in two categories, both of which are significant with regard to data protection. The first concerns the collection of private company data by government and judicial authorities, whilst the second is the use by government and judicial authorities of instruments and technologies provided by private companies for organisational and investigative purposes.

With regard to the first category, the acquisition of data may take place by means of a court request after the commission of a crime, or by government agencies for the purpose of public security or by law enforcement agencies for the prevention and repression of crime.

When the court makes the data request, the fundamental rights of the person under investigation are usually respected as required in Europe by article 8 of the European Human Rights Convention[9] and in the United States by the Fourth Amendment. However, in May 2012, Congressman Edward Markey wrote to nine US wireless carriers, asking about their routine disclosure of customer information to law enforcement agen-

7 See Ohm, P. (2010), 1701-1777; United States General Accounting Office (2001), 68-72. See also Zang H., Bolot J. (2011); Golle, P., (2006); Sweeney, L., (2000). Simple Demographics Often Identify People Uniquely (also on the limited effort required to re-identify the data); Sweeney, L., (2000). Foundations of Privacy Protection from a Computer Science Perspective. But cf. Tene, O., Polonetsky, J, (2013), 19-21.

8 See Mayer-Schonberger, V., Cukier, K. (2013), 154-156. See also Schwartz, P.M., Solove, D.J. (2011). 1841-45.

9 See also articles 6 and 8 of the «Charter of Fundamental Rights of the European Union». With regard to the different approaches to privacy and security between Europe and America, Vaciago G., (2012), 109.

cies. The responses from the carriers reveal that the request without a court order were approximately 250.000 from law enforcement agencies in 2011[10]. Further more, in countries where the human rights protection threshold is much lower[11] the request is not made by the Court, but only from law enforcement agencies without judicial review.

When government agencies proceed to data acquisition, the issue of the possible violation of fundamental rights becomes more delicate. The Echelon Interception System[12] and the Total Information Awareness (TIA) Program[13] are concrete examples which are not isolated incidents. One only needs to think about the considerable amount of electronic surveillance legislation which, particularly in the wake of 9/11, has been approved in the US and, to a certain extent, in a number of European countries. The US has two main laws that make up the backbone of the relevant legislative framework. The first is the Foreign Intelligence Surveillance Act (FISA) of 1978[14] which lays down the procedures for collecting foreign intelligence information through the electronic surveillance of communications between foreign powers or their agents (who may well be US citizens), for homeland security purposes. The second is the Communications Assistance For Law Enforcement Act (CALEA) of 1994[15], which authorizes the law enforcement and intelligence agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in surveillance. Following the Patriot Act of 2001, which will hereinafter be described, a plethora of bill has been proposed. The most recent are the Cyber Intelligence Sharing and Protection Act (CISPA) of 2013[16], which would allow Internet traffic information to be shared between the U.S. government and certain technology and manufacturing companies and the Protecting Children From Internet Pornographers Act of 2011[17], which extends data retention duties to US Internet Service Providers. In Europe, the Communications Capabilities Develop-

10 Soghoian G., (2012), 24.

11 Lum, T., Figliola, P.M., Weed, M.C., (2012). *Report by the Congressional Research Service China, Internet Freedom, and U.S. Policy*. Retrieved March 4th, 2013, from http://www.fas.org/sgp/crs/row/R42601.pdf.

12 European Parliament, (2001). *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)*. Retrieved March 4th, 2013, from http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.

13 See fn. 3.

14 Foreign Intelligence Surveillance Act (50 U.S.C. § 1801-1885C).

15 Communications Assistance for Law Enforcement Act (18 USC § 2522).

16 Jaycox, M.M., Opsahl, K., (2013). *CISPA is Back*, Electronic Frontier Foundation. Retrieved March 4th, 2013, from https://www.eff.org/cybersecurity-bill-faq.

17 Protecting Children From Internet Pornographers Act of 2011.

ment Programme has prompted a huge amount of controversy, given its intention to create a ubiquitous mass surveillance scheme for the United Kingdom[18] in relation to phone calls, text messages and emails and extending to logging communications on social media. In France, Law 239 of 18 March 2003 concerning Internal Security and its subsequent amendments have led to the development of authorized data mining software such as ANACRIM (Système d'analyse criminelle-crime analysis system), which analyses various types of data. Without a shadow of doubt, there are provisions of the law already in force, or in the pipeline for approval, which authorize governmental authorities to gain access to a vast amount of personal and sensitive data held by private companies without any judicial review.

Other than judicial authorities' requests and government agencies's monitoring activities, there are cases in which Internet Service Providers collaborate over a simple request from the law enforcement agencies. The exponential increase in Big Data since 2001 has provided a truly unique opportunity. In this respect, a key role has been played by Social Media. One need only reflect on the fact that Facebook, Twitter, Google+ and Instagram, all of which are situated in Silicon Valley, boast around 2 billion users throughout the world[19] and many of these users are citizens of the European Union. Facebook's founder may have intended «to empower the individual,» but there is no doubt that SNSs have also empowered law enforcement[20]. Morozov correctly observes that Facebook candidly admits to monitoring certain online chats between minors and adults according to certain keywords, forwarding this information to the law enforcement officials in order to check whether there are the grounds for investigating whether «grooming»[21] has occurred.

To stay on the topic of information acquisition by the law enforcement, there are two interesting cases of the collection of Big Data for crime prevention purposes. The first is the «PredPol» software initially used by the Los Angeles police force and now by other police forces in the USA (Palm Beach, Memphis, Chicago, Minneapolis and Dallas). Predictive policing, in essence, cross check data, places and techniques of recent crimes with disparate sources, analyzing them and then using the results to anticipate,

18 Barret, D., (2012). *Phone and email records to be stored in new spy plan*, *The Telegraph*. Retrieved March 4th, 2013, from http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html.

19 Google+ currently has 400 million users, Instragram 90 million, Facebook 963 million e Twitter 637 million. Retrieved March 4th, 2013, from http://www.checkfacebook.com; http://socialfresh.com/1000instagram/; http://twopcharts.com/twitter500million.php; http://bgr.com/2012/09/17/google-plus-stats-2012-400-million-members/.

20 Kirkpatrick, D., (2010), 52.

21 Morozov, E., (2012). *Why We Shouldn't Let Facebook Predict Crimes, Fohla de Sao Paolo*. Retrieved March 4th, 2013, from http://www1.folha.uol.com.br/internacional/en/finance/1122328-why-we-shouldnt-let-facebook-predict-crimes.shtml.

prevent and respond more effectively to future crime. Even if the software house created by Predpol declares that no profiling activities are carried out, it becomes essential to carefully understand the technology used to anonimyze the personal data acquired by the law enforcement database. This type of software is bound to have a major impact in US on the conception of the protection of rights under the Fourth Amendment, and more specifically concepts such as «probable cause» and «reasonable suspicion» which in future may come to depend on an algorithm rather than human choice[22]. The second example is X1 Social Discovery software[23]. This software maps a given location, such as a certain block within a city or even an entire particular metropolitan area, and searches the entire public Twitter feed to identify any geo-located tweets in the past three days (sometimes longer) within that specific area. This application can provide particularly useful data to the purpose of social control. One can imagine the possibility to have useful elements (e.g. IP address) to identify the subjects present in a given area during a serious car accident or a terrorist attack.

From a strictly legal standpoint, this social control tools may be employed by gathering information directly from citizens due the following principle «where someone does an act in public, the observance and recording of that act will ordinarily not give rise to an expectation of privacy[24]». However, on a European level, whilst this type of data collection frequently takes place, it has been on the receiving end of criticism in case law from the ECHR which, in the Rotaru vs. Romania case[25], ruled that «public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities». As O'Floinn observes: «Non-private information can become private information depending on its retention and use. The accumulation of information is likely to result in the obtaining of private information about that person»[26]. On a US level, the subject has been addressed in the case People v. Harris[27], currently pending in front of the Supreme Court. On January 26, 2012, the New York County District Attorney's Office sent a subpoena to Twitter, Inc. seeking to obtain the Twitter records of user suspected of having participated in the «Occupy Wall Street» movement. Twitter refused to provide the law enforcement officers with the information requested and sought to quash the subpoena. The Criminal Court of New York confirmed the application made by the New York County District Attorney's Office, rejecting the arguments

22 Ferguson, A. G., (2012), 62

23 Retrieved March 4th, 2013, from http://www.x1discovery.com/social_discovery.html.

24 Gillespie, A., (2009), 552

25 Rotaru v Romania (App. No. 28341/95) (2000) 8 B.H.R.C. at [43].

26 O'Floinn, M., Ormerod, D., (2013), 24.

27 2012 NY Slip Op 22175 [36 Misc 3d 868].

put forward by Twitter, stating that tweets are, by definition, public, and that a warrant is not required in order to compel Twitter to disclose them. The District Attorney's Office argued that the «third party disclosure» doctrine put forward for the first time in United States v. Miller was applicable[28].

The second relationship concerns the use by the state of tools and resources from the private company for the purposes of organization and investigations. Given the vast oceans of big data, US governmental authorities decided to turn to the private sector, not only for purposes of software management but also in relation to management of the data itself. One practical example is the CTO's Hadoop platform[29], which is capable of memorizing and storing data in relation to many law enforcement authorities in US. Similarly, a private cloud system has emerged which conveys the latest intelligence information in near-real time to U.S. troops stationed in Afghanistan[30].

Considering costs saving and massive computing power of a centralized cloud system, it is inevitable that law enforcement, military forces and government agencies will progressively rely on this type of services. The afore-mentioned change will entail deducible legal issues in terms of jurisdiction, security and privacy regarding data management. The relevant legal issues might be solved through a private cloud within the State with exclusive customer key control. However, it is worth considering that, in this way, privates will enter into contact with a highly important and ever expanding information asset. Therefore they will be able to develop increasingly sophisticated and data mining tools, thanks to cloud systems' potential. This scenario, which is already a fact in the USA, might become reality also thanks to the impulse of the Digital Agenda for Europe and its promotion of Public Private Partnership initiatives on Cloud[31].

---

28 United States v. Miller (425 US 425 [1976]). In this case the United States Supreme Court held that the «bank records of a customer's accounts are the business records of the banks and that the customer can assert neither ownership nor possession of those records» .

29 CTO labs, (2012). *Big Data Solutions for Law Enforcement*, Retrieved March 4th, 2013, from http://ctolabs.com/wp-content/uploads/2012/06/120627HadoopForLawEnforcement.pdf.

30 *Big Data Cloud Delivers Military Intelligence to U.S. Army in Afghanistan*, (6 February 2012), Datanami. Retrieved March 4th, 2013, from http://www.datanami.com/datanami/2012-02-06/big_data_cloud_delivers_military_intelligence_to_u.s._army_in_afghanistan.html.

31 Commission of the European Communities, (2009). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. Retrieved March 4th, 2013, from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0479:FIN:EN:PDF. See also The European Cloud Partnership (ECP), (2013). Retrieved March 4th, 2013, from https://ec.europa.eu/digital-agenda/node/10565.

3. THE EU REFORM ON DATA PROTECTION

3.1. The EU Proposal for a General Data Protection Regulation

Modern social control is the result of the interaction between the private and public sector. This collaborative model is not only based on mandatory disclosure orders issued by courts or administrative bodies, but it is also extended to a more indefinite grey area of voluntary and proactive collaboration by big companies. It is difficult to get detailed information on this second model of voluntary collaboration, however the predominance of US companies in the ICT sector, particularly with regard to the internet and cloud services, increases the influence of the US administration on national companies and makes specific secret agreements of cooperation in social control easier.

From this perspective, the political and strategical value of the European regulation on data protection emerges. This regulation can assume the role of a protective barrier in order to prevent and limit access to the information about European citizens and companies[32]. In this sense, the EU Proposal for a General Data Protection Regulation extends its territorial scope[33] through the processing of personal data of data subjects residing in the EU «by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour»[34].

Although the Proposal for a new regulation does not regard the data processed by public authorities for the purposes of prevention, investigation, detection, prosecution of criminal offences or the execution of criminal penalties[35], its impact on social control is relevant, since in many cases the databases of private companies are the target of public authority investigations. For this reason, reducing the amount of data collected by private entities and increasing data subjects' self-determination with regard to their personal information limit the possibility of subsequent social control initiatives by government agencies.

32 Although only information regarding natural persons are under the European regulation on data protection, the data concerning clients, suppliers, employees, shareholders and managers have a relevant strategical value in competition.

33 See Article 3 (2), Proposal for a General Data Protection Regualtion (hereinafter abbreviated as PGDPR).

34 See also Recital 21.

35 This area will fall under the new Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, explanatory Memorandum, (SEC(2012) 72 final).

However, the complexity of data processes and the unclear wording of many privacy policies[36] along with the presence of technological and market lock-in effects reduce data subjects' awareness of the consequences of their consent and facilitate the creation of a wider database which is only accessible by the authorities in the cases provided by the law.

The EU Proposal, in order to reinforce the protection of individual information, interacts with these constraints and shifts the focus of data protection from an individual choice to a privacy-oriented architecture[37]. This approach, which limits the amount of data collected through «structural» barriers and introduces a preventive data protection assessment[38], also produces a direct effect on social control by reducing the amount of information available.

With regard to the information collected, the EU Proposal reinforces users' self-determination by requiring data portability, which gives the user the right to obtain a copy of the data undergoing processing from the controller «in an electronic and structured format which is commonly used and allows for further use by the data subject»[39]. Portability will reduce the risk of technological lock-in due to the technological standards and data formats adopted by service providers, which limit the migration from one service to another.

However, in many cases (e.g. Facebook, Google, Twitter, etc.), the services offered by Big Data owners, which generate these massive collections of information, are worldwide services provided by a very limited number of companies. In terms of social control, this situation reduces the chances for the users not to be tracked by moving their account from one platform to another and it also minimizes the positive effects of data portability.

Finally, the Proposal reinforces the right to obtain the erasure of data processed without the consent of the data subject, against his objection, without providing adequate information for him or outside of the legal framework[40]. An effective implementation of this right can reduce the amount of data stored by service providers, and limit the amount of information existing in the archives without a legitimate reason for the processing of information. In this manner, the possibility of consultation of the history of individual profiles by authorities is also reduced.

All the aspects considered above concur to limit the information available to all entities interested in social control, and therefore effect the request of disclosure held

36 See above § 1.

37 Artt 23, PGDPR.

38 Art. 33, PGDPR.

39 See Article 18, PGDPR.

40 See Mantelero, A., (2013).

by government agencies and courts to private companies. Nevertheless these powers of search and seizure and its exercise represent the fundamental core of social control.

In order to analyse this aspect in the scenario of the future European data protection framework it is necessary to consider both the proposal of the European Commission, the proposal for a new general data protection regulation and the less debated proposal for a directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Although the second proposal is more specific on governmental and judicial control, the first considers this aspect from the point of view of the data flows.

The new proposal, as well as the European regulation in force (Directive 96/46/EC), allows trans-border data flows from the EU to other countries only when the third country ensures an adequate level of protection[41]. In evaluating this level the Commission should also give consideration to the legislation in force in third countries «including concerning public security, defence, national security and criminal law»[42]. From this perspective, also the presence of invasive investigative public bodies and the lack of adequate guarantees to the data subject assume relevance in the decision to limit the trans-border data flows between subsidiaries and holding or between companies.

Once again this limit does not affect public authorities, but restricts the set of information held by private companies which can be scrutinised by them.

An explanatory case of the relationship between trans-border data flows, foreign jurisdiction and the possible effects on citizens and social control is given by the Swift case; the same criticism has been expressed by commentators with regard to the US Patriot Act. These two cases are different as in the first non-EU authorities requested to access information held by a company based in the EU, whereas in the second case the requests were directed to US companies in order to have access to the information they received from their EU subsidiaries.

In the Swift case[43] the Article 29 Data Protection Working Party clarified that a foreign law does not represent the legal base for the disclosure of personal information to non-EU authorities, since only the international instruments provide an appropri-

41 See Mantelero, A., (2012).

42 Art. 41 (2) (a), PGDPR.

43 See Article 29 Data Protection Working Party, *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, adopted on 22 November 2006.

ate legal framework enabling international cooperation[44]. Furthermore, the exception provided by Art. 26 (1) (b)[45] does not apply when the transfer is not necessary or legally required on important public interest grounds of an EU Member State[46].

On the contrary, as emerged in the Patriot Act case, but also with reference to the wider complex and dynamic system of powers the U.S. government has in the realm of criminal investigations and national security[47], the US authorities can access data held by the EU subsidiaries of US companies[48]. However, it is necessary to point out that there is a potential breach of protection of personal data of European citizens and that this happens not only with regards to US laws, but also in relations with other foreign regulations, as demonstrated by the recent Indian and Chinese laws on data protection.

In order to reduce such intrusions the draft version of the EU Proposal for a General Data Protection Regulation limits the disclosure to foreign authorities and provided that «no judgment of a court or tribunal and no decision of an administrative authority of a third country requiring a controller or processor to disclose personal data shall be recognized or be enforceable in any manner, without prejudice to a mutual assistance treaty or an international agreement in force between the requesting third country and the Union or a Member State»[49]. The draft also obliges controllers and processors to notify national supervisory authorities of any requests and to obtain prior authorization for the transfer by the supervisory authority[50]. Unfortunately these provisions have been dropped from the final version of the Proposal.

---

44 See Article 29 Data Protection Working Party, *Opinion 10/2006*, above fn. 43. See also Article 29 Data Protection Working Party, *Opinion 1/2006 on the application of the EU data protection rules to internal wistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against, banking and financial crime*, adopted on 1 February 2006.

45 Art. 26 (1) (b) justifies the transfer Transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims (Article 26 (1) (d) of the Directive.

46 See also Article 29 Data Protection Working Party, *Opinion 10/2006*, 25, above fn. 43 («any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in the Directive»).

47 See above § 2. See also van Hoboken, J.V.J., Arnbak, A.M., & van Eijk, N.A.N.M. (2012). *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act*, Institute for Information Law University of Amsterdam. Retrieved February 4th, 2013, from http://www.ivir.nl.

48 It is necessary to underline that the guarantees provided by the U.S. Constitution in the event of U.S. government requests for information do not apply to European citizens, as well as, legal protection under specific U.S. laws applies primarily to U.S. citizens and residents.

49 See Art. 42 (1), PGDPR , draft Version 56, November 29th, 2011.

50 See Art. 42 (2), PGDPR , draft Version 56, November 29th, 2011.

3.2. The «Police and Criminal Justice Data Protection Directive»

In addition to the Proposal for a General Data Protection Regulation, the above mentioned Directive on the protection of individuals with regard to the processing of personal data by competent authorities sets some important limitations to possible *violation* of *EU citizens' privacy.*

The goal of the directive is to ensure that «in a global society characterized by rapid technological change where information exchange knows no borders» the fundamental right to data protection is consistently protected[51]. One of the main issues at EU level is the lack of harmonization of Member States data protection law even more «in the context of all EU policies, including law enforcement and crime prevention as well as in our international relations»[52].

To achieve this goal, the proposal sets five important pillars that could be really useful to regulate the existing interaction between public and private social control of the citizens.

The first one is the fairly, lawful and adequate data processing during criminal investigations or to prevent a crime. Every data must be collected for specified, explicit and legitimate purposes and must be erased or rectified without delay[53].

The second one is the clear distinction of the various categories of the possible data subjects in a criminal proceeding (persons with regard to whom there are serious grounds for believing that they have committed or are about to commit a criminal offence, person convicted, victim of criminal offense, third parties to the criminal offence). For each of these categories there must be a different level of attention on Data Protection, especially for persons who do not fall within any of the categories referred above[54].

The third one is to prohibit measures which produce an adverse legal effect for the data subject or significantly affect, and which are based solely on automated processing of personal data[55].

---

51 Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, explanatory Memorandum, (SEC(2012) 72 final).

52 European Commission (2010). *Study on the economic benefits of privacy enhancing technologies or the Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*. Retrieved March 4th, 2013, from http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

53 Art. 1, Proposal for a Directive (SEC(2012) 72 final) (hereinafter abbreviated as PD).

54 Art. 5, PD.

55 Art. 9, PD.

The fourth one is the implementation of privacy by design and by default mechanism for ensuring the protection of the rights of the data subject and the processing of only those personal data[56].

The fifth one is the cooperation with the relevant supervisory authority by providing all information necessary to perform its duties.

Further more the proposal for a Directive entails the obligation to designate a data protection officer in the law enforcement agencies, to monitor the implementation and application of the policies on the protection of personal data[57].

These principles constitute an important limitation to possible data mining of personal and sensitive data collection by law enforcement agencies. If it is true that most of these provisions were also present in the Framework Decision 2008/977/JHA[58] , it is also true that propelling privacy by design and by default mechanisms and measures could allow to guarantee data anonymization and to avoid the indiscriminate use of automated processing of personal data.

The good examples we have on EU level with Europol[59] and Eurojust[60] are a good starting point, in the hope that this proposal will receive more attention by national law enforcement and other governmental authorities.

4. BIBLIOGRAPHY

Barrett, D., (18 February 2012). *Phone and email records to be stored in new spy plan, The Telegraph*. Retrieved March 4th, 2013, from http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2010). *Misplaced Confidences: Privacy and the Control Paradox*, Ninth Annual Workshop on the Economics of Information Security. Retrieved February 15th, 2013 from http://www.heinz.cmu.edu/~acquisti/papers/acquisti-SPPS.pdf.

56 Art. 19, PD.

57 Art. 30, PD.

58 Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, (2008), Official Journal L 350, 60-71.

59 Europol (2012), *Data Protection at Europol*, The Hague. Retrieved March 4th, 2013, from https://www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf

60 Rules of Procedure on the Processing and Protection of Personal Data at Eurojust (Text approved by the Council on 24 February 2005) (2005/C 68/01).

Cate, F.H. (2006). The Failure of Fair Information Practice Principles. In Jane Winn (ed.), *Consumer Protection in the Age of the Information Economy*, 343-345. Aldershot-Burlington:Ashgate. Retrieved February 9th, 2013 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972.

Cate, F.H., Mayer-Schönberger, V. (2012). *Notice and Consent in a World of Big Data. Microsoft Global Privacy Summit Summary Report and Outcomes*, 4. Retrieved February 15th, 2013 from http://www.microsoft.com/en-au/download/details.aspx?id=35596

Congressional Research Service, (2008). *CRS Report for Congress. Data Mining and Homeland Security: An Overview*. Retrieved February 10th, 2013 from www.fas.org/sgp/crs/homesec/RL31798.pdf.

European Commission (2010). *Study on the economic benefits of privacy enhancing technologies or the Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*. Retrieved March 4th, 2013, from http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pd.

European Parliament, (2001). *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)* (2001/2098/INI). Retrieved March 4th, 2013, from http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.

Ferguson, A. G., (2012). Predictive Policing: The Future of Reasonable Suspicion, *Emory Law Journal*, 62, 259. Retrieved March 4th, 2013, from .http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2050001##

Gillespie, A., (2009). Regulation of Internet Surveillance, *European Human Rights Law Review*, 4, 552.

Golle, P., (2006). Revisiting the uniqueness of simple demographics in the US population, *Proceedings of the 5th ACM workshop on Privacy in electronic society*, 77-80.

Jaycox, M.M., Opsahl, K., (2013). *CISPA is Back*, Electronic Frontier Foundation. Retrieved March 4th, 2013, from https://www.eff.org/cybersecurity-bill-faq.

Kirkpatrick, D., (2010). *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*, New York: Simon and Schuster.

Lum, T., Figliola, P.M., Weed, M.C., (2012). *Report by the Congressional Research Service China, Internet Freedom, and U.S. Policy*. Retrieved March 4th, 2013, from http://www.fas.org/sgp/crs/row/R42601.pdf. Omand D., Bartlett J., Miller C. (2012). *A balance between security and privacy online must be struck...*, London: Demos.

Mantelero, A., (2012). Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution, *European Journal of Law and Technology*, 3 (2), from http://ejlt.org//article/view/96.

Mantelero, A., (2013). The EU Proposal for a General Data Protection Regulation and the roots of the «right to be forgotten», *Computer Law & Security Review*, XXX, (forthcoming).

Mayer-Schonberger, V., Cukier K., (2013). Big Data: A Revolution That Will Transform How We Live, Work and Think, London: John Murray (Publishers).

National Research Council (2008). *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, Washington, D.C.:The National Academies Press

O'Floinn, M., Ormerod D., (2011). Social networking sites RIPA and criminal investigations, (2011), *Crim. L.R.* 766, 24

Ohm, P. (2010). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA L. Rev.*, 57, 1701-1777

Rubinstein, I.S. (2013). Big Data: The End of Privacy or a New Beginning?, *International Data Privacy Law*, 2, retrieved February 15th, 2013 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2157659.

Schwartz, P.M., Solove, D.J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 New York University Law Review, 1814.

Signorini, A., Segre, A.M., Polgreen, P.M., (2011). The use of Twitter to track levels of disease activity and public concern in the U.S. during the Influenza A H1N1 pandemic, (2011), *PLOS ONE*, 6, 5

Soghoian, G., (2012). *The Spies We Trust: Third Party Service Providers and Law Enforcement Surveillance*, PHD dissertation, Department of Computer Science Indiana University. Retrieved March 4th, 2013, from http://files.dubfire.net/csoghoian-dissertation-final-8-1-2012.pdf.

Sweeney, L. (2000). Simple Demographics Often Identify People Uniquely, *Data Privacy Working Paper 3*, Carnegie Mellon University, Pittsburgh.

Sweeney, L. (2000). Foundations of Privacy Protection from a Computer Science Perspective. *Proceedings, Joint Statistical Meeting, AAAS,* Indianapolis.

Tene, O., Polonetsky, J. (2012). Privacy in the Age of Big Data: A Time for Big Decisions, *Stan. L. Rev. Online* 64, 64.

Tene, O., Polonetsky, J, (2013). Big Data for All: Privacy and User Control in the Age of Analytics, *Northwestern Journal of Technology and Intellectual Property*, (forthcoming). Retrieved April 24th, 2013, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2149364.

The Global Information Society Project (GISP), (2003). *Report to Congress regarding the Terrorism Information Awareness Program, in response to Consolidate Appropriations Resolution*, Pub. L. No 108-7, Division M, 111 (b). Retrieved March 4th, 2013, from http://www.information-retrieval.info/docs/tia-exec-summ_20may2003.pdf.

Turow, J., Hoofnagle, C., Mulligan, D., Good, N., & Grossklags, J. (2007). The Federal Trade Commission and Consumer Privacy in the Coming Decade, *ISJLP* 3, 723-749. Retrieved February 10th, 2013 from http://scholarship.law.berkeley.edu/facpubs/935.

United States General Accounting Office (2001). *Record Linkage and Privacy. Issues in creating New Federal Research and Statistical Information*, April 2011, 68-72. Retrieved April 19th, 2013, from http://www.gao.gov/assets/210/201699.pdf.

Vaciago, G., (2012). *Digital Forensics*, Turin: Giappichelli.

van Hoboken, J.V.J., Arnbak, A.M., & van Eijk, N.A.N.M. (2012). *Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act*, Institute for Information Law University of Amsterdam. Retrieved February 4th, 2013, from http://www.ivir.nl.

Whittaker, Z. (2012). *Yes, the FBI and CIA can read your email. Here's how*, ZDNet. Retrieved March 4th, 2013, from http://www.zdnet.com/yes-the-fbi-and-cia-can-read-your-email-heres-how-7000007319/.

Wind-Cowie, M., Lekhi, R. (2012). *The Data Dividend*, London: Demos.

Zang, H., Bolot, J. (2011). Anonymization of location data does not work: a large-scale measurement study. Proceeding MobiCom '11 Proceedings of the 17th annual international conference on Mobile computing and networking, 145-156, ACM New York.

REDES SOCIALES DE INTERNET, RESPONSABILIDAD NO CONTRACTUAL POR VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES (POR EL RESPONSABLE DEL FICHERO DE DATOS) Y DERECHO INTERNACIONAL PRIVADO*

Alfonso Ortega Giménez
Profesor de Derecho internacional privado de la Universidad Miguel Hernández de Elche (Alicante)-España

RESUMEN: Hoy día, gracias a Internet resulta sencillo navegar entre páginas, y, por ello, entre países y jurisdicciones de tal forma que con sólo hacer click uno abandona una página ubicada en territorio español para pasar a ver otra página almacenada en la otra punta del planeta. Sin duda, hablar de las redes sociales de Internet es hablar de relaciones privadas internacionales, esto es, es hablar de Derecho internacional privado. Es más, la mayor parte de las operaciones realizadas en Internet son internacionales: en tales situaciones hay presente uno o múltiples elementos extranjeros y/o producen efectos en varios países o incluso en todo el mundo. Por tanto, los posibles problemas de vulneración de datos de carácter personal derivados de la utilización de redes sociales de Internet deben ser resueltos, a partir de las normas de Derecho internacional privado español relativas a la responsabilidad civil contractual o extracontractual. Debemos justificar que el Derecho internacional privado sea la rama del ordenamiento jurídico español que resuelva los litigios derivados de la vulneración del derecho a la protección de datos de carácter personal; y, por tanto, reflexionar acerca de dos problemas capitales: la determinación de la competencia judicial internacional, así como de la ley aplicable.

PALABRAS CLAVE: redes sociales, derecho internacional privado, protección de datos, internet, competencia judicial internacional, ley aplicable.

1. PLANTEAMIENTO: LOS POSIBLES RIESGOS DE LAS REDES SOCIALES DE INTERNET, SUS CONSECUENCIAS JURÍDICAS Y EL DERECHO INTERNACIONAL PRIVADO

España, hoy día, es el segundo país europeo en participación en redes sociales de Internet, sólo por detrás de Reino Unido. Al menos 13.000.000 de españoles están co-

* El presente trabajo se ha realizado en el marco del Proyecto de investigación «Los desafíos jurídicos de Internet para la protección de los datos personales: hacia un marco normativo de tercera generación» (DER2009-09157), financiado por el Ministerio de Economía y Competitividad.

nectados a través de *Twitter*, *Facebook*, *Tuenti,* o *MySpace*, por citar sólo las más conocidas. Son el 73.7% de los usuarios de Internet, según la auditora *Comscor*. Es de esas cosas para las que las estadísticas sólo vienen a confirmar algo que ya compruebas mirando a tu alrededor. El número de internautas españoles que están suscritos a una red social ha pasado en un año del 45% al 81%, según destaca el 2º Observatorio de Redes Sociales, elaborado por *The Coctel Analysis*. El número medio de redes sociales a las que está suscrito un internauta ha pasado también de 1.7 en 2008 a 2.3 en 2009.

Los posibles problemas de vulneración de datos de carácter personal derivados de la utilización de redes sociales de Internet deben ser resueltos, a partir de las normas de Derecho internacional privado español relativas a la responsabilidad civil contractual o extracontractual. Debemos justificar que el Derecho internacional privado sea la rama del ordenamiento jurídico español que resuelva los litigios derivados de la vulneración del derecho a la protección de datos de carácter personal, proponiendo soluciones tales como la unificación de las normas estatales de Derecho internacional privado para evitar la relatividad de las soluciones y/o la utilización de criterios subjetivos, flexibles y particulares, que permitan la vinculación del supuesto concreto con un país determinado.

2. REDES SOCIALES DE INTERNET Y RESPONSABILIDAD NO CONTRACTUAL POR VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES: PROBLEMAS DE DERECHO INTERNACIONAL PRIVADO

En el ámbito del Derecho internacional privado, los problemas para el derecho a la protección de datos personales el uso de las redes sociales de Internet que plantean están relacionados con la determinación del órgano jurisdiccional competente para conocer de un determinado litigio, así como de la determinación de la ley aplicable para resolver el conflicto planteado. La delimitación de ambos aspectos será de vital importancia ya que, como es bien sabido, cada sistema jurídico tiene establecido un sistema de normas de conflicto, en virtud del cuál se determina quién será el órgano jurisdiccional competente y cual será la ley aplicable para resolver la controversia que se plantee[1].

El daño derivado de la intromisión ilegítima en el derecho a la protección de datos, manifestado en el uso indebido o ilegítimo de sus datos personales, consecuencia de la utilización de redes sociales de Internet, sobre la base de la existencia o no de una vinculación jurídica entre el causante del daño y el afectado, puede dar lugar a la exigencia de respon-

1 *Vid.*, sobre la materia, en particular, BING, J., «*Data protection, jurisdiction and the choice of law* », en *Privacy Law & Policy. Reporter*, volume 6, 1999, pp. 92-98; y, REIDENBERG, Joel R., «Technology and Internet Jurisdiction», en *UNIVERSITY OF PENNSYLVANIA LAW REVIEW,* Vol. 153, pp. 1951-1974.

sabilidad civil contractual (= cuando entre el autor y la víctima hubiere existido una previa relación contractual y se hubiere producido un incumplimiento de lo pactado), o extracontractual (= exigencia de una indemnización por los daños y perjuicios ocasionados).

La exigencia de una indemnización por daños y perjuicios (contra el responsable del fichero de datos)[2] derivada del tratamiento ilícito de datos, gracias al uso de las redes sociales de Internet, no excluye la posibilidad de ejercitar los derechos de acceso, rectificación y cancelación frente al propio responsable del fichero de datos. Los afectados o interesados por el tratamiento de sus datos, como titulares del derecho fundamental a la protección de datos, se encuentran facultados para conocer y acceder a las informaciones que les pudieran afectar, archivadas en bancos de datos, y controlar su calidad, permitiendo que puedan ser corregidos o cancelen los datos inexactos o indebidamente procesados, y la disposición sobre su transmisión.

3. REDES SOCIALES DE INTERNET, PROTECCIÓN DE DATOS, Y COMPETENCIA JUDICIAL INTERNACIONAL

3.1. El sistema español de competencia judicial internacional

La determinación de la competencia judicial internacional en materia de reclamaciones por la vulneración del derecho a la protección de datos (contra el responsable del fichero de datos) derivada del tratamiento ilícito de datos, gracias al uso de las redes sociales de Internet, nos lleva a un laberinto normativo de intrínseca complejidad, ya que se acumulan fuentes de origen diverso: institucional o comunitario, convencional y autónomo. Así, debemos acudir a los siguientes instrumentos normativos: 1º) al «limitado»[3] Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Bruselas, el 27 de septiembre de 1968 (en lo sucesivo, CB); 2º) a su «gemelo»[4], el «también limitado» Convenio relativo a la competencia judicial y a la ejecución de resoluciones judiciales en materia civil y mercantil, hecho en Lugano, el 16 de septiembre de 1988 (a partir de ahora, CL)[5], y su «sucesor», el Convenio de «Lugano II», de 30 de octubre de 2007, relativo a la competencia judicial, el reconocimiento y la

2 Hemos optado por centrar el tema en un caso concreto de responsabilidad no contractual contra el responsable del fichero de datos, entendido como el responsable por infracción de las normas de tratamiento de datos de carácter personal.

3 El CB se aplica, en la actualidad, únicamente con relación a los territorios franceses de ultramar y a las Antillas holandesas.

4 El CB y el CL poseen un contenido normativo prácticamente idéntico, siendo sus únicas diferencias las referidas al contrato individual de trabajo y a los contratos de arrendamiento de corta duración.

5 *BOE* núm. 243, de 10 de octubre de 1979.

ejecución de resoluciones judiciales en materia civil y mercantil[6] (en adelante, CL II); 3º) al Reglamento (CE) nº 44/2001, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil –Reglamento «Bruselas I»– (a partir de ahora, RB)[7]; o, 4º) a la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (en adelante, LOPJ)[8]. La aplicación de un instrumento jurídico u otro dependerá del domicilio del demandado.

La estructura de los foros de competencia judicial internacional del CB, del CL, del CL II, y del RB, se construye sobre tres niveles jerarquizados: a) el primer nivel está constituido por las «competencias exclusivas» previstas en los artículos 22 del RB/CL II y 16 del CB/CL. En determinadas materias, este precepto atribuye competencia única y exclusiva a los tribunales de un Estado miembro, excluyendo absolutamente la posibilidad de que conozcan cualesquiera otros tribunales. Si se trata de una de las materias previstas en los artículos 22 del RB/CL II o 16 del CB/CL, el tribunal del Estado competente de oficio controlará su competencia, excluyendo la posibilidad de que otros tribunales pudieran declararse competentes para conocer del mismo litigio; b) si no se trata de una de las materias previstas en el artículo 22 del RB/CL II o 16 del CB/CL, es preciso recurrir al segundo escalón en el orden jerárquico: al principio de autonomía de la voluntad. La voluntad de las partes (= «sumisión expresa»), prevista en el artículo 23 del RB/CL II y 17 del CB/CL atribuye competencia exclusiva a los tribunales designados por las partes. No obstante, el acuerdo de sumisión a los tribunales de un Estado miembro siempre puede ser modificado tácitamente, mediante la «sumisión tácita» por ambas partes a otros tribunales (= artículos 24 del RB/CL II y 18 del CB/CL); y, finalmente, c) el tercer escalón jerárquico de las reglas de competencia judicial internacional opera en defecto de sumisión expresa o tácita por las partes y siempre que no se trate de una de las materias objeto de competencias exclusivas. En tales casos, serán competentes, indistintamente, los tribunales del «domicilio del demandado» (= artículo 2 del RB/CL II y del CB/CL), o los designados por los foros especiales de competencia (= «competencias especiales») previstos en el artículo 5 del RB/CL II y del CB/CL.

Por último, debemos acudir a la LOPJ, que, en su artículo 22, recoge las normas de competencia judicial internacional aplicables para que un órgano jurisdiccional español se declare competente, ante la imposibilidad de aplicación del RB/CL II, o del CB/ CL. La LOPJ recoge en su artículo 22.1, en primer término, una serie de foros de competencia que presentan «carácter exclusivo» y que se inspiran y coinciden en buena

6 *DOUE* L 339, de 21 de diciembre de 2007. Este texto convencional entró en vigor el 01/01/2010. Son Estados parte: los Estados miembros de la UE, incluido Dinamarca (desde el 01/01/2010), Noruega (desde el 01/01/2010), Suiza (desde el 01/01/2011), e Islandia (desde el 01/05/2011).

7 *DOCE* 2001 L 12/1.

8 *BOE* núm. 157, de 2 de julio de 1985.

medida con los previstos en el artículo 16 del CB/CL. El artículo 22.2 recoge dos foros generales que atribuyen competencia a los órganos jurisdiccionales cualquiera que sea la materia afectada: sumisión a los Juzgados o Tribunales españoles y domicilio del demandado en España. Por último, el artículo 22.3 recoge diversos foros de competencia que nos recuerdan a las «competencias especiales» del artículo 5 del RB/CL II y del CB/CL.

Centrándonos en la materia que nos ocupa, «lo habitual» será que nos encontremos ante una **reclamación por daños y perjuicios (contra el responsable del fichero de datos) por vulneración del derecho a la protección de datos en el ámbito de las redes sociales de Internet**[9], en aplicación del RB/CL II, del CB/CL, los criterios atributivos de competencia son los siguientes: a) el foro del domicilio del demandado, esto es, los tribunales del país donde esté domiciliado el *presunto vulnerador-demandado* conocerá de todas las pretensiones que se deduzcan contra él, independientemente del país o países en los que se haya producido el hecho dañoso; b) el foro de la sumisión, expresa o tácita, que nos permite concentrar los litigios a los que las partes se refieran, bajo el conocimiento de los tribunales de un solo país; y, c) el foro del lugar del hecho dañoso, que atribuye competencia a los tribunales del «lugar donde se hubiere producido o pudiere producirse el hecho dañoso» del que nace la responsabilidad extracontractual, pudiendo considerarse como *país donde ocurre el hecho dañoso* tanto el país donde ocurre el hecho causal como el país donde se verifica el resultado lesivo, esto es, el país donde radica el fichero de datos. Ahora bien, esto no tiene por qué ser siempre así, ya que, por ejemplo, si la actividad consiste en la recogida ilícita de datos en España para su ulterior almacenaje informático en un fichero sito en Lisboa, el lugar del daño es tanto España como Portugal.

En definitiva, los foros de competencia operativos en materia de reclamación por daños y perjuicios por vulneración del derecho a la protección de datos en el ámbito de las redes sociales de Internet serían los siguientes: los *Tribunales elegidos por las partes en virtud de sumisión expresa o tácita*, el *domicilio del demandado* y el *lugar donde se hubiere producido o pudiere producirse el hecho dañoso*. Veamos cada uno de ellos:

3.2. Foro de la sumisión de las partes

Este fuero de atribución de competencia (= sumisión expresa o tácita de las partes a favor de los Tribunales de un determinado Estado) viene contemplado en los instrumen-

9 Otra posibilidad, que no será objeto de análisis en este trabajo, es el enfoque «presunto infractor (= responsable del fichero de datos)-consumidor (= titular del derecho a la protección de datos)», que nos exigiría analizar, desde el punto de vista de la responsabilidad contractual, cómo podrían influir las normas de protección de los consumidores en relación con el *choice of forum/ius* que se hace en los «contratos de adhesión» que plantean la gran mayoría de redes sociales de Internet, y que responden a una sumisión a favor de los tribunales del lugar donde se encuentran establecidas dichas redes sociales de Internet, y una elección de su ley aplicable.

tos internacionales de atribución de competencia judicial internacional antes mencionados (= artículos 23 y 24 del RB/CL II; y, 17 y 18 del CB/CL), y no introduce ningún cambio sustancial respecto a los criterios aplicables al resto de litigios transfronterizos. Por su parte, el artículo 22.2 de la LOPJ afirma que los tribunales españoles serán competentes «cuando las partes se hayan sometido expresa o tácitamente a los Juzgados o Tribunales españoles». El *acuerdo de sumisión* es un pacto entre las partes de una relación jurídica en cuya virtud éstas determinan el órgano jurisdiccional competente para conocer de los litigios que eventualmente pudieran surgir entre las partes. Tal sumisión puede realizarse mediante acuerdo *expreso* o mediante ciertas prácticas que denotan la voluntad de las partes de someterse a un órgano jurisdiccional: es la sumisión *tácita*.

Para que el acuerdo de *sumisión expresa* sea válido es necesario, fundamentalmente, que: a) se designen claramente los tribunales a los que se someten las partes; y, b) el acuerdo de sumisión expresa puede realizarse en cualquier momento, antes o después de la conclusión de un contrato o negocio internacional.

Por su parte, se entiende que las partes se someten tácitamente a los tribunales españoles cuando el demandante acude a tales tribunales interponiendo la demanda o formulando petición o solicitud que haya de presentarse ante el tribunal competente para conocer de la demanda, y cuando el demandado realiza, después de personado en el juicio tras la interposición de la demanda, cualquier gestión que no sea la de proponer en forma la declinatoria.

La validez de un acuerdo atributivo de competencia exige la prueba del acuerdo efectivo entre el demandante y el demandado: la sumisión debe hacerse por escrito[10]; en este sentido, el RB/CL II, sensible con su adaptación al entorno de Internet, admite la formalización de la sumisión expresa por medios electrónicos; esto es, la elección *online* del tribunal competente, siempre que se encuentre en el territorio cubierto por la aplicación del RB; y, la elección del mismo podrá efectuarse bien mediante intercambio de *emails* o especificándose claramente en el contrato *interpartes*[11].

3.2.1. Foro de la sumisión expresa

Los artículos 23 del RB/CL II y 17 del CB/CL (= *sumisión expresa*) constituyen una prolongación de la autonomía de la voluntad al campo de la competencia judicial internacional, ya que permiten a las partes (a ambas o a una con el consentimiento de la

10 *Vid.*, en general sobre la validez de las cláusulas atributivas de competencia en el comercio electrónico, DE MIGUEL ASENSIO, Pedro, *Derecho privado de Internet.* 3ª edición, Civitas, Madrid, 2002, pp. 448-455.

11 *Vid.*, en relación con la elección *online* de los Tribunales competentes, CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Conflictos de leyes y conflictos de jurisdicción en Internet.* Colex, Madrid, 2001, pp. 43-46.

otra) atribuir a los tribunales de un Estado la competencia para conocer de las controversias que puedan surgir del mismo. Asimismo, de acuerdo con los artículos 24 del RB y 18 del CB/CL, las partes se pueden someter tácitamente a un tribunal nacional que, en principio, no resultaría competente.

El foro de competencia judicial internacional de la sumisión expresa exige que nos encontremos ante un *litigio internacional* (= que quede dentro del ámbito de aplicación material del RB, CB/CL); que al menos una de las partes litigantes tenga su domicilio en un *Estado contratante* (esto es, miembro del RB/CL II, CB/CL); y, que se designe como competente un determinado tribunal (de un Estado del RB/CL II, CB/CL).

En este contexto, p. ej., la letra de las Condiciones de uso de **Tuenti** nos permite concluir que las partes (Tuenti –responsable del fichero de datos– y el usuario) «[...] con renuncia expresa a cualquier otro fuero que pudiera corresponderles, se someten a los **Juzgados y Tribunales de la ciudad de Madrid** [...]».

3.2.2. Foro de la sumisión tácita

Se considera que existe *sumisión tácita*[12], de acuerdo con el artículo 24 del RB/CL II y el artículo 18 del CB/CL la siguiente conducta procesal de las partes: cuando el demandante presenta una demanda ante el tribunal de un Estado miembro y la comparecencia del demandado ante ese tribunal no tiene por objeto impugnar su competencia judicial[13]. En tal caso, debe entenderse que las partes aceptan tácitamente someter el litigio a ese tribunal. Aunque no lo diga explícitamente el artículo, resulta independiente para su aplicación que el domicilio de las partes se halle en el territorio de un Estado miembro; lo relevante, en la práctica, es que el litigio sea «internacional»; que se presente la demanda ante un tribunal de un Estado del RB/CL II, CB/CL; y, que el demandado comparezca y conteste o formule reconvención.

Los requisitos básicos para que se entienda que se ha producido sumisión tácita son los siguientes: por un lado, que, interpuesta la demanda por el demandante ante

12 El foro del acuerdo de sumisión tácita para la determinación del Tribunal internacionalmente competente permite el ahorro de costes procesales y (al igual que con la sumisión expresa) que las partes decidan ante qué tribunal quieren litigar. *Vid.*, en general, sobre el concepto, límites y requisitos de la sumisión tácita como foro de competencia judicial internacional, *Vid.* CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, «La sumisión tácita como foro de competencia judicial internacional y el artículo 24 del Reglamento 44/2001, de 22 de diciembre 2000», en CALVO CARAVACA, Alfonso-Luis y AREAL LUDEÑA, Santiago, *Cuestiones actuales del Derecho mercantil internacional*. Colex, Madrid, 2005, pp. 203-215.

13 Tampoco operará la sumisión tácita cuando nos encontremos ante materias que son objeto de competencias exclusivas, *Vid*. CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier*, Derecho internacional privado.* vol. I, Comares, Granada, 2003, pág. 130.

los órganos jurisdiccionales de un Estado concreto, el demandado efectúe después de personado en juicio cualquier gestión distinta de la de impugnar la competencia; y, por otro lado, que la controversia no verse sobre ninguna de las denominadas *competencias exclusivas* (artículos 22 del RB/CL II y 16 del CB/CL).

Para que no exista sumisión tácita, la impugnación de la competencia del tribunal ante el que se presenta la demanda debe realizarse de acuerdo con las normas de Derecho procesal del Estado del foro (esto es, el Derecho procesal del país cuyos tribunales conocen del asunto). En el caso de España, la impugnación debe realizarse en el momento y de acuerdo con los cauces procesales previstos en el artículo 64 de nuestra LEC.

3.2.3. Sumisión a tribunales extranjeros

Y ¿qué ocurriría si el actor presentara su demanda ante los tribunales españoles, pero, existiera un acuerdo de sumisión entre las partes a favor de tribunales extranjeros?... ¿deberían los tribunales españoles declararse incompetentes por la razón de que existe un pacto de sumisión a favor de los tribunales extranjeros? (= admitir o no la declinatoria internacional –*derogatio fori*– sobre la base de la *sumisión a tribunales extranjeros*). En otras palabras, ¿pueden derogar las partes las partes la competencia judicial internacional atribuida a los órganos jurisdiccionales españoles vía artículo 22 de la LOPJ –ya que este problema sólo se plantea en los supuestos en los que la competencia judicial internacional deba resolverse conforme a este precepto y no con arreglo al RB/CL II o al CL/CL–, a través de un acuerdo en virtud del cual someten el litigio a tribunales extranjeros o a arbitraje privado internacional?

Si bien la LOPJ guarda silencio sobre esta cuestión, la jurisprudencia del TS ha sido la que ha arrojado algo de luz sobre la materia: en un primer momento, se mostró radicalmente contraria a admitir la *derogatio fori*; pero, en un segundo momento, aceptó y acepta una admisión matizada de la misma. Por tanto, hoy día, si el asunto ha sido sometido por las partes a tribunales extranjeros (o a arbitraje privado internacional), estos (o la Corte arbitral) y no los tribunales españoles, son los que deben conocer del litigio[14].

En nuestro caso, las principales redes sociales abogan por esta solución: así, de la lectura de las diferentes Condiciones de uso se deduce: en el caso de **Facebook** (= **responsable del fichero de datos**), que: « [...] Al visitar o hacer uso del Sitio o el Servicio, aceptas que las leyes del estado de Delaware, sin tener en cuenta los principios del conflicto de leyes, regularán estas condiciones de uso así como cualquier disputa que pudiera surgir entre tú y la Compañía o con alguno de nuestros afiliados. Respecto a toda disputa o queja no sujeta a arbitraje (tal y como se indica abajo), estás de acuerdo en no emprender ninguna acción fuera del estado y de los tribunales federales de California, y

14 *Vid.*, en sentido amplio, CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Derecho internacional privado.* vol. I, 9ª edición, Comares, Granada, 2008, pp. 200-205.

con esto das el consentimiento, y prescindes de toda defensa de carencia de jurisdicción personal o de foro de no conveniencia respecto a esto, lugar de reunión y órgano jurisdiccional del estado y **tribunales federales de California** [...] »; y, en el caso de **MySpace** (= **responsable del fichero de datos**) las partes « [...] aceptan someterse a la jurisdicción exclusiva de los **tribunales con asiento en el Estado de Nueva York** para resolver cualquier controversia que surja en relación con el Acuerdo o los Servicios MySpace [...] ».

3.3. Foro del domicilio del demandado

La aplicación del foro general del domicilio del demandado (= *forum defensoris*) viene contemplado en los diferentes instrumentos jurídicos relativos a la atribución de competencia judicial internacional antes reseñados; así, a falta de pacto expreso o tácito atributivo de jurisdicción, el criterio que atribuye competencia es el del *domicilio del demandado* (= artículo 2 del RB/CL II, o del CB/CL), que lo hace a favor de los tribunales del domicilio del juez natural, esto es, del demandado (= *actor sequitur forum rei*)[15].

De acuerdo con el artículo 2.1 del RB/CL II o del CB/CL «las personas domiciliadas en un Estado miembro/contratante estarán sometidas, sea cual fuere su nacionalidad, a los órganos jurisdiccionales de dicho Estado». Sin perjuicio de esta disposición, el artículo 3.1 establece que estas personas podrán ser demandadas ante los tribunales de otro Estado miembro/contratante en virtud de las reglas establecidas en el RB o en el CB/CL. Dichos foros de competencia resultan aplicables, como hemos señalado, en defecto de cláusula de elección de foro a los tribunales de un Estado miembro/contratante.

Eso sí, el domicilio del demandado (en nuestro caso, el responsable del fichero de datos) se configura como una nueva forma de ataque del demandante; una solución fácil, neutra y práctica[16]. El *domicilio* constituye un concepto jurídico cuyo significado debe venir determinado por una norma legal.

En el caso de las *personas jurídicas*, dicha norma es el artículo 60.1 del RB que establece una noción autónoma de domicilio. Se considera que, en el sentido del Reglamento, las personas jurídicas están domiciliadas en aquel Estado miembro en el que tienen: a) su sede estatutaria, o b) su administración central, o c) su centro de actividad principal. Esta disposición supone un cambio respecto a la norma contemplada en los CB/CL –artículo 53– que establece que el domicilio de las personas jurídicas se determina a partir de la ley señala por la norma de Derecho internacional privado del foro –la *lex societatis*–.

---

15 Para determinar si una persona está domiciliada en un Estado o en otro, el Tribunal competente aplicará su ley interna, según señalan los artículos 59 y 60 del RB/CL II, y 52 y 53 del CB/CL.

16 *Vid.*, en relación con los motivos que favorecen el recurso al foro general del domicilio del demandado en los supuestos de responsabilidad civil producidos a través de Internet, PALAO MORENO, Guillermo, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», *op. cit.*, pp. 282-283.

En el caso de las *personas físicas*, el RB no establece una noción autónoma. Para determinar si están domiciliadas en el Estado miembro cuyos tribunales conocen del asunto, el juez aplicará su ley interna[17]. Cuando sea necesario determinar si el demandado está domiciliado en otro Estado miembro, se aplicará, según el artículo 59 del RB, la ley de dicho Estado.

Ahora bien, en la práctica, esta atribución de competencia plantea dos *dificultades principales*[18], que justifican la habitual derogación de tal foro general por medio del recurso a la autonomía de la voluntad: la falta de neutralidad de la jurisdicción resultante y la llamada genérica que el artículo 2 realiza a todos los órganos en ella integrados: a) en primer lugar, el recurso al foro general situaría al demandante en la nada cómoda situación de tener que litigar en casa de su contraparte, con lo que ello supone: desconocimiento del idioma, aumento de los costes, desconocimiento de las normas procesales aplicables, etc.; y, b) en segundo lugar, el artículo 2 nos conduce a la designación de la jurisdicción competente en términos genéricos: tribunales españoles, alemanes, suizos, belgas, etc.; y, a partir de ahí, serán las normas de reparto territorial de la organización jurisdiccional correspondiente quienes deban designar el órgano jurisdiccional concreto ante el cual plantear la reclamación.

Es más, se trata de un foro de competencia poco útil en nuestro caso por dos razones prácticas más: a) por un lado, porque en ocasiones el presunto responsable actúa desde países lejanos o exóticos, de modo que el demandante no conoce o puede no averiguar fácilmente el domicilio del demandado; y, b) por otro lado, porque es un foro de competencia poco adecuado para acciones de cesación cuando el servidor en el que se aloja la página web o la información se halla en un país distinto al país del domicilio del demandado[19].

3.4. Foro especial en materia de obligaciones extracontractuales: el *lugar donde se hubiere producido o pudiere producirse el hecho dañoso*

El artículo 5.3 del RB/CL II o del CB/CL recoge el foro de competencia especial del *lugar donde se hubiere producido o pudiere producirse el hecho dañoso*[20]. Se trata de una

17 En el caso de España, el artículo 40 del CC señala que «para el ejercicio de los derechos y el cumplimiento de las obligaciones civiles, el domicilio de las personas naturales es el lugar de su residencia habitual, y en su caso, el que determine la Ley de Enjuiciamiento Civil».

18 *Vid.* , en particular, sobre los problemas que plantea este foro en materia de comercio electrónico, CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Conflictos de leyes y conflictos de jurisdicción... op. cit*, pp. 37-41; y, DE MIGUEL ASENSIO, Pedro, *Derecho privado de Internet.* 3ª edición, *op. cit*, pp. 455-456.

19 *Vid.* CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier*, Derecho internacional privado.* vol. I, 9ª edición, Comares, Granada, 2008, pág. 783.

20 *Vid.* SUQUET CAPDEVILA, Josep, «Internet, marcas y competencia judicial internacional: ¿O la superación de la regla *forum loci delicti commissi*?. A propósito de la sentencia de la Cour

norma –manifestación del principio de proximidad– que en el mundo analógico, en los últimos tiempos, ha planteado numerosos interrogantes: p. ej., su aplicación en supuestos donde la acción causal y el resultado dañoso se presentan disociados en diversos países, o su aplicación en casos de plurilocalización del hecho dañoso; y, cuya aplicación en el mundo virtual se hace difícil, pues la duda nos embarga: ¿dónde debe considerarse que se ha producido un hecho dañoso cometido a través de Internet?

En lo que respecta a la responsabilidad civil extracontratcual en esta materia establece el artículo 5.3 del RB/CL II (y del CB/CL) que, «[...] las personas domiciliadas en un Estado miembro podrán ser demandas en otro Estado miembro [...] en materia delictual o cuasidelictual, ante el tribunal del lugar donde se hubiere producido el hecho dañoso [...]»; además, el artículo 5.3 del RB, permite la indeterminación del lugar de producción del hecho dañoso, al señalar que «[...] las personas domiciliadas en un Estado miembro podrán ser demandas en otro Estado miembro [...] en materia delictual o cuasidelictual, ante el tribunal del lugar donde se hubiere producido o pudiere producirse el hecho dañoso [...]».

Por su parte, la LOPJ señala que, en defecto de cláusula de elección de foro, cuando el demandado está domiciliado en un tercer Estado, los tribunales españoles se pueden declarar competentes de acuerdo con su apartado 3 del artículo 22 de la LOPJ. La posición jerárquicamente superior que ocupan el RB en los ordenamientos jurídicos de los Estados miembros, respecto de las normas de producción interna implica la desactivación de ciertos foros de competencia previstos en estas disposiciones. Esto ocurrirá cuando los elementos necesarios para su aplicación sean los mismos que los establecidos en los foros previstos en el RB o CB/CL[21].

El artículo 22.3 de la LOPJ ofrece una serie de foros de competencia judicial internacional en cuya virtud los Tribunales españoles pueden conocer de situaciones privadas internacionales. En la materia que nos ocupa, nos interesa el contenido de su regla VIII (= responsabilidad civil extracontractual). Así las cosas, los tribunales españoles pueden resultar competentes cuando el hecho del que derivan haya ocurrido en territorio español[22].

---

de Cassation de 9 de diciembre de 2003», en *La Ley Unión Europea*, Nº 6073, Madrid, 2004, pp. 1- 7.

21 Así, no resulta aplicable en materias incluidas en el ámbito de aplicación del RB el artículo 22.2 de la LOPJ que atribuye competencia a los tribunales españoles, cuando de demandado esté domiciliado en España o cuando las partes así lo hayan pactado tácita o expresamente, si al menos una de las partes estuviera domiciliado en un Estado miembro.

22 El artículo 22.3 otorga también la competencia a los tribunales españoles, en materia extracontractual, si «el autor del daño y la víctima tengan su residencia habitual común en España». Ahora bien, esto implica que el demandado tendrá su domicilio en un Estado miembro, por lo que se estaría dando el elemento necesario para aplicar los artículos 2 y 5 del RB, por lo que este foro previsto en el artículo 22.3 ya no resulta aplicable.

La competencia del tribunal del lugar donde se produjo el hecho dañoso (ya sea donde se haya producido el hecho generador del daño o donde se padezca el daño)[23] –*forum locus delicti commissi*– constituye la solución tradicional en esta materia. Solución que, frente a la ventaja de su sencillez, atrae sobre el apartado 3 del artículo 5 del RB/CL II, o del CB/CL todos los problemas tradicionalmente anejos a la responsabilidad extracontractual, entre otros: heterogeneidad y complejidad de supuestos, diversificación funcional del propio concepto de responsabilidad, dificultad de concreción del *forum locus delicti commissi*, y dificultades de adaptación a los ilícitos desarrollados en y a través de Internet[24].

El principal problema que plantea el *forum locus delicti commissi* es el de determinar si por país en que se produce el daño debemos entender el del lugar en el que se localiza el hecho causal (p. ej. el Estado desde el que se introduce el contenido ilícito en Internet, siendo irrelevante el lugar donde radica el servidor que aloja la *webpage*) o el del lugar en que se verifica el resultado dañoso (p. ej., el Estado desde el que se accede al contenido ilícito vertido en Internet)[25], sobre todo, en casos de disociación geográfica del ilícito (cuando el daño y el hecho generador se localizan en distintos países).

La determinación del *lugar donde se ha producido el hecho dañoso* plantea, en el mundo virtual, dos dificultades: por un lado, la determinación del lugar donde tienen lugar el evento generador del daño; y, por otro lado, la concreción del lugar del resultado lesivo. Respecto de la primera cuestión, la doctrina mayoritaria entiende que se debe ubicar dicho lugar donde se han introducido tales contenidos perjudiciales por parte del causante del daño. Y, respecto de la segunda cuestión, decir que, en tales supuestos, dicho lugar puede ser: a) el lugar desde donde se han introducido los datos; b) en el marco de Internet, el lugar donde está ubicado el servidor que los alberga; c) el lugar desde donde se puede tener acceso a los datos; o, d) el lugar donde reside el titular del derecho infringido, que es, en definitiva, donde se ha producido el hecho dañoso.

---

23 *Vid.*, en relación con la determinación del *locus delicti*, en general, REST, Alfred, «Transfrontier Environmental Damages: judicial competence and the forum delicti commissi», en *Environmental Policy and Law*, vol. 1, 1975, pp. 127-131.

24 *Vid.* PALAO MORENO, Guillermo, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», *op. cit.*, p. 288-291; y, XALABARDER PLANTADA, Raquel, «Cuestiones de derecho internacional privado: jurisdicción competente y ley aplicable», en *Derecho y nuevas tecnologías*, Editorial UOC, Barcelona, 2005, pp. 484-486.

25 El *forum locus delicti commissi* plantea algunas dificultades de adaptación cuando nos encontramos ante «delitos a distancia», ya que abre al demandante tres alternativas posibles a la hora de localizar el lugar del hecho dañoso: a) el lugar donde se hubiere cometido la acción lesiva (= lugar de acción); b) el lugar donde se hubiere sufrido el perjuicio (= lugar de resultado); o, c) optar por uno u otro. *Vid.* PALAO MORENO, Guillermo, «Competencia judicial internacional en supuestos de responsabilidad civil en Internet», *op. cit.*, pág. 287.

Lo habitual es que el hecho dañoso se produzca en el *país donde radica el fichero de datos*, aunque no tiene por qué ser siempre así[26]; ya que, el lugar donde se ha producido el hecho dañoso puede ser, efectivamente, el país o países (si se han producido transferencias de datos sucesivas, y sólo para los perjuicios causados en cada uno de esos territorios) donde se han transferido los datos (que en las transferencias de datos de España al extranjero, ese lugar será, por aplicación del artículo 2.1 de la LOPD, España), así como, el país donde se haya manifestado el daño por el tratamiento de datos realizado en ese lugar, por parte del que recibió los datos.

4. REDES SOCIALES DE INTERNET, PROTECCIÓN DE DATOS, Y DETERMINACIÓN DE LA LEY APLICABLE

La determinación de la ley aplicable en materia de tratamiento de datos de carácter personal a través de una red social de internet supone la aplicación del artículo 2.1 de la LOPD, que transpone el artículo 4 de la Directiva 95/46/CE del Parlamento 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 (en adelante, Directiva 95/46/CE)[27], y que implica alinearse en alguno de estos dos bandos: el de la liberalización de la circulación de datos automatizados, o el de la protección del derecho a la intimidad de las personas[28]. Así, mientras el artículo 4 de la Directiva 95/46/CE opta por la aplicación de la ley del lugar de residencia del responsable del fichero de datos (no es relevante el lugar de tratamiento de los datos ni la nacionalidad, domicilio o residencia habitual del sujeto cuyos datos se tratan o del sujeto responsable del tratamiento, sino que sólo es relevante el lugar de su establecimiento); el artículo 2.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo, LOPD)[29] opta por la ley del lugar de tratamiento de los datos de carácter personal[30].

La Directiva 95/46/CE opta por el criterio de la residencia del responsable del fichero en la medida en que de esta forma, « [...] 1º) Se evita la aplicación de la regla ge-

---

26 *Vid.* CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Conflictos de leyes y conflictos de jurisdicción... op. cit*, pág. 153.

27 *DOCE* núm. L 281, de 23 de noviembre de 1995.

28 *Vid.*, en el mismo sentido, *íbidem*, pp. 154-155.

29 *BOE* núm. 298, de 14 de diciembre de 1999

30 Nos encontramos ante dos preceptos que, por su contradicción, inducen a la confusión, que cubren tanto las relaciones administrativas como las relaciones entre particulares en asuntos internacionales, y que aparecen preocupadas por fijar el ámbito de aplicación de la normativa del Estado cuyos Tribunales conocen del asunto. *Vid.*, *íbidem*, pp. 156-157.

neral en materia de responsabilidad no contractual: no se aplica la *lex loci delicti commissi* o ley del país donde se produce el tratamiento ilícito de los datos [...] 2º) [Se recurre a una argumentación económica que se aleja] de la Ley del país más vinculado al supuesto [, de forma que] la proximidad del supuesto con un país no guía la mano del legislador comunitario a la hora de construir la solución de Derecho internacional privado en esta materia [favoreciendo, así, a las empresas informáticas que operan en este sector por cuatro razones:] 1º) El criterio promueve la actividad internacional de tratamiento de datos en la UE, ya que, sean cuales sean los países en los que la empresa desarrolle sus actividades, la Ley aplicable al tratamiento de datos será siempre la misma, la Ley del fichero [...] 2º) Se trata, además, de una Ley conocida por la empresa [...] 3º) Por otro lado, la empresa que trata los datos queda sometida a un mismo Derecho nacional tanto por lo que respecta a sus relaciones administrativas con las Autoridades públicas, como por lo que se refiere a las relaciones con los particulares afectados por el tratamiento de datos [...] 4º) La norma de conflicto contenida en el artículo 4 [de la] Directiva es una norma de conflicto específica, diseñada para una materia concreta. Por eso, difícilmente admite excepciones o reducciones teleológicas, desviaciones que permitan apartarse del criterio de la aplicación de la Ley de situación del responsable del fichero, lo que sería factible si la norma fuera una norma general o principal. Tampoco el artículo 4 [de la] Directiva se ve corregido por una cláusula de escape o por una cláusula de excepción [...] ».

Además, el artículo 4 de la Directiva 95/46/CE concreta el criterio de la ubicación del fichero de datos en dos supuestos especiales que, por su fisionomía, la localización del fichero de datos supone casi misión imposible: a) según el artículo 4.1.a *in fine* de la Directiva, si el responsable del fichero de datos posee distintos establecimientos en diferentes Estados de la UE, el tratamiento de datos realizado *en el marco de las actividades de cada establecimiento* se rige por la Ley del país donde radica cada establecimiento; y, b) en virtud del artículo 4.1.b de la Directiva, en el supuesto de un responsable del tratamiento establecido en un lugar que no pertenece a la UE, pero en el que se aplica la legislación nacional de un Estado miembro en virtud del Derecho internacional público, se aplicará la Directiva 95/46/CE.

Para la determinación de la ley aplicable en materia de responsabilidad civil extracontractual por vulneración del derecho a la protección de datos en el ámbito de las redes sociales de Internet se distinguen tres supuestos:

4.1. Redes sociales de Internet cuyo establecimiento se encuentra en un Estado miembro de la Unión Europea

Cuando el tratamiento de datos, a través de la red social de Internet, es llevado a cabo por un responsable situado en un Estado miembro de la Unión Europea, se aplicará la Ley de dicho Estado miembro, en virtud del artículo 4 de la Directiva 95/46/CE. Además, si el tratamiento es efectuado en territorio español en el marco de las activida-

des de un establecimiento del responsable del tratamiento, se aplicará la Ley española (= LOPD), en virtud del mencionado artículo 2.1 de la LOPD.

4.2. Redes sociales de Internet cuyo establecimiento se encuentra en un «tercer país» no comunitario

En este supuesto, y en virtud de una combinación del artículo 2 de la LOPD y del artículo 4 del Reglamento «Roma II»[31], el tratamiento de datos personales por parte de un responsable cuyo establecimiento se encuentra en un tercer Estado no comunitario se rige por las siguientes Leyes: a) la Ley elegida por las partes; b) en su defecto, se aplicará la Ley del país de residencia habitual común de las partes; c) en su defecto, se aplicará la Ley del país donde se lleve a cabo el tratamiento de datos, sea un Estado miembro o un tercer Estado (= Ley del país de comisión del hecho dañoso); y, d) no obstante, si del conjunto de circunstancias se desprende que el hecho dañoso presenta vínculos manifiestamente más estrechos con otro país distinto, se aplicará la Ley de ese otro país[32]. Ahora bien, si el hecho dañoso se produce en varios países, entonces el perjudicado deberá reclamar con arreglo a cada una de las Leyes de los países en los que su derecho ha sido vulnerado y por los daños allí sufridos.

Las principales redes sociales de Internet abogan por la autonomía de la voluntad (= Ley elegida por las partes): así, de la lectura de sus Condiciones de uso se deduce: en el caso de **Facebook**, que: « [...] Al visitar o hacer uso del Sitio o el Servicio, aceptas que las **leyes del estado de Delaware**, sin tener en cuenta los principios del conflicto de leyes, regularán estas condiciones de uso así como cualquier disputa que pudiera surgir entre tú y la Compañía o con alguno de nuestros afiliados. Respecto a toda disputa o queja no sujeta a arbitraje (tal y como se indica abajo), estás de acuerdo en no emprender ninguna acción fuera del estado y de los tribunales federales de California, y con esto das el consentimiento, y prescindes de toda defensa de carencia de jurisdicción personal o de foro de no conveniencia respecto a esto, lugar de reunión y órgano jurisdiccional del estado y tribunales federales de California [...]»; que en el caso de **LinkedIn** las partes acuerdan que « [...] Este Contrato y cualquier conflicto con LinkedIn o sus sociedades relacionadas en virtud de este Contrato o de LinkedIn (los «Conflictos») se regirán por la **legislación vigente en California**, sin hacer referencia a disposiciones relativas al principio de conflicto de leyes y excluyendo las disposiciones de la CNUCCIM-CISG [...]»; o, que os usuarios de **MySpace** saben que « [...] El Acuerdo se regirá e interpretará de

31 Reglamento (CE) Nº 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la ley aplicable a las obligaciones extracontractuales («Roma II»), *DO* L 199/40, de 31/07/2007.

32 *Vid.* CALVO CARAVACA, Alfonso-Luis y CARRASCOSA GONZÁLEZ, Javier, *Derecho internacional privado.* vol. I, 9ª edición, Comares, Granada, 2008, pág. 796.

acuerdo con las **leyes del Estado de Nueva York**, sin tener en cuenta sus disposiciones sobre conflictos de leyes [...])».

4.3. Redes sociales de Internet cuyo establecimiento se encuentra en un «tercer país» no comunitario pero se utilizan medios situados en España

Finalmente, es de reseñar el siguiente supuesto: cuando el responsable del tratamiento de datos no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos, *medios* situados en territorio español (= ordenadores personales, terminales, cámaras de televisión, *cookies*, etc.), salvo que tales medios se utilicen únicamente con fines de tránsito (= artículo 4.1.c de la Directiva 95/46/CE)[33]. Se halla ampliamente extendido el criterio de que esas normas imponen la aplicación del régimen comunitario de protección de datos personales en los diversos supuestos en los que sitios *web* cuyos responsables no estén establecidos en la Unión Europea emplean dispositivos para la recogida activa de datos procedentes de los ordenadores de los usuarios situados en Estados miembros con el objetivo de su tratamiento futuro. En los supuestos en los que el sitio *web* se limita a obtener datos personales mediante formularios en los que los usuarios facilitan cierta información, resulta más controvertido en qué medida ello implica utilizar medios situados en el territorio de un Estado miembro, si bien tiende a afirmarse que no es determinante que ahí se encuentre el ordenador desde el que el usuario accede al servicio sino que desde el punto de vista técnico más relevante sería dónde se ubica el servidor en el que se aloja el correspondiente sitio *web*.

Una interpretación amplia del ámbito de aplicación de la Directiva 95/46/CE ha sido objeto de críticas, en la medida en que puede conducir en la práctica a extender la aplicación de la normativa española (= la LOPD) y, por ende, de la europea (=Directiva 95/46/CE) y, por supuesto, la competencia de las correspondientes autoridades de protección, a un número extraordinario de entidades de todo el mundo (en nuestro caso, redes sociales de Internet), incluso respecto de supuestos en los que la captación de datos en la Unión Europea puede ser no sólo ocasional sino incluso accidental. Por lo tanto, el criterio de que la actividad vaya dirigida a un determinado territorio resultaría también determinante en este entorno, lo que contribuiría a excluir de la exigencia de cumplir con la legislación europea (Directiva 95/46/CE), entre otros, a sitios *web* cuya captación de datos en la Unión Europea sea meramente accidental.

33 Nada dispone la Directiva 95/46/CE sobre la Ley aplicable al tratamiento de datos personales realizado en territorio de terceros Estados sin intervención de medios técnicos en Estados de la Unión Europea. Ello explica que la Directiva 95/46/CE someta a un régimen muy estricto la circulación de datos personales desde la Unión Europea con destino a terceros países. *Vid. íbidem*, pág. 795.

5. REFLEXIONES FINALES

Un buen día abres tu correo, y te encuentras algo nuevo: una invitación para unirte a ***Facebook***, ***MySpace*** o ***Tuenti***. Has oído hablar de ello, parece que la gente se divierte, queda con los colegas, se reencuentra con antiguos amigos... Es por la mañana, no estás para leerte las Condiciones de uso (de las cuales en el momento de ingresar sólo aparece un pequeño fragmento, por cierto), aceptas sin miramientos y ya eres uno más. Cuando quieres acordarte, te dejas llevar por la emoción de saber más y más sobre otros usuarios, porque *éste era vecino mío*, porque *mira mi ex ahora con quién se junta*, porque *si mi madre viera estas fotos, se caía redonda*, etc. No hay control. Quiere haberlo, es cierto, pero no lo hay, el tema de la privacidad está cogido con pinzas de papel, y no se puede hacer mucho para luchar contra ello, salvo informar y formar a los usuarios de las redes sociales de los problemas que acarrea el exponer su intimidad a los cuatro vientos.

Confiemos en que las iniciativas legislativas en curso y las numerosas recomendaciones, guías de uso y códigos de conducta promovidas, hoy día, tanto a iniciativa pública como privada nos permitan minimizar los riesgos legales que su uso ilegítimo o inadecuado puede llevar aparejado ya que, en última instancia, como usuarios, somos responsables de nuestros datos... Cuando eres pequeño, te enseñan que si un niño te pregunta ¿quieres ser mi amigo? debes decir que sí. Con las redes sociales de Internet nos ocurre lo mismo, nos cuesta decir que no a alguien que nos invita. Sin embargo, nuestros padres también nos advirtieron otra cosa: *no hables con extraños*…

6. BIBLIOGRAFÍA

Bing, J. (1999). «*Data protection, jurisdiction and the choice of law* ». En *Privacy Law & Policy. Reporter*, volume 6, pp. 92-98.

Calvo Caravaca, Alfonso-Luis y Carrascosa González, Javier (2007). *Derecho internacional privado. Vol. II*, 8ª edición. Granada: Comares.

Calvo Caravaca, Alfonso-Luis y Carrascosa González, Javier (2001). *Conflictos de leyes y conflictos de jurisdicción en Internet*, Madrid: Colex.

Campuzano, Herminia (2000). *Vida privada y datos personales.* Madrid: Tecnos.

De Miguel Asensio, Pedro (2002). *Derecho privado de Internet.* 3ª edición, Madrid. Civitas.

Fernández Burgueño, Pablo (2009). «El peligro de las redes sociales y sus principales consecuencias jurídicas»: En *Revista Economist & Jurist*, nº 131.

Llaneza González, Paloma (2003). *Aplicación práctica de la LSSI-CE*. Barcelona: Bosch.

Monsoriu Flor, Mar (2008). *Manual de Redes Sociales en Internet*. Madrid: Creaciones Copyright.

Ortega Giménez, Alfonso. «Derecho Internacional Privado, Protección de Datos y Redes Sociales de Internet» (Capítulo XI). En Rallo Lombarte, Artemi y Martinez Martinez, Ricard (Coords.) (2010). *Derecho y Redes Sociales*, Cizur Menor (Navarra): Civitas Thomson Reuters, pp. 299-318.

Palao Moreno, Guillermo (2006). «Competencia judicial internacional en supuestos de responsabilidad civil en Internet». En Plaza Penadés, Javier, *Cuestiones actuales de derecho y Tecnologías de la Información y Comunicación (TICs)*. Cizur Menor (Navarra). Editorial Aranzadi.

Rest, Alfred (1975). «Transfrontier Environmental Damages: judicial competence and the forum delicti commissi», en *Environmental Policy and Law*, vol. 1, pp. 127-131.

Suquet Capdevila, Josep (2004). «Internet, marcas y competencia judicial internacional: ¿O la superación de la regla *forum loci delicti commissi*?. A propósito de la sentencia de la Cour de Cassation de 9 de diciembre de 2003»: En *La Ley Unión Europea*, Nº 6073, Madrid.

Xalabarder Plantada, Raquel (2005). «Cuestiones de derecho internacional privado: jurisdicción competente y ley aplicable». En AA.VV. *Derecho y nuevas tecnologías*, Barcelona: Editorial UOC.

LA PROTECCIÓN DE LA IDENTIDAD PERSONAL FRENTE A AFIRMACIONES INCIERTAS EN LA RED

María Dolores Palacios González
Profesora Titular de Derecho civil de la Universidad de Oviedo

RESUMEN: La revolución digital está transformando los comportamientos humanos y generando nuevos problemas de convivencia. Además, otros ya existentes adquieren mayor dimensión porque antes solo se presentaban fuera de la red, con mucha menor difusión y trascendencia social. Uno de esos «problemas» que, más que surgir, se acrecienta en Internet, es el que se produce cuando se imputan falsamente hechos a una persona o se ponen en su boca manifestaciones que no ha vertido. En las líneas que siguen se analiza si puede defenderse la existencia de un «derecho» a la identidad personal entendida como el modo de ser y de actuar propio de cada sujeto. Desde una perspectiva constitucional se trataría de revisar la vinculación del interés de cada persona a que sus pensamientos, ideas y modo de vida no sean tergiversados, con derechos como el honor o, más en general, con la dignidad humana. Además, se reflexiona sobre las posibilidades legales que ofrece el Derecho europeo y español para la defensa frente a esas conductas analizando, en concreto, si pueden tener alguna relación con los derechos de propiedad intelectual y en qué medida pueden ser aplicables el derecho de rectificación, la normativa de protección del honor, de protección de datos o, más en general, si cabrá exigir responsabilidad extracontractual sobre la base del artículo 1902 del Código civil, en su caso en relación con los artículos 16 y siguientes de la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico.

PALABRAS CLAVE: Identidad. Propiedad intelectual. Honor. Imagen. Protección de datos. Derecho de rectificación. Derecho al olvido. Responsabilidad extracontractual.

1. INTRODUCCIÓN

En un artículo de opinión publicado en el diario español El País el 23 de octubre de 2012, el novelista y escritor Mario Vargas Llosa llamaba la atención acerca de la incidencia de la revolución tecnológica a su modo de ver, no jurídico, en dos «derechos» diferentes como son el derecho a la identidad y el derecho de propiedad intelectual. Se refería el articulista a otro escritor, en este caso el norteamericano Philip Roth, que a su vez envió una carta abierta a Wikipedia por medio del The New Yorker el 7 de septiembre del mismo año. Al parecer Roth se había dirigido al administrador de Wikipedia con la pretensión de que se modificara información errónea publicada en la wiki sobre quién era la persona que había inspirado su novela The Human Satín. Desde Wikipedia se le contestó que pese a reconocerle «una indiscutible autoridad sobre su propia obra» no bastaba con su palabra sino que eran necesarias «otras fuentes secundarias». A esta

anécdota se suman en el artículo otras en las que el protagonista es ahora el propio Vargas Llosa al que en Internet se le atribuye la autoría de dos textos que nunca ha escrito realmente, uno al parecer bastante o muy malo y el otro malintencionado. Seguramente si indagamos podremos encontrar casos similares como el de otro escritor, Jose Luis Sampedro, que tuvo que desmentir públicamente ser autor de un artículo publicado en una página web insultando al presidente del gobierno español y a sus ministros.

Pese a que en su artículo Vargas Llosa parece que se resigna a tener que soportar, al menos de momento, lo que ya hemos dicho que valora como atentado a la identidad personal, desde aquí vamos a tratar de examinar, desde un punto de vista jurídico y sobre la base de nuestro Derecho –europeo y español– la problemática que se presenta y las posibles soluciones.

2. EL CONCEPTO DE IDENTIDAD Y SU DESFIGURACIÓN EN LA RED

Generalmente cuando se alude al «derecho a la identidad» desde una perspectiva jurídico-privada, aunque se encuentre implícita una concepción amplia como derecho a la propia individualidad, suelen tratarse aspectos más concretos como el derecho al nombre, al cambio de nombre y sexo como problema específico dentro de la transexualidad, al derecho a la propia imagen como derecho a que la misma no sea reproducida ni comunicada sin el consentimiento del titular, el derecho a la protección de los datos personales o incluso la problemática que presenta la utilización de los avances genéticos como en el caso de la clonación.

En nuestro país encontramos pocas referencias concretas a este «derecho», desde una perspectiva en la que se quiera hacer referencia al derecho a ser uno mismo. En algunos países latinoamericanos como Argentina o Perú, por el contrario, en mayor o menor medida sí se ha construido la categoría dogmática de derecho a la identidad. En Perú incluso se reconoce en el artículo 2 de la Constitución. El autor de esta nacionalidad Fernández Sessarego, C., partiendo de la consideración de la identidad como el conjunto de características de la personalidad de cada cual que permite conocer a la persona en lo que ella es en cuanto específico ser humano, la define como el derecho de los sujetos a ser fielmente representados en su proyección social de acuerdo con el bagaje ideológico cultural que ha construido con sus pensamientos, opiniones, creencias y comportamientos[1].

También en Derecho italiano se ha abordado la construcción de un Derecho a la identidad como derecho específico, sobre la base de la práctica jurisprudencial y, concretamente, de distintas resoluciones de las Cortes de casación y constitucional. Posteriormente este «*interés de toda persona a no ver tergiversado o alterado externamente su propio patrimonio intelectual, político, social, religioso, profesional a causa de la atribución de ideas, opiniones o comportamientos diferentes de los que el interesado considere propios y*

1 Fernández Sessarego, C. (1992). *Derecho a la identidad personal*, Buenos Aires, pp. 113 ss.

*haya manifestado en su vida de relació*n», como ha sido definido por la doctrina italiana[2], ha sido también objeto de tratamiento por esta última.

El derecho a la identidad ha sido reconocido en la sentencia de la Corte Suprema de 22 de junio de 1985, en el «caso Veronesi»[3]. Se trataba de un oncólogo cuyas palabras, efectivamente pronunciadas en una entrevista, fueron utilizadas por una empresa que fabricaba cigarrillos para publicitar sus productos. Si bien la cuestión se planteó inicialmente desde la perspectiva del derecho al nombre, la Corte de Casación elabora una definición del derecho a la identidad personal y articula tanto el fundamento normativo como la relación con otros derechos de la personalidad de tal manera que se puede concluir la existencia de un derecho subjetivo específico[4]. Concluye la sentencia que el derecho tutela «*l'interesse di essere representato, nella vida di relazione, con la sua vera identità, così come questa nella relata sociale, generale o particolare, è conosciuta o poteva essere riconosciuta con l'esplicazione dei criteri della normale diligenza e della buona fede oggetiva*»; en otras palabras de la misma resolución, derecho «*a non vedersi all'esterno alterato, travisto, offuscato, contestato il propirio patrimonio intellettuale, político, sociale, religioso, ideológico, professionale, ecc. quale si era estrinsecato od appariva, in base a circostanze concrete ed univoche, destinato ad estrinsecarsi nell'ambiente sociale*». Asimismo la sentencia diferencia los derechos al nombre y a la imagen del derecho a la identidad al entender que a diferencia de los primeros este último representa una fórmula sintética para distinguir al sujeto desde un punto de vista global en sus múltiples y específicas característica y manifestaciones (morales, sociales, políticas, intelectuales, profesionales, etc.), expresando la concreta y efectiva personalidad individual que el sujeto ha consolidado. Posteriormente, como veremos al tratar de la perspectiva constitucional del derecho, la Corte Costituzionale ha confirmado este reconocimiento sobre la base del artítulo 2 de la Carta Magna.

Siguiendo a Pino puede verse también cuál es el tratamiento del derecho a la identidad en otros ordenamientos. Concretamente en su exposición se refiere a la situación en su país, Italia, de la que ya hemos hablado, en Alemania, Francia y Estados Unidos[5].

---

2 Pino, G.(2006). Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali. En *Libera circolazione e protezione dei dati personali*, a cura di Panetta. Giuffrè. Milano, t. 1, pp. 257 a 321.

3 Cass. 22.6.1985, n. 3769, FI, 1985, I, 2211.

4 Pino, G., cit. Vid. también, Raffiota, E.C., Appunti in materia di diritto all'identità personale, enero de 2010, www. forumcostituzionale.it (fecha de consulta febrero de 2013).

5 También Farré López, al reflexionar sobre la naturaleza jurídica del derecho de rectificación en los distintos ordenamientos, y dado que, como se verá, existe una consideración bastante generalizada de su virtualidad para tutelar la identidad, analiza el reconocimiento del derecho a la identidad en esos mismos ordenamientos (2008). *El Derecho de rectificación. Un instrumento de defensa frente al poder de los medios*, Madrid, pp. 31 ss.

Al parecer la jurisprudencia alemana ha individualizado un *Recht auf Identität*, vinculado al derecho general de la personalidad, que sería violado cuando se atribuyan a un sujeto opiniones que ofrecen una imagen que no se corresponde con la realidad[6]. Esta posibilidad de reconducir derechos sin reconocimiento legal a la fórmula general del derecho de la personalidad ha permitido que en Alemania la identidad haya adquirido dimensiones específicas que van más allá de la identidad personal: identidad política, identidad sexual, respeto a la identidad cultural de los sujetos pertenecientes a minorías o a la identidad del grupo. También se ha hablado del derecho a la correcta representación de la propia imagen existencial (*Lebensbild*) y del derecho a la libre autodeterminación informativa (*Recht auf informationelle Selbstimmung*). El primero ha permitido considerar ilícito que en una novela en la que al protagonista, en principio un personaje ficticio, era perfectamente reconocible, se le atribuyera ideología nazi[7]. El derecho a la identidad se contraponía en este caso con el derecho a la libertad artística.

En el Derecho francés lo que aquí estamos llamando derecho a la identidad ha sido tutelado por la jurisprudencia como derecho a la autenticidad distinguiendo según que la presentación pública de la personalidad de un sujeto sea consecuencia o no de una relación contractual u otra forma de acuerdo. En el primer caso, cuyo ejemplo paradigmático es la entrevista, la jurisprudencia ha establecido una serie de criterios que han de ser respetados: así, nos dice Pino siguiendo a Bessone[8], el entrevistador puede usar libremente el material de la entrevista según su estilo, el entrevistado no puede revocar su consentimiento sin perjuicio de la posibilidad de subordinarlo a la revisión del texto definitivo y, por último, el entrevistador está obligado a no desnaturalizar la presentación que el entrevistado haya hecho en relación con su personalidad y sus opiniones. Tanto en estos supuestos como en los que no exista tal acuerdo, más difíciles de valorar, en el orden civil se ha acudido a la responsabilidad contractual o extracontractual, según los casos, así como al derecho de rectificación y al derecho de respuesta tal y como vienen configurados en el Derecho francés. También en algún caso se ha acudido a la protección de los datos personales para evitar que su tratamiento dé lugar a una manipulación de la identidad.

De acuerdo con lo expuesto por Prosser y Keeton[9], en derecho norteamericano el *tort de false light* entra en juego cuando se difunde una representación de un sujeto que genera error en una persona media, teniendo en cuenta las circunstancias del caso

---

6 Cfr. Pino, G. cit.

7 Caso Mephisto, BverfG, 24 febbraio 1971, *k in BVerfGE*, vol.30, 1971, pp.173 ss.

8 Pino, G., cit. Bessone (1973). Diritto soggetivvo e «droits de la personnalité». A propósito di un recente saggi. *Riv.trim.dir.proc.civ.*, pp. 1175-1199 y (1974) Principio della tradiciones e nuove direttive in tema di diritto all'immagine. *Foro it.*, IV, cc. 182-184.

9 Prosser W.L - Keeton W.P. (1984). *On the Law of Torts*, West Publishing, Sr Paul, II ed., recogido por Pino, G., cit.

concreto, lo que puede darse bien por la recreación ficticia de un personaje real tanto con finalidad artística como un contexto informativo en sentido amplio o por apropiación comercial del nombre o la imagen de una persona sin su consentimiento. Ahora bien, aun cuando la falsa representación puede no ser difamatoria, la Corte suprema ha extendido a casi todas sus decisiones la disciplina de la *Law of defamation*, con el fin de restringir la tutela e impedir que por vía judicial se vea afectado el *marketplace of ideas*.

De manera similar en Derecho inglés, en el que no está reconocido un derecho de réplica, la tutela en este ámbito y al margen de los mecanismos de autolimitación de los medios se constriñe a los procesos por libelo sobre la base del *Defamation Law*.

Por lo que se refiere al Derecho español es defendible que dentro del ámbito de los derechos de la personalidad atinentes a la integridad moral de la persona pueda distinguirse el derecho a la identidad desde la perspectiva que aquí le estamos dando y que, aun siendo evidente la interrelación, es un derecho distinto a los derechos al nombre, al honor, a la intimidad o a la propia imagen. También es distinto del llamado derecho al olvido, entendido como el derecho a que se eliminen y/o dejen de difundirse los datos o manifestaciones del interesado que este no quiera mantener públicos y que actualmente se articula desde la perspectiva del derecho a la protección de datos.

El conflicto sobre el que aquí pretende llamarse la atención es, precisamente, el de la desfiguración y tergiversación de la identidad, en sentido amplio, en general en esa proyección social del sujeto, pero en particular, porque ahí es realmente donde se está generando el problema, en su plasmación en la red. Esta es la que permite no solo la deformación, que también puede darse por otros medios de comunicación social, sino, sobre todo, la más amplia difusión, a nivel incluso mundial, de dicha desfiguración.

Además, Internet amplía el campo de posibles actuaciones lesivas. Mientras en el entorno no digital el mayor peligro de lesión de determinados derechos de la personalidad, incluyendo la identidad si lo admitimos como tal, proviene de los medios de comunicación, la red permite que las actuaciones de cualquier persona, en cualquier momento –y hay millones de usuarios activos cada día «subiendo» información visible– tenga a veces incluso la misma potencialidad dañina que los medios (piénsese, por ejemplo, en la página de un bloguero muy visitado). El gran avance que supone que cualquier persona pueda tener su página web o su blog o entrar a hacer comentarios en las de otras, incluidas las de los medios digitales, implica en contrapartida el gran riesgo de la multiplicación sin límites de conductas potencial o efectivamente lesivas.

3. LA PERSPECTIVA CONSTITUCIONAL

Ciñéndonos al Derecho europeo y pese a que, al igual que ocurre en nuestro ordenamiento, la Constitución italiana no recoge un específico derecho a la identidad, se ha afirmado que se trata de un derecho con relevancia constitucional, consecuencia tanto

de su interrelación con el pleno desarrollo de la personalidad individual como con el derecho de participación en la organización política y social del país. Aunque para algunos autores resultaría adecuado reconducir la garantía constitucional del Derecho a la libertad de «manifestaciones del pensamiento» desde la perspectiva negativa del derecho a no manifestar ideas u opiniones y a ver reconocida la paternidad solo de sus propias ideas y opiniones[10], la Corte Costituzionale, en la sentencia de 3 de febrero de 1994[11], reconoce y garantiza, sobre la base del artículo 2 de la Constitución, un derecho a la identidad personal, a ser uno mismo, como respeto de la imagen en la vida social con las ideas, la experiencia, las convicciones ideológicas, religiosas, morales y sociales que diferencian y califican al individuo. En este sentido se manifiesta también la sentencia de casación de 7 de febrero de 1996[12]. De acuerdo con ello para la doctrina italiana el derecho de rectificación es un derecho subjetivo privado que protege la proyección pública de la personalidad, facultando al individuo para exigir que la representación de su persona en los medios de comunicación sea «fiel, correcta y completa» protegiendo al individuo tanto de lesiones que puedan producirse en el honor o la intimidad como las que se generan cuando un medio de comunicación atribuye afirmaciones que al no ser ciertas o ser incorrectas pueden falsear la imagen o la reputación social del sujeto[13].

Esa posibilidad de individualizar un derecho autónomo a la identidad no tiene plasmación en nuestro texto constitucional, si bien podría plantearse su inclusión tanto en la dignidad de la persona como en el derecho al libre desarrollo de la personalidad. En nuestro ordenamiento, a día de hoy, no existe una tutela constitucional autónoma del derecho a la identidad. En su caso, la tutela deberá de canalizarse, si es posible, a través de otros derechos fundamentales que también puedan verse lesionados.

4. LA PERSPECTIVA LEGAL

4.1. La protección desde la perspectiva de la propiedad intelectual

Desde los orígenes de la protección de la propiedad intelectual el centro de actuación siempre ha sido la defensa de los derechos del autor sobre su obra. Esta protección se ha basado bien en los derechos puramente patrimoniales o de explotación, desde la perspectiva del copyright o, de manera más amplia, en el derecho europeo continental, teniendo también en cuenta los llamados derechos morales. Entre estos últimos se encuentra el derecho a la paternidad de la obra o a exigir el reconocimiento de la condición de autor, en el

10 Cfr. Pino, G., cit.

11 Corte Costituzionale, n.13, *FI*, 1994, I, 1668.

12 Cass. Civ. Sez. I, 7.2.1996, n.978, *Dinf*, 1997, 116.

13 Farré López, P., cit., p.181.

que a su vez se integra el derecho a no revelar la autoría bien divulgando la obra mediante seudónimo o signo o bien, directamente, de manera anónima. Pero a lo que no se hace referencia ni legal, ni judicial, ni doctrinalmente es a la facultad de evitar que a una persona se le atribuya, falsamente, la condición de autor de una obra determinada.

Un pretendido derecho –o más bien «facultad»– en este sentido, no parece que pueda configurarse como una vertiente de los derechos de autor y concretamente del derecho a la paternidad porque faltaría el presupuesto básico para el nacimiento de derechos de propiedad intelectual: la creación por un autor de una obra original. Aquí hay creación de una obra por alguien, por un lado, y un pretendido, pero no cierto, «autor», por otro, de tal manera que no confluyen creación del autor y obra.

La otra imputación falsa o –siendo benevolentes– errónea a la que nos hemos referido, esto es, que se afirme que el hecho o la persona que han inspirado una obra es uno determinado cuando el autor lo desmiente categóricamente, tampoco parece que pueda constituir un comportamiento que pueda considerarse como infracción de los derechos del autor sobre su obra. Ni afecta a la paternidad de la obra ni supone un atentado contra su integridad porque la obra en sí no ha sido deformada, modificada ni alterada. Lo que ha sido deformado o alterado es la idea que terceros puedan hacerse de la obra respecto de la idea que de la misma tiene el propio autor, lo que por razones obvias no puede ser objeto de protección desde la perspectiva de la propiedad intelectual.

4.2. El derecho al honor y a la propia imagen

Ciertamente, conductas como las descritas más arriba pudieran constituir una intromisión ilegítima en el honor de la persona, cuando la hagan desmerecer en la consideración propia o ajena. En estos casos podría acudirse a la tutela civil específica –sin perjuicio de la penal si es el caso– que otorga la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del honor, la intimidad personal y familiar y la propia imagen y que incluye tanto la acción indemnizatoria, que abarca los daños morales, como la posibilidad de exigir la publicación total o parcial de la sentencia condenatoria y la adopción de medidas para prevenir intromisiones inminentes o ulteriores. Pero el atentado contra la identidad, tal y como la hemos venido configurando, no implica necesariamente esta lesión, consecuencia de que se trataría de una derivación de la dignidad de la persona autónoma e independiente del honor de la misma.

Tampoco es protegible mediante la tutela de la imagen ya que aunque el derecho a la misma no se agota en la figura humana, sino que abarca cualquier manifestación que permita su recognoscibilidad, no va más allá.

4.3. El derecho a la protección de datos

También es posible que actuaciones como las que aquí nos ocupan puedan ser calificadas de vulneración a la protección de los datos personales. El derecho a la protección

de nuestros datos ha sido deslindado por el Tribunal Constitucional de otros derechos con los que tiene indudablemente relación, como es el caso del derecho a la intimidad, reconociéndole así un carácter autónomo en el ámbito de la red, la llamada «libertad informática» (STS 292/2000). Si efectivamente se considera que el tratamiento de datos ajenos sin consentimiento del titular, en la modalidad que sea, constituye una violación de los datos personales, aquel podrá ejercitar sus derechos, según los casos, ante la Agencia Española de Protección de Datos o, en caso de una pretensión indemnizatoria, ante la jurisdicción ordinaria (art. 19 de la Ley Orgánica 15/1999 de Protección de datos de carácter personal).

El problema que aquí se nos plantea tiene que ver en muchas ocasiones con el derecho a la autodeterminación informativa que está detrás de la protección de datos. En este sentido el D. Legs. N 196/2003 italiano (Codice della Privacy) afirma en su art. 2., comma 1, que el tratamiento de los datos se desenvuelve «en el pleno respeto de los derechos, de las libertades fundamentales, no solo de la dignidad de la persona, con especial referencia a la reserva, a la identidad personal y al derecho a la protección de los datos personales».

4.4. La responsabilidad extracontractual

Si hay en los ordenamientos y concretamente en el español una cláusula general de gran amplitud y eficacia para defender los derechos de las personas de los perjuicios que puedan ocasionarles las actuaciones de otras, al margen de las relaciones contractuales, es la que prevé la obligación de reparar el daño que se causa a quien no tiene obligación de soportarlo. Y es indudable que las conductas a que aquí nos estamos refiriendo son susceptible de generar un daño, que podría calificarse de patrimonial según los casos, moral o de ambos tipos. Si efectivamente se determina la existencia de un daño antijurídico la responsabilidad será exigible entonces al autor del daño por la vía del artículo 1902 CC siempre y cuando se den todos los requisitos legales de acuerdo con la aplicación actual del precepto. En cuanto a la reparación del daño, no tiene por qué ceñirse necesariamente a una indemnización compensatoria sino que, por el contrario, puede también exigirse la reparación «in natura» que en estos casos podría consistir, por ejemplo, en el contenido del derecho de rectificación o la cesación de la conducta.

4.5. El derecho de rectificación

Podríamos plantearnos también si el derecho de rectificación recogido en la Ley Orgánica 2/1984 podría servir en algún caso para defender los bienes jurídicos de los que aquí se está hablando. Como derecho a que los medios de comunicación social que hayan difundido información errónea, inexacta e incluso falsa, se vean obligados a difundir igualmente aquellas apreciaciones que el afectado por las mismas considere necesarias para clarificar la cuestión, se nos aparece como un medio adecuado para tutelar derechos entre

los que se ha incluido la identidad. Señala Farré que ya desde hace tiempo tanto la jurisprudencia alemana como la italiana han atribuido al derecho de rectificación la tutela del derecho a mostrarse ante los demás de un determinado modo, señalando el Tribunal Constitucional alemán que el derecho de rectificación protege la autodeterminación de las personas en cuanto manifestación de su derecho a decidir de qué manera quieren ser públicamente presentadas frente a terceros y frente a la opinión pública[14].

En España tanto la jurisprudencia constitucional como la doctrina, sobre la base de la misma, configuran el derecho de rectificación tanto como un derecho subjetivo de defensa y garantía de los derechos e intereses del rectificante como un complemento a la garantía de la opinión pública libre[15]. Ahora bien, respecto de la tutela de los derechos de la persona, se considera como un derecho instrumental en relación con esos otros derechos, fundamentalmente el honor[16]. Sin perjuicio de ello y aun cuando el Tribunal Constitucional no se haya manifestado nunca a favor de su consideración como instrumento protector de la identidad, no parece que exista ningún obstáculo relevante[17]. De hecho, de la configuración del derecho que hace el artículo 1.1 de la Ley Orgánica reguladora del derecho de rectificación cuando establece que «toda persona, natural o jurídica, tiene derecho a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicios» se desprende que dichos perjuicios pueden ser consecuencia de la lesión de cualquier derecho o bien jurídico y no solo del honor.

En todo caso un obstáculo que podría aparecer en algún supuesto de protección de la identidad es que en la mayoría de los ordenamientos, incluido el nuestro, y a excepción de alguno como el francés, el derecho de rectificación solo puede ejercitarse en relación con hechos y no frente a opiniones y juicios de valor[18].

5. LA VULNERACIÓN A TRAVÉS DE LA RED

La problemática que plantea el atentado contra la identidad no es, como casi nunca ocurre, específica de Internet. Pero también como casi siempre, lo que la red aporta es una agravación de la misma cuando no derivaciones autónomas consecuencia de la di-

14 Farré López, P., cit., p. 88.

15 Vid. STC 168/1986.

16 Cfr. Farré López, P. cit., p. 296.

17 Farré lo fundamenta en el modo amplio en que la jurisprudencia constitucional define el contenido al honor (cit., p.296).

18 Pensemos, por ejemplo, en el problema que plantearía una afirmación de que una persona es «de izquierdas» o «de derechas» no basada en la afiliación a ninguna fuerza política.

fusión que se genera. Así, por ejemplo, en materia de protección de datos ya no se trata solo de que la publicación de datos personales en la red pueda producir un mayor daño que si se realiza fuera del ámbito digital, sino que hay ocasiones en que es precisamente la publicidad indiscriminada que se origina con la visibilidad que da Internet la que convierte en ilícita una conducta inicialmente lícita. La cuestión que se plantea, por tanto, ya no es únicamente la necesidad de evitar la conducta atentatoria contra la identidad sino también y sobre todo, la difusión a través de la red. Además, en el ámbito de la responsabilidad se plantea la posibilidad de imputar objetiva y subjetivamente a los prestadores de servicios de la sociedad de la información, incluidos los prestadores de servicios de intermediación, en aras a que tengan que hacer frente a una eventual reparación del daño causado. Y ello nos lleva al régimen de responsabilidad recogido en la Ley de Servicios de la Sociedad de la Información, que remite en general a la normativa civil, penal y administrativa (art. 13) y a la exoneración de responsabilidad prevista en los artículos 14 a 17 que, sin embargo permite examinar, de acuerdo con la normativa aplicable para la cada caso concreto, la de los prestadores de servicios de intermediación –incluidos los que prestan servicios de alojamiento o la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet– cuando pueda probarse que han tenido conocimiento efectivo de que la actividad o la información almacenada o a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización y pese a ello no han actuado con diligencia para retirar los datos o hacer imposible el acceso a ellos o, en su caso suprimir o inutilizar el enlace correspondiente. Si es así, podrán adoptarse contra ellos las medidas previstas por la legislación aplicable (legislación de protección del honor o la intimidad, de propiedad intelectual, de protección de datos, etc.) y, en su caso, exigirles la reparación del daño causado con el fundamento de la responsabilidad extracontractual del artículo 1902 o con cualquier otro previsto por la normativa especial. Y esto es muy importante porque en muchos casos no basta con ejercitar la acción contra el proveedor de los contenidos que se reputan ilícitos. Es fácil que no se pueda saber quién es o incluso que el sitio web en el que inicialmente fueron «colgados» haya desaparecido. Para la efectividad de la tutela de los derechos será entonces necesario ejercitar las acciones que correspondan contra la web, blog o wiki en que se encuentran los enlaces o incluso frente a los buscadores que por medio de la indexación hacen posible la difusión de los contenidos a nivel mundial.

En todo caso en muchas ocasiones vamos a encontrarnos con los problemas que plantean las excepciones de falta de legitimación pasiva, de competencia judicial y de inaplicación del derecho europeo, en las que aquí no podemos entrar, y que son consecuencia del carácter global e inmaterial de la red.

Por lo que se refiere al derecho de rectificación hemos visto que por su naturaleza puede resultar útil para la defensa de la identidad frente a los riesgos de Internet. No obstante, la protección que ofrece en la mayoría de los ordenamientos encuentra el

obstáculo de que, como límite a la libertad de prensa e información, es ejercitable frente a los medios de comunicación social y, además, es necesario que el medio ostente el control de la información que se pretende rectificar como se desprende del hecho de que en España la ley reguladora del derecho de rectificación legitime pasivamente al director del medio. Si bien es cierto que en Alemania está previsto expresamente en el Convenio estatal de los Länder denominado *Mediendienste-Staatsvertrag* (1997), que el derecho se ejerza frente a algunos servicios *online*, el supuesto parece limitarse a los proveedores de servicios de medios de comunicación que oferten textos o impresos reproducidos de forma periódica, a quienes obliga a difundir inmediata y gratuitamente una rectificación de la persona afectada por una afirmación de hechos integrada en sus contenidos[19]. Dado que estos servicios permiten que la información aparezca durante un periodo de tiempo, la rectificación podrá ser emitida durante tanto tiempo como se ha ofrecido la afirmación rectificada, pero teniendo en cuenta la fugacidad de los contenidos en la red también es posible que el derecho se ejerza incluso si la afirmación ha desaparecido, en cuyo caso el afectado podrá exigir la publicación de la rectificación durante un plazo que no exceda de un mes y en un lugar equiparable a aquel en el que se ofreció la información controvertida[20].

Como ha ocurrido con tantas cuestiones Internet ha dejado obsoleta la tradicional clasificación entre medios de comunicación interpersonales y medios de comunicación social o de masas, estos últimos los que permiten la difusión de sus contenidos a un número indeterminado de receptores anónimos. De hecho, como señala Farré, Internet ha generado un proceso de convergencia e integración entre sectores que hasta ahora permanecían separados: los medios de comunicación, las telecomunicaciones, y las tecnologías de la información[21]. Su carácter de medio de comunicación de masas lleva a este mismo autor a defender que en nuestro Derecho y sobre la base de que como vehículo de intercambio de informaciones la red está protegida constitucionalmente por el derecho fundamental a la libertad de expresión e información, el ejercicio de las libertades de la comunicación a través de Internet ha de estar sometido a los límites que afectan a las mismas. Desde esta premisa defiende el autor que «cualquier información, opinión o idea, sustentada en el ciberespacio a través de texto, imagen o voz, se convierte automáticamente en difusión (al menos en algunos de los servicios ofrecidos por Internet) y debe, por tanto, respetar los límites constitucionalmente aplicables»[22]. Afirma en consecuencia y no podemos dejar de estar de acuerdo con ello, que no existe motivo

19 Farré López, cit., pp. 163 y 164.

20 García Morales, M.J. (1999). La regulación de los servicios multimedia en Alemania. *Autonomíes*, nº 25, p. 56.

21 Cit., p. 328.

22 Cit., p. 329.

para no ejercitar el derecho de rectificación en Internet. Lo que ocurre es que en Internet hay plataformas y herramientas de distinta naturaleza. Hay, por ejemplo, plataformas de páginas web que pertenecen a titulares de medios de comunicación convencional –prensa y televisión– respecto de las cuales no cabe duda de que cumplen el requisito de ser un medio de comunicación social legitimado pasivamente frente al ejercicio del derecho de rectificación. Pero hay otras, muchas, que pertenecen a personas físicas o jurídicas que no ejercen esa función de información pública y respecto de las cuales nos cabe la duda de si pueden ser consideradas medios de comunicación social a estos efectos.

Por otra parte, si pudiéramos configurar el llamado «derecho al olvido» –y no digo que lo postulemos– otorgando a los sujetos la posibilidad de conseguir que cualquier información pasada que les ataña y que permanezca en Internet sea eliminada o desindexada tanto porque ya resulte obsoleta como porque les afecte negativamente, sí se conseguiría en una gran medida la autodeterminación de la identidad en la red. Pero lo cierto es que el derecho al olvido, al menos desde la perspectiva de la propuesta de Reglamento de protección de datos que se ha elaborado en el seno de la Unión Europea[23], no significa eso. Como ya se ha defendido en otras ocasiones lo que supone es, sencillamente, el tratamiento unitario del ejercicio de las facultades de revocación del consentimiento, oposición y cancelación de los datos personales frente a los responsables del tratamiento digital, facultades que ya están recogidas en las legislaciones de protección de datos y que implican la concurrencia de los requisitos y condiciones de ejercicio de cada una de ellas. Además, el efecto de un derecho indiscriminado y sin condiciones a exigir la supresión de cualquier información que nos afecte llevaría a la construcción ficticia de la identidad ya que presumiblemente se haría desaparecer todo lo malo y se conservaría lo bueno. En definitiva, no puede mantenerse que, así las cosas, supusiera la tutela de un interés digno de protección.

6. LA IDENTIDAD DIGITAL

Enlazando con lo dicho en relación con el olvido digital y sin salir de la idea de identidad como derecho a ser uno mismo pero ampliando la perspectiva, conviene también hacer referencia a la realidad que cada vez va adquiriendo más predicamento en la vida de relación de una gran parte de los sujetos de los países desarrollados, y que es la identidad digital. Si partimos de su consideración como la manera libre en que una persona se presenta a sí misma en el entorno de Internet, en principio debería de coincidir con la identidad personal, al menos en aquellas facetas de esta última que hayan tenido reflejo en la red, y de hecho puede ocurrir perfectamente. Como hemos señalado, muchos de los problemas de tutela de la identidad personal que se están planteando

23 25.1.2012 COM (2012) 11 final 2012/001(COD)

actualmente se derivan del tratamiento que terceros puedan difundir a través de Internet. En este caso podemos seguir hablando de identidad personal en un sentido amplio inclusivo de la digital. Pero ello no quita que en la actualidad se esté ya planteando la necesidad específica de proteger autónomamente la identidad digital. Se habla incluso de un nuevo «derecho a existir en Internet», a poder tener un perfil en redes sociales y a no ser excluido de las mismas, a recibir resultados en búsquedas de uno mismo y a poder ejercitar para el perfil *online* los mismos derechos que para el *offline*[24]. El mayor problema que puede plantearse aquí en relación con la lesión de derechos es que los contenidos y datos que aparecen sobre cada persona y que configuran esa identidad digital hayan sido introducidos por otros sujetos.

Pero también hay ocasiones en que la propia persona construye una identidad *online* diferente a la identidad personal que refleja fuera de este entorno y que, aunque no tiene por qué ser necesariamente falsa solo por este motivo, es muy frecuente que lo sea. Con independencia de la cuestión de si esa identidad digital es o no protegible y en qué medida, lo que entiendo que no se puede contestar de manera general sino que habrá que ver las circunstancias de los casos concretos, pueden plantearse también otro tipo de problemas de todo orden relacionados con la suplantación o falsificación de la identidad.

7. CONCLUSIÓN

La falta de autonomía que el derecho a la identidad tiene en nuestro ordenamiento no debe llevar necesariamente a una postura negativa que considere inviable su protección en la red. Aunque desde luego existen problemas y lagunas que esperemos que el legislador español enfrente en algún momento, siempre es posible acudir a instrumentos protectores de otros derechos relacionados que hayan podido verse también vulnerados en el caso concreto o, en su caso, a fórmulas más generales como el recurso a exigir responsabilidad civil extracontractual sobre la base del artículo 1902 del Código civil si se dieran los presupuestos para ello. Por tanto, que se consiga tutelar de manera más o menos satisfactoria no solo depende de la existencia de una regulación específica sino también de la sensibilidad del jurista para articular con esa finalidad la legislación vigente.

BIBLIOGRAFÍA

Bessone (1973). Diritto soggetivvo e «droits de la personnalite». A propósito di un recente saggio. *Riv.trim.dir.proc.civ.*, pp. 1175-1199.

24 Fernández Burgueño, P. (2012), Aspectos jurídicos de la identidad digital y la reputación *online. AdComunica*, nº 3, pp. 127 y 139.

– Principio della tradiciones e nuove direttive in tema di diritto all'immagine. *Foro it.*, IV, cc. 182-184.

Farré López, P. (2008). *El Derecho de rectificación. Un instrumento de defensa frente al poder de los medios*, Madrid.

Fernández Burgueño, P. (2012), Aspectos jurídicos de la identidad digital y la reputación *online* . AdComunica, *Revista Científica de Estrategias, Tendencias e Innovación en Comunicación*, nº 3. Castellón: Asociación para el Desarrollo de la Comunicación adComunica, Universidad Complutense de Madrid y Universitat Jaume I. DOI: http://dx.doi.org/106035/2174-0992.2012.3.8. pp. 127 y 139.

Fernández Sessarego, C. (1992). *Derecho a la identidad personal*. Buenos Aires.

García Morales, M.J. (1999). La regulación de los servicios multimedia en Alemania. *Autonomíes*, nº 25, pp. 38 a 66.

Pino, G. (2006). Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali en *Libera circolazione e protezione dei dati personali,* a cura di R. Panetta, Giuffrè, Milano, t. 1, pp. 257-321.

Raffiota, E. C. (2010). Appunti in materia di diritto all'identità personale. Enero de 2010. www. forumcostituzionale.it (fecha de consulta febrero de 2013).

COMUNICACIONES SOBRE POLÍTICA

ABRIENDO BRECHAS: CENTRALIZACIÓN DE LAS DECISIONES E INTERACCIÓN ONLINE EN CIU, ERC Y EL PSC

Marc Esteve Del Valle
Doctorando del Programa de Sociedad de la Información y el Conocimiento de la Universitat Oberta de Catalunya (UOC)
Internet Interdisciplinary Institute (IN3)

Rosa Borge Bravo
Profesora Agregada de Ciencia Política de la Universitat Oberta de Catalunya (UOC)
Internet Interdisciplinary Institute (IN3)

RESUMEN: Los objetivos de este paper son estudiar la relación entre la centralización de las decisiones en tres de los partidos más significativos del panorama político catalán actual –CIU, ERC y PSC- y la interacción que éstos llevan a cabo tanto en sus páginas web como Facebook. Nuestras hipótesis de trabajo son dos. La primera se refiere a que los partidos con una mayor centralización de las decisiones ofrecen menos ventanas de interacción en sus páginas web que aquellos que poseen un grado menor. La segunda hipótesis apunta a que la implicación de los ciudadanos en las redes sociales de los partidos, en este caso Facebook, no tiene por qué corresponder al grado de centralización del partido. La razón de ello está en que los canales de interacción de las páginas web son diseñados por el propio partido mientras que la estructura de Facebook ya está predeterminada y su uso depende en mucha mayor medida de los internautas que se quieran implicar y de los temas que vayan surgiendo en el entorno político. Los resultados muestran que la centralización de todos los partidos es alta, aunque haya alguna variación y que, además, se dan pocas diferencias respecto a los canales de interacción que ofrecen los partidos en sus páginas web. En cambio, existen diferencias importantes entre los partidos en cuanto a la interacción existente en las páginas de Facebook. Dicha interacción parece depender más de los temas predominantes en la actualidad política que del nivel de centralización de las decisiones que pueda distinguir a los partidos. Este es un primer trabajo preliminar que posteriormente será completado con la inclusión del resto de partidos del arco político catalán.

PALABRAS CLAVE: Partidos políticos catalanes; Grado de centralización de las decisiones; Interacción online; Páginas web; Facebook.

INTRODUCCIÓN

Estamos viviendo en un mundo donde la información es el motor de un nuevo sistema socioeconómico y la Tecnologías de la Información y la Comunicación (TICs) los cables que a ella nos conectan. En este contexto, los partidos políticos de Catalunya tienen que gestionar algunos retos importantes entre los cuales se hallan el continuo declive de sus miembros (Scarrow y Gezgor, 2010; Whiteley, 2010), la desafección política de la ciudadanía y la necesidad de adaptar sus organizaciones a la nueva realidad de la

Sociedad Red (Castells, 2000). De hecho, la adaptación de los partidos a esta Sociedad Red debería ser considerada como uno de los principales retos a los que éstos se enfrentan. Se están desencadenando presiones internas y externas para la transformación de sus actuales estructuras jerárquicas en instituciones más abiertas y en red, en las que el poder y la agencia comienzan a desplazarse más hacia las redes y hacia los militantes y activistas, en vez de mantenerse únicamente en posiciones centrales como las de los líderes de las organizaciones clásicas (Bimber, Flanagin y Stohl, 2012).

En este mismo sentido, la red ofrece a los partidos políticos una nueva oportunidad para hacer más permeable su hasta ahora rígida estrategia partidista construida bajo el prisma de una aguda diferencia entre sus miembros y la ciudadanía (Margetts, 2006; Gibson, Ward y Lusoli, 2003; Löfgren, 2003). Asimismo, Internet añade nuevos recursos tecnológicos tanto para las organizaciones de los partidos como para sus luchas electorales. De este modo, los partidos se ven empujados hacia el uso de las TICs (Tecnologías de la Información y la Comunicación) tanto para la campaña electoral como para mejorar sus posiciones frente a otros partidos, como para comunicarse e incrementar la interacción con sus militantes y simpatizantes.

Sin embargo, el aprovechamiento de las nuevas TICs por parte los partidos políticos catalanes en pos de generar una mayor interacción con sus miembros y con el electorado no ha respondido ni a unos criterios fijos ni unívocos (Padró-Solanet y Cardenal, 2008). De hecho, aunque del uso que éstos han hecho de las TICs pueda corroborarse la tesis de la normalización y el efecto contagio (Gibson, 2013), cierto es también que el contexto político al que éstos se ven abocados así como sus propias características institucionales (Padró-Solanet, 2009) dan lugar a que lleven a cabo distintas estrategias de interacción en línea. Por lo tanto, creemos que puede ser científicamente relevante estudiar la relación entre las características organizativas y los rasgos de la interacción en línea del partido en el gobierno de Catalunya (*Convergència i Unió*), del siguiente partido en número de escaños y que ofrece su apoyo a CIU en el *Parlament* a través del *Pacte de Governabilitat* (*Esquerra Republicana de Catalunya*) y del principal partido de la oposición (*Partit dels Socialistes de Catalunya*). Este estudio se llevará a cabo desde una doble perspectiva: a. Analizando la interrelación entre el grado de centralización de las decisiones de los partidos con los elementos de interacción que éstos proveen en sus páginas web; b. Analizando las ventanas y el tipo de interacción existentes en las páginas *Facebook* de estos partidos.

En la siguiente sección reseñamos la literatura previa sobre los partidos y las TICs y explicamos las razones que motivan nuestro estudio. A continuación presentamos el diseño de la investigación y planteamos las hipótesis del estudio. Posteriormente exponemos los datos hallados en el análisis descriptivo de la interacción de las páginas web y *Facebook* de los partidos catalanes con miras a corroborar o refutar nuestras hipótesis. Finalmente discutimos las implicaciones de los hallazgos del estudio y esbozamos distintas vías para profundizar en la comprensión del fenómeno analizado.

1. LAS TICS Y LOS PARTIDOS POLÍTICOS

Desde la primeriza participación de los partidos políticos en el ciberespacio hacia mediados de los años 90 han surgido múltiples estudios intentando analizar su proceso de adaptación a este nuevo medio. Estos análisis pueden dividirse en tres grupos: 1. aquellos que estudian desde un punto de vista interno el impacto de las TICs en la relación entre los partidos y sus miembros; 2. aquellos que analizan desde una perspectiva externa el impacto de las TICs en las campañas electorales de los partidos, y 3. los que examinan los factores internos y externos que puedan afectar el uso de las TICs para la interacción con la ciudadanía.

1.1. El análisis de la adaptación de los partidos a las TICs desde un punto de vista interno

Los estudios relacionados con el impacto de las TICs en las organizaciones de los partidos políticos han sido limitados debido al problema de acceso a los datos de los partidos por parte de los investigadores sociales. Sin embargo, en términos generales, dos han sido los grandes ámbitos que se han analizado: 1. La adaptación de los partidos políticos a las TICs y el impacto de éstas en la participación en red que éstos ofrecen así como las posibilidades de descentralización y democratización de las decisiones generadas por estas tecnologías; 2. El análisis de las nuevas posibilidades de movilización y participación derivadas de la utilización de las TICs por parte de los partidos, es decir, si el uso de las TICs puede favorecer un mayor activismo entre los miembros de los partidos así como mejorar sus capacidades de captación de nuevos seguidores.

En lo que atañe a los estudios que analizan la transformación organizativa de los partidos debido a las TICs, Gibson y Ward (1999) fueron de los primeros autores en observar que la mayoría de los partidos habían desarrollado redes internas de computarización de la comunicación. No obstante, descubrieron que aunque la mayoría de partidos eran muy optimistas respecto las posibilidades que les ofrecían las TICs en aras a conseguir una mayor deliberación y consulta con sus miembros, el uso que éstos hacían para tal fin no era tan evidente. Antes al contrario, según estos autores los partidos valoraban más el uso de las TICs como instrumentos de coordinación e información que como herramientas para la discusión interna y el debate en el seno de sus organizaciones. Sin embargo, esta posición que podríamos considerar como «ciberrealista» fue rápidamente contrarrestada por H. Margetts (2001) quien con su primer paper sobre el «Cyber Party» abrió la puerta de la nueva corriente «ciberoptimista» en lo que atañe a las posibilidades que ofrecían las TICs a los partidos. Más específicamente, Margetts apuntó que las TICs podían modificar las estructuras de los partidos en una triple perspectiva: a. Democratizando sus decisiones; b. Gestando nuevas redes de interrelación con sus miembros más laxas e informales; c. Ofreciendo nuevas posibilidades de captación de fondos. Esta misma corriente fue seguida por los autores Heidar y Saglie (2003) quienes con su concepto

del «Network Party» apuntaron que el uso de las TICs daría lugar a partidos más desterritorializados, basados en redes temáticas informales (las cuales podían incluso llegar a ser virtuales). Según estos autores, estas redes serían más abiertas a las demandas de la ciudadanía, de los grupos de presión y de los expertos en políticas públicas y devendrían un punto de partida para el debate y la toma de decisiones partidistas así como para el reclutamiento de nuevos líderes.

En lo que concierne al análisis relativo a las nuevas posibilidades de participación y movilización ofrecidas por las TICs, si bien es cierto que los primeros resultados parecían dar la razón al grupo de los «ciberrealistas», también lo es el hecho que los recientes estudios llevados a cabo en el marco de la web 2.0 (O'Reilly, 2004) parecen reequilibrar la situación. En este sentido, el estudio de los usuarios de las intranets del Partido Liberal y del Partido Laborista llevado a cabo por Lusoli y Ward (2004) reveló que en ambos intranets los miembros visitaban las páginas web de los partidos de manera poco frecuente y que una minoría bastante significativa no lo hacía nunca. Además, aun habiendo cierta esperanza puesta en el hecho que las redes podrían atraer jóvenes votantes a los partidos y acrecentar el activismo de los ya miembros, los datos del estudio contravinieron tal perspectiva. De hecho, Sarah Vissers (2009) con su «espiral de desmovilización» de los miembros de los partidos corroboró este mismo comportamiento. En esta misma línea, el estudio de Pederson y Saglie (2005) del comportamiento y el uso de las TICs de los miembros (en la red y de fuera de ésta) de los partidos noruegos y daneses reveló que solo un tercio de éstos había visitado las páginas web de los partidos. Además, éstos autores llegaron a pronosticar una clara división entre los miembros activos y pasivos de los partidos en lo que al uso de las tecnologías atañe arguyendo, a la vez, que esta tendencia podía llegar incluso a empoderar las élites de los partidos.

No obstante, con el paso de la web 1.0 a la denominada web 2.0 las investigaciones recientes se han encargado de reequilibrar las posiciones entre los «ciberrealistas» y los «ciberoptimistas» a la vez que se ha comenzado a analizar las nuevas interrelaciones que se producen entre la sociedad y los partidos debido a la presencia constante y ubicua de las TIC. Autores como Bimber, Stohl y Flanagin (2008, 2012) han demostrado que para comprender la presente acción colectiva política se debe primero entender el contexto tecnológico y social al que las organizaciones están sometidas. En este mismo sentido, Bennett y Segerberg (2012) profundizan un poco más en el estudio de las actuales características de la acción colectiva y consideran que el auge de las «Digitally Networked Actions» nos permite hablar de un nuevo tipo de acción colectiva diferenciada a la apuntada por Olson (1965) a la que ellos conceptualizan con el término de «Acción Conectiva»[1]. Otra línea de análisis prometedora es la recientemente iniciada por R. Gib-

1 Según estos autores las principal diferencia entre la acción colectiva definida en términos Olsonianos y la actual «Acción Conectiva» es que: «Las redes de acción conectiva son mucho más individualizadas y tecnológicamente estructuradas en conjuntos de procesos que dan lugar a una

son (2013), en la que estudia las denominadas «Citizen Initiated Campaigns», las cuales son campañas online iniciadas por simpatizantes de los partidos, no necesariamente militantes, y que emplean las herramientas en la red creadas por los partidos o por los equipos de los candidatos (p. 5). Facebook y twitter, tanto de los partidos como de los propios de los simpatizantes, son elementos imprescindibles de estas campañas.

1.2. El análisis de la adaptación de los partidos a las TICs desde un punto de vista externo

Esta segunda área de investigación relativa a los partidos políticos y las TICs es la que ha suscitado mayor interés. Ya desde el año 1997, Margolis et al (1997) fueron de los primeros investigadores en estudiar durante las elecciones presidenciales estadounidenses del año 1996 el uso de la web por parte del Partido Demócrata y del Partido Republicano. Su estudio ofreció algunas conclusiones relevantes entre las cuales cabe señalar el hecho que el mundo político online reflejaba en cierta medida el mundo offline con los partidos de mayor tamaño dominando a los más pequeños. Sin embargo, no fue hasta el uso de las redes que hizo Howard Dean en 2003 durante las elecciones primarias del Partido Demócrata que los investigadores se interesaron aún más por estudiar este fenómeno. De hecho, el año 2003 Ward y Gibson publicaron un artículo que corroboraba en cierta medida la tesis de Margolis et al anteriormente mencionada. En éste apuntaban que en el plano político europeo, las democracias parlamentarias con sistemas políticos con fuertes partidos centrípetos tendieron a ofrecer campañas en red más elaboradas. No obstante, Ward y Gibson también expusieron que tanto los partidos Verdes (debido al hecho que sus miembros suelen utilizar mucho Internet) y las organizaciones políticas de extrema derecha (que utilizaban las herramientas de Internet para evadir las restricciones impuestas por los Mass Media) también obtuvieron importantes beneficios del uso de estas TICs (Ward y Gibson, 2003).

Finalmente, recientemente ha habido ciertos autores que han estudiado el uso de los Social Media por parte de los partidos políticos. En este sentido, Lynch y Hogan (2011) analizaron cómo los partidos irlandeses utilizaron los Social Media para llegar a conquistar a los miembros de la que ellos llaman la «Generación Z». Además, Tamara (2010) y Tumasjan et al (2010) concentraron sus esfuerzos en comprender el papel que Twitter puede desempeñar en las campañas electorales. De un lado, del análisis del contenido de los tweets de la población de Alemania durante las últimas elecciones nacionales, Tamara concluyó que se podía prever el resultado de éstas. Del otro, Tumasjan et al realizaron también un análisis de contenido de los tweets de la población de Corea

---

acción la cual no requiere ningún marco de identidad colectiva o de ciertos niveles de recursos organizacionales para responder eficientemente a las oportunidades que puedan emerger» (Bennett y Segerberg, 2012: 750).

del Sur durante las últimas elecciones presidenciales en el país y llegaron a la misma conclusión que la expuesta anteriormente por Tamara.

En último término cabe destacar el estudio de Aragon et al (2012) quienes analizaron más de 3 millones de tweets durantes las elecciones generales españolas de 2011. Los tweets procedían de los partidos políticos españoles, sus miembros, activistas, periodistas o medios de comunicación o eran tweets con hastags de contenido electoral o que mencionaban perfiles de twitter de candidatos o partidos. Los principales resultados que estos autores hallaron fueron: a. La existencia de una correlación positiva entre el incremento de la actividad política offline (concretamente, el debate electoral, el día de las elecciones y el día en que se cerraba la campaña electoral) y el volumen de tweets realizados durante el periodo electoral; b. El uso de distintas técnicas de marketing aplicadas a la utilización de hashtags durante la campaña electoral como métodos usados por algunos partidos con miras a conseguir una efectiva transmisión de sus mensajes electorales; c. La existencia (derivada del análisis de las emociones de los tweets) de un tono más positivo en los mensajes de los miembros del partido ganador de las elecciones; d. El bajo nivel de retweets entre los miembros de las distintas formaciones políticas; e. La mayor cohesión y conectividad entre los miembros y activistas de los partidos políticos más pequeños y nuevos y, por tanto, con un menor acceso a los mass media; f. La existencia de una mayor comunicación entre los miembros de un mismo partido (aunque los autores exponen que se observa una tendencia a aumentar la comunicación entre miembros de ciertos partidos equiparables –Por ejemplo: CIU/ERC o PP/PSOE); g. La imposibilidad de prever el resultado de las elecciones mediante el análisis del compromiso (medido por los autores vía los retweets emitidos por los miembros de los partidos) de los usuarios de twitter analizados.

1.3. El análisis de los factores que influyen en la adaptación de los partidos a las TICs

Algunos autores han estudiado distintos factores internos y externos a los partidos que pueden tener un impacto en las campañas electorales en red que éstos realizan y en el uso de las TIC para la movilización y la interacción con los ciudadanos. Römmele (2003) fue una de las primeras autoras en destacar que el uso de las TIC no sería uniforme por parte de los partidos y que dependería de los fines u objetivos del partido (maximización de votos, implementación de políticas, obtención de cargos, democracia interna). Así, los partidos centrados en la maximización de votos y cargos adoptarán una estrategia comunicativa top-down, mientras que los partidos que buscan implementar políticas y ampliar la democracia interna desarrollarían estrategias de comunicación bottom-up y más participativas. No obstante, estas teorías se recogen en una introducción a un monográfico sobre partidos y usos de las TICs[2] de forma que el modelo no es

2 Monográfico de «Party Politics» titulado «Party Politics on the Net», editado por Rachel K, Gibson, Andrea Römmele, y Stephen J. Ward. Vol. 9 (1), Enero 2003. http://www.partypolitics.

contrastado de forma sistemática por Römmele sino que emplea los estudios concretos publicados en el monográfico como ejemplos algo laxos de sus teorías.

En este sentido, destacan los análisis empíricos realizados por Padró-Solanet y Cardenal (2008) y Cardenal (2011) porque muestran en los casos concretos de los partidos catalanes y españoles cómo las características internas y la posición en el mercado electoral (ideología y coherencia ideológica, tipo de partido, centralización, importancia de la organización, existencia de conflicto interno, posición en el gobierno o en la oposición) de los partidos estructuran los canales interactivos y de participación que los partidos ofrecen en sus páginas web. Estos autores descubren que los grandes partidos, sobre todo cuando están en la oposición, tienden a abrir más canales de comunicación y participación en sus páginas web (Cardenal, 2011: 95). El ejemplo paradigmático sería el PP, teniendo presente que el análisis de Cardenal se realizó en febrero del 2010, casi un año antes de las elecciones de 2011. Asimismo, los partidos poco coherentes ideológicamente y con organizaciones pequeñas desarrollan más los canales de participación y comunicación, salvo los correspondientes a la movilización partidista controlada por el partido (o vertical) (Ibídem). Este sería el caso de CiU, poco coherente ideológicamente y con una organización extraparlamentaria más pequeña, frente al PSC o el PSOE que muestran más cohesión ideológica y poseen organizaciones importantes lo que desemboca en un desarrollo mayor de los canales más centralizados para el activismo y el apoyo al partido o para activar las redes de contacto (Cardenal, 2011: 96-97; Padró-Solanet y Cardenal, 2008: 58, 61).

Asimismo, Wall y Sudulich (2010) se centran en uno de estos factores explicativos: el grado de centralización de las decisiones partidistas, y en el caso de los partidos irlandeses. Frente a las dos únicas dimensiones que emplean Padró-Solanet y Cardenal para medir la centralización de la toma de decisiones (2008: 52), Wall y Sudulich emplean 3 dimensiones más (2011: 579). Estos últimos autores descubren, para el caso irlandés, que los partidos centralizados y con organizaciones jerárquicas desarrollan menos posibilidades de interacción en sus páginas web que partidos con una estructura más descentralizada y menos jerárquica. Precisamente el partido más grande y con más recursos del panorama político irlandés (Fianna Fáil) es el que menos elementos interactivos presenta en su página web (Wall y Sudulich, 2008: 588).

2. DISEÑO DE LA INVESTIGACIÓN E HIPÓTESIS

Esta investigación, sobre todo en relación a la primera hipótesis, sigue la estela del trabajo realizado por Wall y Sudulich (2010) sobre el comportamiento en la red de los partidos políticos irlandeses. En este sentido, intentaremos demostrar que tal y como exponen los autores anteriormente citados «los partidos organizados menos jerárquicamente utiliza-

org/Volume09/v09i1.html

rán Internet con fines inclusivos hacia sus miembros y el público en general, mientras que los más jerárquicos adoptarán estrategias top-down» (Wall y Sudulich, 2010: 578). Sin embargo, la principal aportación que realizaremos con respecto al estudio de Wall y Sudulich es que en el presente artículo mediremos tanto la ligazón entre los rasgos organizativos de los partidos catalanes (PSC, CIU y ERC) en su comportamiento en sus páginas web como en las de sus páginas Facebook de los tres partidos. Más específicamente, consideramos que si bien es cierto que hay un número elevado de estudios que han analizado los rasgos característicos de la interacción online que los partidos promueven en sus páginas web, también lo es el hecho que existe un fuerte desconocimiento del comportamiento de los partidos en sus Social Media. Por ende, siguiendo las investigaciones iniciadas por R.Gibson (2013), creemos que el estudio de las páginas Facebook de los partidos nos puede ayudar a comprender aún más su comportamiento online.

De este modo, formalmente queremos probar las siguientes hipótesis:

- H1: Los partidos con estructuras organizativas fuertemente jerarquizadas y centralizadas tienen menos probabilidad de tener instrumentos de interacción en sus páginas web que los partidos con estructuras organizacionales menos centralizadas (Wall y Sudulich, 2010).
- H2: El grado de centralización de las decisiones de CIU, PSC y ERC parece no estar relacionado con el número de ventanas de interacción ni con el tipo de interacción que estos partidos promueven en sus páginas Facebook.

La razón de estas dos hipótesis diferentes está en que los canales de interacción de las páginas web son diseñados por el propio partido mientras que la estructura de *Facebook* ya está predeterminada y su uso depende en mucha mayor medida de otros factores, como la coyuntura política que hace que ciertos temas y debates produzcan una mayor implicación por parte de los ciudadanos internautas.

Con el objetivo de corroborar o refutar nuestras hipótesis tendremos que operacionalizar los siguientes conceptos: 1. La centralización del poder en las estructuras organizacionales de los partidos; 2. El grado de interacción que los partidos facilitan en sus páginas web; 3. El grado y el tipo de interacción que los partidos llevan a cabo en sus páginas Facebook. Por lo tanto, nuestra variable independiente será el grado de centralización del poder en las estructuras de los partidos y nuestra variable dependiente la interacción en la red que éstos llevan a cabo.

2.1. Medición de la centralización de las decisiones en los partidos políticos catalanes

Con miras a medir el grado de centralización de las decisiones en las organizaciones de los partidos políticos catalanes seguiremos el esquema de codificación usado por Janda (1980). A cada partido se le atribuirá un nivel total de centralización de las decisiones que de manera estandarizada se situará entre 0 (completa descentralización

de las decisiones) y 1 (completa centralización). Con el fin de determinar dicho nivel se han analizado los estatutos del PSC, CIU y ERC (que descargamos de sus páginas web el 21-02-2013 entre las 10:22 y las 10:45) los cuales nos permiten hacer un análisis comparado entre estos partidos. Más específicamente, se han analizado las ocho dimensiones del índice de Janda con el objetivo de obtener el grado final de centralización de las decisiones para cada uno de los tres partidos anteriormente mencionados. Las dimensiones analizadas[3] son: a. Nacionalización de la estructura del partido; b. Elección del líder del partido; c. Elección de los candidatos al Parlamento; d. Distribución de los fondos del partido; e. Elaboración de las políticas del partido; f. Control de las comunicaciones; g. Ejercicio de las medidas disciplinarias; h,- Concentración del liderazgo.

Nuestra variable independiente principal que influye en el grado de interacción en las páginas web de los tres partidos analizados es el grado de centralización de las decisiones de los partidos (Wall y Sudulich, 2010), pero es necesario incorporar a nuestro estudio otros indicadores de las características de los partidos y su entorno electoral que pueden influir también en la existencia de canales de interacción en las páginas webs de los partidos (Solanet y Cardenal, 2008; Cardenal, 2011).

2.2. Medición de las posibilidades de interacción facilitadas por los partidos catalanes en sus páginas web

Varios han sido los estudios que desde finales del siglo pasado hasta muy recientemente han medido el contenido de las páginas web de los partidos (Gibson, 1999; Gibson y Ward, 2000; Norris, 2003; Padró-Solanet y Cardenal, 2008; Wall y Sudulich, 2010; Cardenal, 2011; Gibson et al, 2012; Gibson, 2013). Mayoritariamente, el método que estos autores han utilizado ha sido el de clasificar de forma dicotómica la presencia o ausencia de ciertas variables observadas en las páginas web de los partidos políticos y después realizar un recuento total. Seguiremos este enfoque dado que creemos que es el más empleado para evaluar las posibilidades de interacción que PSC, CIU y ERC ofrecen en sus páginas web. Sin embargo, antes de abordar más detalladamente cómo mediremos cuantitativamente dicha interacción creemos que es necesario definir este término. Al respecto, cabe decir que utilizaremos la misma definición que usaron Wall y Sudulich cuando la definieron como «los instrumentos capaces de facilitar de una

3 Los autores anteriores que han medido la centralización de los partidos para comprobar su influencia en el despliegue de ventanas de interacción y participación en las páginas web no han tenido presente las 8 dimensiones del índice de Janda (1980). Padró-Solanet y Cardenal (2008: 52) sólo emplearon las dos dimensiones que se pueden considerar más importantes: la selección del líder (b) y de los candidatos (c), y Wall y Sudulich (2010: 579), aunque tuvieron presente 5 dimensiones (a, b, c, e, g) no analizaron las otras 3 porque no se recogían en los estatutos de los partidos (d, f, h).

manera bilateral o multilateral la comunicación e interrelación, la cual incluye tanto los líderes de los partidos, sus miembros así como a los internautas no alineados con el partido» (Wall y Sudulich, 2010: 581).

Una vez definida la interacción creemos que es el momento de exponer cuáles han sido las variables que hemos utilizado para medir dichas posibilidades de interacción ofrecidas por el PSC, CIU y ERC en sus páginas web[4]. De un lado, hemos tomado en consideración las variables utilizadas por los estudios anteriormente mencionados (Wall y Sudulich, 2010; Gibson et al, 2012; Gibson, 2013) las cuales son: a. Links a los blogs de los miembros del partido; b.-Respuestas a los cuestionarios online realizados por los partidos; c. Contactar con los líderes del partido; d. Unirse al partido; e. Firmar peticiones del partido; f. Permitir a los usuarios donar al partido; g. Ponerse en contacto con el partido. No obstante, hemos añadido a estas variables otras que se refieren a las redes sociales que ofrecen los partidos: h. Compartir fotos subidas por los partidos en Flickr; i. Interactuar en la página Facebook del partido; j. Interactuar con el Twitter del partido; k. Compartir vídeos de Youtube del partido.

La medida agregada que utilizaremos para medir el grado de interacción en red ofrecido por los tres partidos en sus páginas web es el número total de categorías de interacción presentes en cada una de estas páginas dividido por el número total de categorías analizadas (en nuestro caso 11). El objetivo final será pues el de crear un índice estandarizado (0-1) en el que cada uno de los partidos pueda emplazarse según sus menores (0) o mayores (1) facilidades de interacción online.

2.3. Medición de las ventanas y del tipo de interacción de los partidos catalanes en sus páginas Facebook

La medición de las ventanas de interacción y del tipo de interacción de PSC, CIU y ERC se ha realizado de la siguiente forma: en lo que atañe a las posibilidades (o ventanas de interacción) que estos tres partidos ofrecen en sus páginas Facebook se han analizado: a. La capacidad de responder a los «posts» realizados por el partidos; b. La capacidad de hacer «like» a los «posts» realizados por el partido; c. La capacidad de compartir los posts del partido; d. La capacidad de iniciar un post por parte del usuario de la página.

Del otro lado, el análisis del tipo de interacción de PSC, CIU y ERC en sus páginas Facebook se ha llevado a cabo desde una doble perspectiva: a. Analizando los datos que Facebook nos ofrece en las páginas web de los tres partidos; b. Realizando un estudio analítico de la interacción que los tres partidos llevan a cabo en sus páginas Facebook. En lo que atañe a los datos que Facebook nos ofrece se han contemplado: a. La fecha

4 Cabe mencionar que para la medición de estas variables se han obtenidos los datos de las páginas web de los partidos visitadas el día 22-02-13 durante la franja horaria de 10:00 a 12:00.

en la que los partidos iniciaron su actividad en Facebook; b. El número total de *likes* que tiene cada partido; c. El número total de usuarios que está «talking about this»[5] de esta página. Al respecto, se debe apuntar que los datos anteriormente mencionados se obtuvieron el lunes 25-02-13 capturando primero aquellos relativos a la página del PSC (10:04), en segundo término los de CIU (10:05) y en último lugar los del ERC (10:06).

En lo que concierne a la obtención de los datos analíticos se ha utilizado en primer lugar la aplicación Netvizz[6] para obtener los datos relativos a la interacción de estos partidos en sus páginas Facebook[7]. Debemos mencionar al respecto que hemos limitado nuestra búsqueda a los últimos 100 posts originados por los tres partidos dado que no queríamos que nuestro estudio abarcase ni el período electoral ni el post-electoral en el que éstos se han visto inmersos tras las elecciones del 25 de Noviembre del 2012 al Parlamento de Catalunya. En segundo lugar, se ha realizado la lectura de los datos con el programa Gephi[8]. En último término, se han elaborado distintas categorías que nos permiten caracterizar los rasgos de la interacción de los tres partidos en sus páginas Facebook. Dichas categorías son: a. El número total de posts analizado para cada partido; b. El número total de posts con un link y/o con un video para cada partido; c. El número total de posts con fotos para cada partido; d. El numero total de likes derivados de los 100 posts para cada partido; e. El «engagement» (número total de posts, likes y sharings)

5 Al respecto, según Facebook, el «talking about this» se refiere al número total de usuarios que han creado una historia a raíz de un post de la página que se analiza. Según Facebook dichas historias contemplan los siguientes hechos: 1.-Compartir, darle al *like* o comentar uno de los posts de la página; 2. Responder a una pregunta; 3. Responder a un evento; 4. Solicitar una oferta (normalmente comercial).

6 Netvizz es una aplicación para Facebook que permite hacer archivos *gdf* de las redes de los amigos de un usuario, de los miembros de los grupos y de las páginas a los que éste pertenece. En nuestro caso hemos utilizado la aplicación Netvizz para captar (de los 100 posts analizados de las páginas Facebook del PSC, CIU y ERC) los datos relativos a las siguientes dimensiones: a. El número total de posts; b. El número total de usuarios; c. Las características de los posts (es decir, si son links con fotos, videos o solo links con texto); d. El compromiso; e. El número total de comentarios; f. El número total de likes; g. El género de los usuarios.

7 El momento de captación de datos con Netvizz ha sido el siguiente: 1. De la página Facebook del PSC se capturaron los datos el 25-02-13 a las 10:09; 2. De la página de CIU se capturaron el mismo día a las 10:13; 3. De la página de ERC se capturaron el mismo día a las 10:15. El período que cubren los 100 posts de cada partido hasta el día 25 de febrero son: 1. PSC: del 8 al 25 de febrero; 2. CIU: del 23 de enero al 25 de febrero; 3. ERC: del 15 de enero al 25 de febrero. Como puede comprobarse, los marcos temporales no son iguales debido a que el PSC realiza más posts por día, mientras ERC es el partido que publica menos posts por día (véanse más adelante las cifras de la tabla 6).

8 Gephi es un programa open software para la visualización y el análisis de redes. En nuestro caso hemos utilizado este programa para única y exclusivamente visualizar los datos obtenidos con la aplicación Netvizz.

para los 100 posts elaborados por cada partido; f. La media diaria de posts para cada partido; g. El número total de usuarios participantes en los 100 posts; h. El número de hombres y mujeres usuarios para los 100 posts.

3. RESULTADOS

3.1. Centralización de las decisiones de los partidos catalanes y otras características que pueden influir en su interacción online

En lo que concierne al grado de centralización de las decisiones de los partidos la tabla (1) nos presenta distintos datos relativos al grado de centralización de las decisiones de les tres partidos estudiados. La primera conclusión que se deriva de los resultados expuestos en ésta es que de un modo agregado el grado de centralización de las decisiones de los tres partidos es bastante elevado (siendo la media de los tres partidos del 0,71). En segundo lugar, otro de los datos relevantes para nuestro análisis es que los tres partidos obtienen resultados distintos, es decir, que CIU (0,76), el PSC (0,68) y ERC (0,67) distribuyen el poder de tomar las decisiones en sus organizaciones de una forma distinta, siendo CiU el partido más centralizado.

Al respecto cabe mencionar que si bien es cierto que los tres partidos obtienen valores equivalentes en 4 de las dimensiones del índice, también lo es el hecho que en las otras 4 éstas son dispares. Más específicamente, las dimensiones que presentan una mayor divergencia entre los tres partidos son las siguientes: a. La Nacionalización de la estructura; b. La elección de los candidatos al Parlamento; c. La formulación de las Políticas; d. El control de las comunicaciones.

En suma, el análisis de la centralización de las decisiones nos permite aseverar que los partidos de centro-izquierda e izquierda del sistema político catalán (PSC y ERC respectivamente) se diferencian muy poco entre ellos (un 0,09) pero que lo hacen de una manera significativa (0,8 en el caso del PSC y 0,89 en el caso de ERC) con respecto a CIU, partido que puede considerarse de centro-derecha.

Tabla 1: Grado de Centralización de las decisiones del PSC, CIU y ERC

Partidos	NE (0-10)	SLP (0-10)	SCP (0-10)	DF (0-10)	FP (0-10)	CC (0-10)	AD (0-10)	CL (0-10)	GCD (0-1)
PSC	6,66	3,75	10	8,57	6	5	5	10	**0,68**
CIU	8,33	3,75	10	8,57	7	8,75	5	10	**0,76**
ERC	6,66	3,75	5,55	8,57	6	8,75	5	10	**0,67**

NE: Nacionalización de la Estructura; SLP: Selección del líder del Partido; SCP: Selección de los candidatos al Parlamento; DF: Distribución de Fondos; FP: Formulación de las Políticas; CC: Control de las Comunicaciones; AD: Administración de la disciplina; CL: Concentración del liderazgo; GCD (estandarizado 0-1): Grado de centralización de las decisiones

Estos resultados son, además, compatibles con los obtenidos por Padró-Solanet y Cardenal (2008: 54) puesto que sólo emplean las dimensiones de selección del líder y de los candidatos para medir la centralización. Padró-Solanet y Cardenal clasifican a PSC y CiU como partidos centralizados, frente a ERC, que muestra una estructura descentralizada. En nuestro análisis, si bien en la elección del líder los tres partidos obtienen las mismas puntuaciones, en la selección de los candidatos al parlamento CiU y PSC muestran el máximo grado de centralización, frente a ERC con una elección del líder mucho más descentralizada.

Por otra parte, en lo relativo a las características de los partidos políticos y del mercado electoral que pueden influir en la interacción que éstos promueven en sus páginas web cabe destacar los siguientes elementos resumidos en la Tabla 2:

Tabla 2: Factores influyentes en la interacción online

Partido	Ideología	Organización		Mercado Electoral	
	Izquierda/ derecha[9]	Tipo Partido[10]	Conflicto Interno[11]	Tamaño[12]	Acuerdo de gobierno[13]
CIU	D	Catch-all	No	Grande	Si
PSC	I	Masas	Si	Pequeño	No
ERC	I	Masas	No	Pequeño	Si

Fuente: Elaboración propia a partir de los indicadores obtenidos de los estudios de Padró-Solanet y Cardenal (2008) y Cardenal (2011).

91011

9 Para clasificar a los partidos como de izquierdas o de derechas, se ha utilizado la misma clasificación que realizan Cardenal y Padró-Solanet (2008). En este sentido, y según éstos mismos autores "Cuando en la escala se les sitúa (a los partidos) entre 0 y un valor inferior a 5, se clasifican como de izquierdas, y cuando en la escala se les sitúa entre 10 y un valor superior a 5, se les clasifica como de derechas. En el estudio postelectoral de las elecciones al Parlamento de Cataluña del 2006 (CIS 2660, noviembre), las medias de las ubicaciones que el conjunto del electorado catalán atribuye a los partidos y coaliciones en la escala izquierda-derecha son las siguientes: ICV (3,0) ERC (3,0) PCS (4,2) CiU (6,5) Cs (6,8) y PP (8,7)" (Cardenal y Padró-Solanet, 2008: 52).

10 Con miras a clasificar los partidos de masas o partidos catch-all, se han utilizado dos indicadores expuestos por Cardenal y Padró-Solanet (2008): "a) los vínculos con los grupos de interés, si son más o menos estables y b) el tipo de base electoral, en términos sociales (si se basa en la clase u otro tipo de apoyo diferenciado o bien es transversal) o en términos geográficos (si la distribución geográfica es dispersa y homogénea por todo el territorio o bien se concentra en ciertas áreas)" (Cardenal y Padró-Solaent, 2008: 52).

11 En lo que concierne al conflicto interno en los partidos el indicador que se ha utilizado el grado de cohesión de las votaciones de los grupos parlamentarios de CIU, ERC y PSC al Parlamento

En suma, la tabla 2 nos muestra ciertas características de los tres partidos analizados que podrían influir en la interacción que éstos realizan en internet, tanto en sus páginas web como en sus páginas facebook. Aunque sería necesario un estudio con más casos (más partidos) para llegar a conclusiones más firmes, se observa que hay unas características comunes entre los dos partidos más descentralizados (ERC y PSC): son partidos de izquierdas, de masas, y un tamaño pequeño. En cambio el partido más centralizado (CiU) difiere respecto a estas características: es un partido de centro-derecha, catch-all, y con una representación parlamentaria grande.[12][13]

3.2. Ventanas de interacción facilitadas por los partidos en sus páginas web

Habiendo observado los distintos niveles de centralización de las decisiones en el PSC, CIU y ERC, es el momento de analizar los resultados del análisis descriptivo de las ventanas de interacción facilitadas por los tres partidos en sus páginas web. La Tabla (3) nos presenta distintos datos al respecto. En primer lugar, se observa que los tres partidos obtienen valores poco diferenciados siendo en este caso el PSC quien posee una mayor cantidad de ventanas de interacción online (9), situándose a continuación ERC y CIU (8). En segundo lugar, en lo que atañe a estas ventanas de interacción debe mencionarse que en cierta medida parece existir un contagio entre los partidos dado que de las 11 dimensiones analizadas los resultados entre los partidos estudiados sólo divergen en tres de ellas que son: a. Compartir las imágenes Flickr colgadas por el partido (ERC no dispone de esta posibilidad, el resto sí); b. Firma de peticiones online del partido o defendidas por el partido (PSC sí, el resto no); c. Donaciones al partido (ERC sí, el resto no). En último término, de las dimensiones usadas se debe remarcar el hecho que en la de los «Cuestionarios online del partido» los tres partidos catalanes obtienen valores nulos. Esto se debe a que se han empleado dimensiones analizadas en estudios de partidos de otros países en los cuales dicha dimensión sí se mostraba relevantes (Wall y Sudulich, 2010; Gibson et al, 2012; Gibson, 2013).

En suma, los resultados del análisis de la interrelación entre el grado de centralización de las decisiones del PSC, CIU y ERC con las ventanas de interacción en red que

---

de Catalunya. Los datos se refieren a las votaciones producidas en el Parlamento catalán tras las elecciones de 2012.

12 En lo relativo al tamaño de los partidos se utilizará el mismo indicador que el utilizado por Wall y Sudulich (2010) y Cardenal (2011). Es decir, se considerará a los partidos desde una doble vertiente: a.-Grandes: aquellos que tienen más del 20% de representantes en el Parlamento; b.- Pequeños: aquellos con menos del 20% de representantes en el Parlamento. Los valores se refieren a la representación en el Parlamento catalán tras las elecciones de 2012.

13 En lo relativo al acuerdo de gobierno el indicador valorará: a.- Si existe un acuerdo de gobierno entre algunos partidos; b.- Si no existe este acuerdo de gobierno. Los valores se refieren a la situación resultante en Cataluña tras las elecciones de 2012.

éstos ofrecen en sus páginas web no corrobora de forma suficiente la primera hipótesis (H1) de nuestro estudio. El partido más centralizado –CIU– tiene tantas ventanas de interacción online como ERC que resulta ser un partido más descentralizado y sólo una ventana menos que el partido más descentralizado –PSC–. Por tanto, los indicios de que a mayor centralización menos ventanas de interacción en las páginas web son débiles. No obstante, como ya se ha comentado, las variaciones entre los partidos en cuanto al grado de centralización y, principalmente, en cuanto al número de ventanas de interacción son pequeñas.

Tabla 3: Ventanas de interacción ofrecidas por el PSC, CIU y ERC en sus páginas web

Partidos/ventanas de interacción	PSC	CIU	ERC
CIF	1	1	0
CVY	1	1	1
IPF	1	1	1
ITP	1	1	1
ABMP	1	1	1
UP	1	1	1
RCP	0	0	0
CLP	1	1	1
FPR	1	0	0
DP	0	0	1
CP	1	1	1
Total (11)	**9**	**8**	**8**

CIF: compartir imágenes de Flickr colgadas por el partido; CVY: compartir videos de Youtube colgados por el partido; IPF: interactuar con la página Facebook del partido; ITP: interactuar con el usuario Twitter del partido; ABMP: tener un acceso a los blogs de los miembros del partido; UP: unirse al partido; RCP: responder a los cuestionarios online del partido; CLP: contactar con los líderes del partido; FPR: firmar peticiones online de los partidos; DP: hacer donaciones al partido; CP: contactar con el partido.

Los resultados obtenidos parecen discrepar de los análisis de Padró-Solanet (2008) y de Cardenal (2011) en los que CIU desarrollaba más intensamente que otros partidos los canales de participación y comunicación. No obstante, hay que tener presente que los análisis de los autores mencionados se llevaron a cabo cuando CIU estaba en la oposición tanto a nivel municipal de Barcelona como autonómico y, por lo tanto, es lógico que abran más canales de interacción y movilización ciudadana, como estos mismos autores descubren en sus propios análisis para el caso de otros partidos grandes (Cardenal, 2011: 95). Además, hay que tener en cuenta la diferencia en el número y tipo de indicadores empleados por los autores mencionados y el presente análisis, así como diferencias en la codificación de las ventanas de interacción.

3.3. Interacción del PSC, CIU y ERC en sus páginas Facebook

En primer lugar, en lo que atañe a las posibilidades de interacción que los partidos ofrecen en sus páginas Facebook la Tabla 4 nos muestra los datos para cada partido:

Tabla 4: Ventanas de Interacción que los tres partidos ofrecen en sus páginas Facebook

Partidos	Acciones Facebook			
	Comentar los posts	Darle al me gusta	Compartir el post	Iniciar un post *
CIU	Si	Si	Si	No
PSC	Si	Si	Si	No
ERC	Si	Si	Si	No

*Iniciar un post: por parte del usuario.

En suma, esta tabla nos permite observar cómo en lo que atañe a las ventanas de interacción que los tres partidos estudiados ofrecen en sus páginas facebook no existe variación alguna entre ellos.

En segundo lugar, el tipo de interacción que PSC, CIU y ERC llevan a cabo en sus páginas Facebook se estructura en un doble plano: a. El plano descriptivo; b. El plano analítico. En lo que atañe al plano descriptivo la Tabla (5) dispone distintos elementos al respecto. En primer lugar, se observa que los tres partidos iniciaron su actividad en Facebook el año 2009 y con un margen temporal de siete meses entre el primero que tomó esta decisión (PSC) y el último (ERC). Por lo tanto, una vez más, parece que la tesis del contagio se corrobora también en lo que concierne a la decisión de los tres partidos de usar Facebook como un instrumento de su comunicación política. En segundo lugar, en lo que atañe al número de total de *Likes*, se observa que existe una diferencia significativa entre los obtenidos por el PSC (8934) y aquellos obtenidos por CIU (11.211) y ERC (11.114). Sorprende, en este sentido, el escaso margen entre CIU y ERC. En último término, creemos que es en la dimensión «Hablando de esto» donde se halla el dato descriptivo más relevante. De hecho, este dato nos permite aseverar que los usuarios de la página Facebook de ERC (2092) utilizan 5 veces más que aquellos del PSC (436) y casi dos veces más que los de CIU (1201) la información que en ésta dispone el partido como elemento para articular su propia comunicación política online. Consecuentemente, de estos datos se puede concluir que los usuarios de la página Facebook de ERC utilizan la información que el partido subministra mediante este *Social Media* para crear sus propias historias en Facebook de una manera muy superior a aquellos que lo hacen a través de las páginas Facebook tanto de CIU como sobre todo del PSC.

Tabla 5: Análisis descriptivo de las páginas Facebook del PSC, CIU y ERC

Partidos	Fecha inicio actividad en Facebook	Numero total de Likes a la página del partido	«Talking about this»	Hora y día de la obtención de los datos
PSC	30/04/2009	8.934	436	Lunes 25-02-12 a las 10:04
CIU	22/09/2009	11.121	1.201	Lunes 25-02-13 a las 10:05
ERC	9/10/2009	11.114	2.092	Lunes 25-02-12 a las 10:06

En lo que atañe al plano analítico, la Tabla 6 nos muestra ciertos datos destacados. En primer lugar, respecto al tipo de interacción que llevan a cabo los tres partidos en sus páginas Facebook, se observa que mientras tanto el PSC (con un total de links + vídeos de 98) como ERC (con un total de links + vídeos de 82) realizan posts con breves frases y con links (o links con vídeos), CIU por su lado utiliza mayoritariamente fotos con poco texto[14]. En segundo lugar, del análisis de los 100 posts de cada partido se puede aseverar que el «Compromiso» o «Engagement» de los usuarios de la página Facebook de CIU (30476)[15] es más del doble al de los usuarios de ERC (14614)[16] y unas 17 veces superior al de los usuarios del PSC (1777). Además, esta misma tendencia se reproduce también en lo que concierne al número de links y comentarios totales que obtienen los tres partidos. Por lo tanto, estos datos nos indican que en los 100 posts analizados, los usuarios de las páginas Facebook de CIU han mostrado un compromiso mucho mayor tanto al de aquellos de ERC como a los del PSC con las ideas que el partido exponía en su página Facebook. En tercer lugar, los resultados de los datos sobre la media de posts realizados por los tres partidos políticos también nos indican un comportamiento muy diferenciado entre ellos permitiéndonos concluir que el PSC es el partido con más iniciativa de los tres (con una media de 5,88 posts/día) mientras que tanto CIU (con una media de 2,94 posts/día) como ERC (con una media de 2,38 posts/día) apenas llegan a los tres posts diarios. En cuarto lugar, de los 100 posts analizados para cada uno de los tres partidos se puede corroborar que el total de usuarios que han interactuado con los iniciados por CIU (5159) es muy superior al de los que interactuaron en las páginas Facebook del PSC (400) y ERC (2698) hecho que

14 La diferencia en el tipo de elementos empleados por CiU en los posts respecto a los utilizados por ERC y el PSC puede ser debida a diferentes estrategias de campaña y de comunicación. Los estrategas de la comunicación en Facebook recomiendan emplear fotos (aunque también vídeos) y frases breves para situar los posts de la página de Facebook entre los más visibles por los seguidores (véase el funcionamiento del EdgeRank).

15 Conviene destacar que, en el caso de CIU, 3039 elementos del «Compromiso» (shares, likes y comentarios) se realizaron el día 23 de Enero del 2013 y se referían al tema de la Declaración de Soberanía realizada por parte del Parlament de Catalunya ese mismo día.

16 En el caso de ERC, se efectuaron 1074 elementos del «Compromiso» el día 23 de Enero del 2013 cuando el Parlament adoptó la Declaración de Soberanía de Catalunya.

nos confirma la mayor interacción que acabamos de exponer cuando hemos comentado el compromiso de los usuarios de los distintos partidos. Finalmente, desde una perspectiva de género, el dato más relevante es que mientras la interacción de los usuarios de CIU ha sido casi paritaria en la de los usuarios de las páginas Facebook del PSC y de ERC se observa un claro predominio de la interacción masculina, ya que sólo el 36% son mujeres.

En conclusión, resalta el alto grado de interacción en las páginas de Facebook de ERC y CiU frente al que existe en la página del PSC, aunque en el caso de CiU gran parte de los posts iniciados por el propio partido son fotos con un mensaje corto y en el caso del PSC la media de post diarios originados por el partido es superior al de los otros partidos. Los resultados muestran que no parece existir una relación directa entre el grado de centralización de las decisiones del PSC, CIU y ERC con la interacción que se despliega en sus páginas Facebook, de forma que en este sentido se corrobora la segunda hipótesis (H2) de nuestro análisis.

Tabla 6: Estudio analítico de las páginas Facebook del PSC, CIU y ERC

Ventanas Interacción/ Partidos	Posts totales	TPL+V	TPF	Compromiso	NTL	NTC	MPD	NTU	NTH	NTM	V
PSC	100	98	2	1777	1233	179	5,88	406	249	140	17
CIU	100	3	97	30476	19360	2152	2,94	5159	2613	2439	107
ERC	100	82	18	14614	8353	518	2,38	2698	1659	953	86

TPL+V: número total de posts con link o con link con un vídeo; TPF: número total de posts con foto o infografías; Compromiso: número total de Shares, Likes y comentarios; NTL: número total de Likes; NTC: número total de comentarios; MPD: media de posts diarios realizados por los partidos; NTU: número total de usuarios; NTH: número total de hombres; NTM: número total de mujeres; V: valores perdidos del análisis de género.

En suma, probablemente hay otros factores que influyen en el desarrollo de una mayor interacción en las redes sociales de los partidos. El hecho de que CiU sea el partido en el gobierno, ERC le apoye, y que en el momento de la recogida de datos el tema soberanista estaba en pleno auge puede haber desencadenado una mayor participación en la página Facebook de CiU y de ERC, que en la del PSC.

4. CONCLUSIONES

En el presente estudio hemos continuado los análisis que realizaron autores como Padró-Solanet y Cardenal (2008) y Wall y Sudulich (2010) sobre la interrelación entre el grado de centralización de las decisiones de los partidos políticos y las ventanas de interacción que éstos ofrecen en sus páginas web. Sin embargo, hemos introducido en éste análisis el nuevo contexto tecnológico en el que los partidos catalanes están actualmente

inmersos, es decir, el auge de los *Social Media* como instrumentos de su comunicación política.

Los resultados finales nos demuestran que el grado de centralización de las decisiones no parece ser un elemento importante en lo que atañe a las ventanas de interacción que ofrecen en sus páginas web el PSC, CIU y ERC, en contraste con los resultados obtenidos por Wall y Sudulich (2010) para el contexto irlandés. Los tres partidos se caracterizan por una alta centralización en las decisiones, aunque CIU supera a los otros dos. La variación entre partidos en cuanto a despliegue de canales interactivos en la página web se limita a la existencia de un canal más en el caso del PSC. Por tanto, estas diferencias varían en muy poco grado dependiendo del nivel de centralización de las decisiones, el tamaño del partido o si está en el poder o en la oposición. Se corrobora, en definitiva, la tesis del contagio entre partidos al no haber grandes diferencias en los canales que se ofrecen en la web. Además, respecto a las páginas de Facebook los tres partidos inician su actividad en Facebook el año 2009 y con similares estructuras (no permiten iniciar posts).

No obstante, las diferencias sí son importantes en cuanto al tipo de mensajes que los partidos inician en el Facebook y en cuanto al nivel de interacción que producen: CIU emplea sobre todo las infografías y frases breves (mostrando la importancia de las estrategias de comunicación); el PSC es el partido que más posts inicia al día; y la mayor interacción se produce en el Facebook de CIU y, en menor medida, en el de ERC.

Hay que tener presente también que los niveles de análisis son distintos: por una parte, se examinan los elementos interactivos de las páginas web partidistas, es decir, los canales que ofrecen los partidos, y por otra parte, se estudia la participación de los Internautas en los Facebook centrales de los partidos, es decir, la demanda o el uso que los ciudadanos hacen de las redes sociales partidistas. El uso o participación en las redes sociales de los partidos no parece depender tampoco del grado de centralización del partido sino de otros factores que se deberían estudiar con más profundidad como la posición gubernamental del partido o la irrupción de temas más dominados por unos partidos que por otros. En este sentido se ha apuntado como posible explicación el debate soberanista ya que los días antes y después de la adopción de la Declaración de Soberanía el día 23/01/2003 por parte del Parlament, se dispara el «compromiso» sobre todo en CIU pero también en ERC, mientras que en el PSC no produce casi interacción.

Además, otras de las conclusiones relevantes que nos ofrece este análisis son: de un lado, en lo que atañe al impacto de la TICs en los partidos, parece en cierta medida corroborarse los augurios de Pedersen y Saglie (2003) y Margetts (2006) quienes apuntaron a una posible flexibilización en la relación entre los partidos y sus seguidores debido al papel de intermediación de las TICs. Como hemos visto en el Facebook de los partidos, a través de los *Social Media* se crean nodos de opinión sobre temas, que comparten y distribuyen contenidos, sin distinguir entre militantes, simpatizantes o votantes. Del otro, en lo que concierne al análisis de la interacción online de los partidos,

este artículo demuestra que es necesario combinar el análisis de la interacción online de las páginas web de los partidos con la interacción que éstos realizan vía sus *Social Media*. Únicamente el análisis del número y variedad de los canales interactivos de las páginas web no ofrece una descripción completa de la interacción online que promueven los partidos, sino que en la actualidad es necesario el estudio de la interacción que despiertan en las redes sociales. Como hemos comprobado, además, el número de canales interactivos en la página web no tiene por qué ir parejo a la intensidad de la interacción en las redes sociales.

En suma, este estudio debe considerarse como un primer paso necesario para abordar ulteriormente un análisis completo del fenómeno estudiando todos los partidos que forman parte del actual Parlament de Catalunya. Además, otra de las cuestiones que se derivan del presente análisis es la de extender el estudio a otros *Social Media* como Twitter, en el que la iniciativa del usuario es incluso mayor que en el caso de las páginas Facebook de los partidos donde el origen de los posts siempre proviene del propio partido.

BIBLIOGRAFÍA

Aragón, P., Kappler, A., Kaltenbrunner, J., Neff, J.G., Laniado, D. y Volkovich, Y. (2012) «Tweeting the Campaign: Evaluation of Political Party Strategies in Twitter for the 2011 Spanish National Elections» Paper presentado en la *II Internet, Politics and Policy Conference*, Oxford Internet Institute, Oxford.

Bimber, B., Stohl, C. y Flanagin, A. (2009). 'Technological change and the shifting nature of political organization', en A. Chadwick & P. Howard (eds.) *Routledge Handbook of Internet Politics*, Routledge, London, 72–85.

Bimber, B., Flanagin, A. y Stohl, C. (2012). *Collective Action in Organizations: Interaction and Engagement in an Era of Technological Change*. New York: Cambridge University Press.

Cardenal, Ana, S. (2011). Why mobilize support online? The paradox of party behaviour online. *Party Politics*, 19 (1), 83-103.

Castells, M. (2000). *The Rise of the Network Society (The Information Age: Economy, Society and Culture, Volume 1) (Vol 1)* (p. 594). Malden: Wiley-Blackwell.

Gibson, R. K. and Ward, S. J. (1999). 'Party Democracy On-Line: UK Parties And New ICTs', *Information, Communication and Society*, 2:3, 340–367.

Gibson, R. K. and Ward, S. J. (2000). 'A proposed methodology for studying the function and effectiveness of party and candidate web sites', *Social Science Computer Review*. Vol. 3 (18), 301-319.

Gibson, R., Nixon, P. y Ward, S. (2003). *Political Parties and the Internet. Net Gain?* London. Routledge.

Gibson, R., Römmele, A. y Ward, S. (eds.) (2003). Party Politics on the Net. *Party Politics. Special Issue* , Vol. 9 (1). Disponible en: http://www.partypolitics.org/Volume09/v09i1.html

Gibson, Rachel K., Lusoli, W., y Ward, S. (2005). Online Participation in the UK: Testing a «Contextualised» Model of Internet Effects. *The British Journal of Politics and International Relations*, *7* (4), 561-583.

Gibson, R. K., Gillan, K., Greffet, F., Lee, B. J., y Ward, S. (2012). Party organizational change and ICTs: The growth of a virtual grassroots? *New Media & Society*, *15*(1), 31-51.

Gibson, R. K. (2013). Party Change, Social Media and the Rise of «Citizen-initiated» Campaigning. *Party Politics*. Versión online disponible en: http://ppq.sagepub.com/content/early/2013/01/30/1354068812472575

Heidar, K., y Saglie, J. (2003). Predestined Parties?: Organizational Change in Norwegian Political Parties. *Party Politics*, *9* (2), 219-239.

Janda, K. (1980) *Political Parties: A Cross-National Survey*, Free Press, London.

Jansen, B. J., y Zhang, M. (2009). Twitter Power: Tweets as Electronic Word of Mouth. *Journal of the American Society for Information Science*, *60* (11).

Lusoli, W. (2005). «Politics Makes Strange Bedfellows»: The Internet and the 2004 European Parliament Election in Britain. *The Harvard International Journal of Press/Politics*, *10*(4), 71-97.

Lynch, K., y Hogan, J. (2011). Political Parties and Generation Z – Facebook Friends or Something More?, Paper presentado en la *Annual Conference of the PSA*, Londres, 20 de Abril.

Margetts, H. (2001). «Cyber Parties», ECPR Joint Sessions of Workshops, Grenoble, 6 al 11 de Abril.

Margolis, M., Resnick, D. y Ching-Chang, T. (1997). Campaining on the Internet: Parties and Candidates on the World Wide Web in the 1996 Primary Season. *The International Journal of Press/Politics.* vol. 2 no. 1: 59-78.

Olson, M. (1965). *The logic of collective action: public goods and the theory of groups.* Cambrige, MA: Harvard University Press.

Padró-Solanet, A. y Cardenal, A. S. (2008). «Partidos y Política en Internet: Un análisis de los websites de los partidos políticos catalanes». En: «La democracia electrónica» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política.* N.º 6. UOC. Disponible en: http://www.uoc.edu/idp/6/dt/esp/padro-solanet_cardenal.pdf

Padró-Solanet, A. (2009).»The Strategic Adaptation of Party Organizations to the New Information and Communication Technologies : A Study of Catalan and Spanish Parties» *ECPR Joint Sessions of Workshops*, Lisboa, Abril.

Pedersen, K. y Saglie, J. (2005): «New Technology in Ageing Parties: Internet Use in Danish and Norwegian Parties». *Party Politics*. Vol 11. No.3 pp. 359-377.

Römmele, A. (2003). «Political Parties, Party Communication and New Information and Communication Technologies» *Party Politics. Special Issue Party Politics on the Net*. Vol. 9 (1), 7-20. Disponible en: http://www.partypolitics.org/Volume09/v09i1.html

Tumasjan, A., Sprenger, T. O., Sandner, P. G., y Welpe, I. M. (2010). Predicting Elections with Twitter: What 140 Characters Reveal about Political Sentiment. En *Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media* (pp. 178–185). Menlo Park, CA: The AAAI Press.

Vissers, S. (2009). «From preaching to the converted to preaching through the converted». Paper presentado en las *ECPR Joint Sessions of Workshops*. Lisboa. Abril 14-19.

Ward, S., y Gibson, R. (2003). On-line and on message? Candidate websites in the 2001 General Elections. *The British Journal of Politics and International Relations*, *5* (2), 188-205.

Wall, M., y Sudulich, M. L. (2010). *Matrix Revolutions? Information, Communication & Society*, *13*(4), 574-591.

CASUAL POLITICS: FROM SLACKTIVISM TO EMERGENT MOVEMENTS AND PATTERN RECOGNITION

Ismael Peña-López
Professor at the School of Law and Political Science of the Open University of Catalonia

ABSTRACT: Politics have traditionally looked at the exercise of democracy with at least two implicit assumptions: (1) institutions are the normal channel of politics and (2) voting is the normal channel for politics to make decisions. Of course, reality is much more complex than that, but, on the one hand, all the extensions of that model beyond or around voting –issues related to access to public information, to deliberation and argumentation, to negotiation and opinion shaping, or related to accountability– are based on institutions as the core axis around which politics spin. On the other hand, the existence and analysis of extra-institutional political participation –awareness raising, lobbying, citizen movements, protests and demonstrations– have also most of the times been put in relationship with affecting the final outcomes of institutional participation and decision-making, especially in affecting voting.

Inspired in the concept of «feet voting» (developed by Tiebout, Friedman and others) in this paper we want to challenge this way of understanding politics as a proactive and conscious action, and propose instead a reactive and unconscious way of doing politics, based on small, casual contributions and its posterior analysis by means of big data, emergence analysis and pattern recognition.

In our theoretical approach –illustrated with real examples in and out of the field of politics– we will argue that social media practices like tweeting, liking and sharing on Facebook or Google+, blogging, commenting on social networking sites, tagging, hashtagging and geotagging are not what has been pejoratively labelled as «slacktivism» (a comfortable, low commitment and feel-good way of activism) but «casual politics», that is, the same kind of politics that happen informally in the offline world. The difference being that, for the first time, policy- and decision-makers can leverage and turn into real politics. If they are able to listen. If they are able to think about politics out of institutions and in real-time.

KEYWORDS: slacktivism, hacktivism, cyberactivism, emergence, e-democracy, e-participation.

1. INTRODUCTION

In 1956, Charles M. Tibeout published *A Pure Theory of Local Expenditures* (Tiebout, 1956). In his work, the author theorized about a local government model to provide a series of public services to its citizens. Under certain conditions, these citizens would end up moving from one city to the next one so to adjust their preferences to the public policies being run in a specific municipality. Although the term does not appear in the original text, credit is given to Tiebout for the idea of «voting with one's feet» or

«foot voting» as a tacit and extra-representative way of doing politics by citizens – and, thus, a way of making decisions out of the institutionally designed channels for these purposes.

There are two conditions in Tibeout's model that make it difficult to translate from the theoretical to the real world: the fact that the citizen has it easy –both in terms of feasibility as in terms of cost– moving from one place to another, and perfect or complete information.

Half a year after that exposition, digitization of content and communications by means of Information and Communication Technologies make that these conditions –mobility, perfect information– if they are not real, they actually are much less of a barrier in comparison to Tiebout's times. Indeed, ICTs have removed at a stroke the scarcity of information and the transaction costs associated with its management. On the other hand, but still related to that, ICTs have almost made irrelevant the matter of mobility when it comes to being informed, debating, negotiating or, after all, expressing one's preferences.

In this sense, Benkler (2006) already stated that a new model of working or a new model of doing politics would rarely fit within the parameters of the traditional «hub and spoke» model of the industrial society. In that model, hubs concentrate communications and decision-making, while the rest of the nodes are fed by these centres in spike architecture, isolated from each other. To replace this industrial model, Benkler expects the building of a progressive networked public sphere, thus modifying the fundamental processes of social communication.

This change in the way of communicating and doing does not only happen at the individual level but –and above all– at the collective level (Noveck, 2005). That is, technology does not only empower the particular citizens, but it provides them with new tools after which or upon which they can build up new forms of collective action. Despite the fact that Benkler's approach is undoubtedly much broader and deeper, Noveck's is partly more ambitious: «we should explore ways to structure the law to defer political and legal decisionmaking downward to decentralized group-based decisionmaking».

Notwithstanding, the technical possibility of carrying out a specific change or movement –even if exploratory– should not be a sufficient condition (though probably yet necessary) for accomplishing it.

But this fundamental condition is provided by Inglehart (2008) when he speaks of the change in values among generations and, in general, compared with the years immediately after the revolution of May 1968 and the pacifist movements during the following decade. In his analysis, the author clearly identifies how the changes in values that were breaking in 1971 have consolidated even to the point of an ending to the intergenerational confrontation in matters of values. Indeed, values more identified with materialism –with survival– are already part of generations in their way towards di-

sappearance. On the contrary, post-materialist values centred in autonomy and self-expression become hegemonic, values that, not surprisingly, several authors have identified as resonating with the hippy philosophy of the decade of 1960 or the hacker philosophy bound to the development of the (Himanen, 2003; Lanier, 2010).

2. POLITICS AND/ON THE INTERNET

Thus, technological changes along with a change in values are a perfect ground for changes in behavior to take place and, above all, for changes of approach in everything that is related with collective or community matters. Several authors have, consequently, analyzed the potential of the Internet on economic development, civic engagement or citizen participation, following the idea that «the Internet may be a new stimulus for political knowledge, interest, and discussion» (Mossberger et al., 2008). But is that really so?

The first thing that scientific evidence tells is that on the Internet, and concerning its use in politics, the knowledge gap hypothesis (Tichenor et al., 1970) is increasingly been confirmed by research. Thus, political participation is highly determined by educational level, employment situation and, in a lesser extent and with decreasing importance, by age. It does not happen this way, though, with socio economic status or class (Robles Morales et al., 2012).

Notwithstanding, it has been proved (Borge & Cardenal, 2012) that usage –or the experience in usage– of the Internet does have a direct effect on political participation, and that this effect is independent from political motivation. In other words, digital competence increases the probability that a person ends up participating in online politics, and this will happen independently of their initial political motivation. The explanation, among other reasons, would be that the abundance of political content on the Internet increases the probability that a given Internet user finds by chance and reads this political content, despite the fact that it was not within their original purposes. On the other hand, this probability is yet again increased by the intensive usage of search engines in quest for online information that broadband users usually perform. Last, because this information is gathered by non-traditional websites, that is, by websites that do not belong to political parties or organizations explicitly related with political activity (labour unions, lobbies, etc.), thus offering political information for the non-political information seeker (Horrigan, 2004).

Once information is found on the Internet –oftentimes unintentionally or by serendipity– it is also usual that users find open forums where to engage in a debate –or a discussion– about politics. These «'open source' spaces for dialog» (Kelly et al., 2005) enable all kind of encounters that do not necessarily are partisan or flocks of the same feather.

The final result of this political participation on the Internet can be summarized in three different ways. Firstly, things do not change at all or, in any case, what already was taking place in the offline world is reinforced by online practices. Indeed, and as we have already stated referring to the use of the Internet in relationship with the socio-demographic status, and referring too to the knowledge gap hypothesis, it has been evidenced that online activities do not substitute but reinforce political actions that the engaged citizen was already performing outside of the Net (Christensen, 2011). Secondly, greater exposition to political information on the Internet has been identified too with a higher level of criticism in one's own political positions that, often –though still in a reduced and minority context–, have ended up being transformed in an also critical vote, and thus favourable to minority political alternatives; alternatives that, if not opposed to one's initial ideas, certainly not mainstream and quite marginal within the hegemonic political system. Thirdly, the use of the Internet and accessing the information found in there have also been linked with going beyond critical voting, and with the increase in both the intensity and the amount of participation in extra-representative initiatives and political actions, that is, not marginal to the hegemonic political system, but completely outside of it (Cantijoch, 2009).

Notwithstanding, we believe that this approach –how does the Internet affect voting, how does the Internet affect motivation, how does the Internet affect participation in institutional politics or in extra-representative movements– still is too partial for the depth of the changes that we are witnessing in our streets.

Sádaba (2012) reminds us about the same issue with which we also began our reflection: the dire importance of the political and socioeconomic changes, associated with social movements, which can hardly stick to causal relationships related to technological changes or changes in communications. So, when doing the exercise of explaining the «virtualization of social movements» it does not seem sufficient with just superimposing a «digital layer» to what already exists, but it is very likely that a comprehensive rethinking of the whole model is much needed, including in this new model how political commitment, participation or activism work, so that we can understand the newly appearing trends.

An interesting approach about the limitations of seeing the upcoming political transformation enabled by the Internet as a mere virtualization of existing practices and actors comes from Martínez Roldán (2011) and his revisit of lefebvrian theory (Lefebvre, 1991). In his work, we can read the new movements as redesigns of the *Spaces of Representation* coming to «displace the hegemonic *Representations of Space* established by the dynamics of the capital». As a result, a hybridization of the urban space and the cyberspace takes place, affecting, in return, the spaces of representation and, above all, the representations of space and the institutions that inhabit and shape them.

The idea of these new spaces as something more than mere virtual carbon copies of the reality has already been explored by Castells (2012) in his spaces of autonomy, or

by Echeverría (1999) in his idea of the third environment. Both approaches can also be understood as interesting complements to Marc Augé's non-spaces (2000): the citizenry reinventing spatiality and, by doing it, reinventing the institutions of our society that now have to yield to the new leisure and consumption habits, but also to political activism. Of course, the re-location of the political action has to necessarily go hand-in-hand with a «process of formation and exercise of power relationships in the new organizational and technological context derived from the rise of global digital networks» (Castells, 2009).

We believe there is enough evidence to state that politics with and on the Internet runs on two different levels: firstly, an evolutionary one, where old practices and actors are replacing procedures and tools from the past by new digital protocols and tools; secondly, a transformative and disruptive one, where old spaces and power relations are being altered in their essence with new practices, actors and scenarios that escape traditional characterization schemes.

3. ONLINE PARTICIPATION AND EXTRA-REPRESENTATIVE PARTICIPATION: FROM EMPOWERMENT TO PARA-INSTITUTIONS

We have already seen how the Internet makes it more likely being informed about politics, or having a higher degree of engagement and participation. But it is also true that this impact does not only happen at the quantitative level, but also the quality of such engagement and participation is affected. Colombo et al. (2012) clearly show how, in addition to greater interest, the Internet makes that internal political efficacy –the degree with which people consider themselves more or less competent in politics– is also positively affected. In other words, greater interest and higher internal efficacy levels can be seen as good proxies for the level of empowerment of the citizen considered as a political actor. This empowerment –understood as the freedom to act within the system– is notwithstanding not matched by higher levels of governance –understood as the freedom to act upon the system–: that is, internal efficacy is not matched by more external efficacy –the idea that the citizen has on the disposition and capability of their leaders and institutions to provide answers to the demands of the population– and often turns into disaffection with the actual democratic system.

At this point, a relevant question is worth being put: whether this disaffection will join the ranks of abstention, or whether this disaffection will be transformed into extra-representative political action.

What so far has been found is that further empowerment of the citizens has resulted in a new elite, a *leetocracy* (Breindl & Gustafsson, 2011) of *goverati* (Peña-López, 2011) that defines a hard core of activists coalescing temporarily to run campaigns or to include a specific issue in the public agenda, thus becoming a sort of new mediators

between public decision-makers and the citizens. This «small group of highly specialised movement entrepreneurs» (Breindl, 2012) defines new hierarchies whose evolution begins in the constitution of the core of the movement, its enlargement and further participation of other agents of the public sphere –this time coming from the lines of the traditional activists–, and the conversion of the movement into new para-institutions that look much like the traditional pattern on their outside, but that are radically different, network-like, in their inside (Peña-López et al., 2013).

These networks and sub-networks, linked to each other, live together in «strong symbiosis between [the] established commercial players of the mainstream media» (Kelly, 2008), sometimes threatening their mere existence, some other times collaborating with them, though now creating new forms of relationship and partnership between the actors of the political scene. But it is not only about changes: the actors themselves that participate in these networks are transformed too, as are their respective roles, among them mass media and the tasks that these used to carry on.

New forms of being informed and new forms of informing. Nevertheless, we have already seen how its impact is usually centred in extra-representative participation and only marginally in abstention or vote to minority alternatives. So far, we could understand that the whole change of paradigm towards which we seem to be heading is but limited to some procedures and communities acting in the margin of huge majorities. On the contrary, if there is something at the core that has been extremely altered that is debate. Anduiza et al. (2012) state that the impact of the exposition to online political information is certainly determined by social extraction. These determinants, indeed, affect –and again following the knowledge gap hypothesis– affect all areas related to political information and the motivation to vote, either online or by other traditional channels. However, while the impact on motivation or on activism of online political information is small compared to other socioeconomic factors, it is not so with political debate: the existence of information on the Net sparks the debate and does have a major impact in the involvement of citizens in political discussions.

Font et al. (2012), and after the work by Hibbing & Theiss-Morse (2002), provide some insights that can complete some of the ideas presented here. There is an apparent paradox that citizens seem to demand higher levels of involvement in politics while the data show a decline in party membership, unions and NGOs. But the paradox is cleared when we ascertain that participation is actually increasing in alternative ways such as non-formal or extra-representative political participation. The citizenry that demands greater involvement also has a certain bias (left-winged, urban) that matches the profile of the average Internet user. Furthermore, while this citizenry is suspicious and critical towards professional politicians and elected officials, it seems to rely more on their peers, in the same way that social networking platforms are reflecting the dynamics of this collective behaviour.

It is also worth noting that extra-representative participation is activated by extremes cases: extreme cases such as those seen during the Arab Spring in 2011, or in

Spain in March 2004 and in May 2011, the latter already out of the local sphere and embedded in an international financial crisis. Thus, and after the debate is sparked partly thanks to ICTs, these extreme cases would be the ones that enable the forging and setting of extra-representative participation that, at its own turn, finds in ICTs a perfect tool for its organization and coordinated action. And the circle closes.

4. ONLINE PARTICIPATION, CYBERACTIVISM AND SLACKTIVISM

Almost a decade has passed since the bloom of the so-called Web 2.0 and soon a second decade will have passed since the Internet was made available to the general public. Along the years, evidence (Smith, 2013) has refuted some myths while it has reinforced some of the ideas we have been presenting in the last paragraphs. That is, the constantly –and in recent years rapidly– growing political activity on social networking sites has not implied the decoupling of the «virtual world» with the «face-to-face world» or «real world», but the opposite: there is a total consensus about social networking sites being yet another part of any political activity.

However, while not detached from what happens offline, the patterns of online behavior begin to have clear differentiating features from traditional politics (Rainie et al., 2011; Obar, 2012): communication becomes more frequent and intense; it is believed that the digital medium favors the achievement of fixed goals; there is greater participation accompanied by greater engagement and greater satisfaction with the obtained results. Fernández-Prados (2012) even opposes Activism 1.0 with Activism 2.0, the second one much more oriented to debate and action, much more horizontal in form and more aimed at social transformation in its core. The author also contrasts the concept of e-participation and other procedures closer to conventional or representative participation, against e-protest as identified with new forms of political action such as cyberactivism, digital activism, or hacktivism, definitely far from the institutions and forming new channels of extra-representative democracy.

Drawing a parallel with the virtual communities dedicated to content creation, Fuster & Subirats (2012) define new communities of political action where participation is highly open, both in terms of «membership» –if this word is of any relevance in this context– as in terms of different profiles, forms and levels of commitment. This participation is also a highly decentralized and asynchronous one, with no dependencies of space –association venue, party headquarters– or time –scheduled meetings or assemblies. It is a participation that is also open in the sense of public participation, widely reported by the networks, and autonomous, where the individual is ultimately responsible for their commitment as well as the tasks they undertake. Finally, it is a form of participation also open in the way action happens and is implemented, initiated by individual initiative and fostered by individual endorsement. It is politics and it is democracy grounded in doing things and making things happen: a do-ocracy.

These new political communities, open, «forming around interested and knowledgeable discussants» (Kelly, 2008), are already replacing the existing hierarchies and substructures.

Far, then, from the «daily me» (Negroponte, 1995) or from the «echo chambers» (Sunstein, 2001), what emerges is a brand new political participation that hardly fits neither in the theories of mobilization nor in the theories of reinforcement (Norris, 2001), but seems instead to emerge as a new para-institutional way (Peña-López et al., 2013), halfway between mobilization and the new political forms and the reinforcement of the existing traditional institutions.

A new political mobilization that also has a fundamental feature that distinguishes it from other previous forms of involvement, both in its forma and in its scope: the constant logging and reporting of each and every activity and piece of participation, the traceability of all tasks and actions, the comprehensive and detailed documentation of the processes, the opening/openness of these processes and, finally, the publication and making available to the public the entire data sets, protocols, tools and results used in and resulting from political action.

It is in this context, and closely related with the high granularity accepted in the commitment and level of participation in these new communities of political activism, that the figure of slacktivism appears and progressively gains momentum. We want to here present two approaches to this concept. The first one, denounced and reviled by Morozov (2011), is the one generally used in the media and the literature and approaches slacktivism from the micro level and the side of the sender or the slacktivist. In this first meaning, the citizen satisfies their need to engage politically by getting involved in almost pointless and isolated actions, either by signing an online petition, either by forwarding a message or re-tweeting a tweet, either by «liking» or just commenting a piece of content shared on a social networking site, a blog or a mass media website. There is no doubt that, from this point of view, seen as a strictly politically unbound activity, slacktivism ranks last in the ladder of commitment, responsibility and effort of political activity.

There is, however, yet another approach, which can be made at the macro and the collective/aggregate level, and emphasizing on the side of the receiver, the one whom the *whole set* of clicks/RT/I-like casted by the whole set of *all* citizens is addressed to.

First, and as shown by Nonneke & Preece (2003), the lurker –the passive user of Internet forums– is a role more than necessary for the good government and health of an online community. Beyond passivity, it is the lurker –and in our case, the slacktivist– who maintains the cohesion of the community, spreads its content by means of their minimal effort actions, acts at critical times and, above all, provides value to the community itself by filtering and critically reading the contents shared or generated in it. But, besides these issues, it is worth being noted that lurking or slacktivism are often, and as mentioned above, activities inherent to the new political activism and their different levels of engagement and participation. Different levels of engagement and participation

that change over time and people and according to their interests and needs, and letting people go through different stages of participation (Peña-López et al., 2013) thanks to the granular nature of the political actions and tasks at reach.

Moreover, and at the collective level, these slacktivists are the same ones that get involved in political actions outside of social networking sites (Ogilvy et al., 2011), providing cohesion to the group and a sense of collective identity. Indeed, theirs are specific actions that come to complement, not replace, other actions of political participation. More importantly, the *passive* visibility of these actions –as they appear in the activists' profiles on social networking sites– ends up providing these actions with a life on their own, making involvement in civic causes be spread and resulting in behavioral changes both at the individual level as in the social circle next to the citizen.

5. CASUAL POLITICS

But, as we have already stated, beyond the individual or collective points of view we believe that it is worth considering the slacktivism not from the point of view of the «couch activist», but from the point of view of the decision maker.

There is an affectionate tradition during election seasons where candidates pay a visit to city markets and civic center cafes to chat with the «common people», to get their pulse, to listen to their demands and needs. Once the election season is over, these hearings usually occur in reverse, namely, with strikes and street demonstrations. To the extent that markets and civic centre bars succeed in repeating the same longings and complaints, or to the extent that strikes and streets are filled up with citizens eager to be heard, issues end up entering the political and/or the public agenda, depending on whether the first step is performed by parties or by mass media.

We can approach slacktivism from its collective aspect and as a small part of a greater whole: as the peripheral portion of the political participation that happens simultaneously offline in the streets and online on social networking sites, highly involved and engaged, carefully documented and disseminated on the Net, totally extra-representative and decentralized, but with outward forms that emulate institutions. In this sense, slacktivism is not as important in relationship to the issuer –the one that just makes a click– but in relationship to the receiver, i.e. the institution that feels questioned or challenged by literally millions of micro-actions that are also, in essence, the echo of a compacted movement. A movement that, as it is not institutionalized, does not fall within our usual parameters to measure the impact of political participation: working hours «lost» by a strike, how many protesters in the street or the number of votes that changed sides in the following election.

We are warned by De Marco & Robles Morales (2012) of the «influence of institutional participation and the new forms of participation [and] that these tools can

facilitate the dissemination of political practices that in the 'real world' usually have less political relevance». Thus, tools that were not originally designed for political purposes manage their way in approaching the citizen to participate in politics, by chance, by accident, serendipitously.

If we recover Hibbing & Theiss-Morse's thesis, we can see that they draw an ideal «democratic arrangement in which decisions are made by neutral decision makers who do not require sustained input from the people in order to function» (Hibbing & Theiss-Morse, 2002). In this arrangement, citizens would have a preference for «stealth» processes that did not require much debate and even less controversy, delegating their responsibility in so-called «technocrats». The authors warn us, however, that the apparent lack of interest is not so. On the one hand because rather than a lack of interest in the *political space*, what we usually find is distrust or loss of hope. On the other hand, because there is palpable interest in the *political process*, in how decisions are made –regardless, again, of the will to engage in participation in the political space. This distinction between the political space –which raises distrust– and the political process –which raises genuine interest– is crucial.

Although we have already seen (Font et al., 2012) that these hypotheses have many edges, this preference for a stealth democracy would totally be in line with a casual way of doing politics, (1) totally informal and (2) based on constant microvotes (slacktivism) (3) around major topics (4) covered in large agorae (5) non-related to formal institutions and the different dynamics of representative politics.

Contradicting Hirschman (1970), we could say that in this choice for the extra-representative way and, especially, for its informal side, the notion of *exit* would not be so, but an *exit* towards *voice*. That is, the choice for extra-representative political participation would not be an exit from the democratic system, but a conscious choice to unleash one's voice as another kind of engagement. And this would be particularly relevant or consistent in an environment where loyalty would be greatly devalued by the rampant political disaffection that plagues many modern democracies.

In this train of thought, the arguments that Hirschman (1991) himself collected as used to counter major political changes –the perversity thesis, the futility thesis and the jeopardy thesis– serve to explain the opposition to slacktivism, especially if consideration as futile.

Notwithstanding, as we will try to point out below, this approach still is the one of an evolution of the political arena, and not the one that is witnessing a deep transformation of the system. On the other hand, it is the approach from the standpoint of view of someone who makes a redemptive click, and not from the standpoint of view of someone who should monitor, organize and infer from millions of data that are produced by all computer activity in real time, i.e. *Big Data*.

6. EMERGENT SYSTEMS AND PATTERN RECOGNITION

We can give yet another twist to the question of slacktivism from the point of view of the decision-maker and his vision of what is collective, aggregate. The huge amount of data that can now be handled now; the limited –or very limited– potential as a political action of one single click, which we can even take as an almost uninformed action that ignores most of its context; and the casual encounters and random coincidences between campaigns and collective promoters are but three of the assumptions or preconditions that Johnson (2001) handles when he speaks about ideal environments for emergent behaviors to take place. Emergent behaviors are understood as collective behaviors whose design was not embedded in the different actions taken at the individual level. They can also be understood as complex collective behaviors that take place by aggregating a good amount of simple individual behaviors. Before emergent systems, Johnson suggests using pattern recognition as a very powerful tool.

Although decisions based on data are not –or should not be– something new, it is undeniable that Information and Communication Technologies and, in particular, the phenomenon of big data, offer new opportunities of magnitudes previously unseen (Esty & Rushing, 2007). It is true that this approach has well-founded criticism due to the coldness of data, the deficiencies when capturing contexts, the over-simplification of reality and the definition itself of the problems we aim at addressing. Added to that, there are also some doubts about relevant aspects such as privacy or security (Morozov, 2013). However, we believe that between the end representing traditional institutionalized representative politics and the end of automated decision making by the data, there is ample leeway for institutional innovation and, especially, hybridization procedures. And there is, above all, a real possibility of taking actions (and data) from slacktivism as living indicators –in every possible meaning– and as citizens who are «voting with their feet» every day, unconsciously and even passively, and with the absence of bias that conscious or proactive action could imply (we are talking here about huge amounts of data difficult to tamper with).

Among the many existing cases that we can use to suggest an approach to slacktivism as big data for decision-making, we can highlight the recognition of patterns of behavior in mobility from the geolocation of mobile terminals (Frias-Martinez et al., 2010; Frias-Martinez & Virseda, 2013) or the use of Twitter to trace the evolution of infectious diseases and as activity levels associated with its spread (Signorini et al., 2011), an exercise that can get translated into very interesting projects like the Health Map[1].

In an area closer to the politics, seemingly trivial experiments like the one by the FloatingSheep collective and their geolocation of racist tweets in response to the re-

1 http://healthmap.org/en/

election of President Obama in the U.S.[2] may be evolved into the mapping of all types of hate speech[3], a most valuable resource with direct impact on awareness raising and policy-making in the field of human rights and risk of social exclusion.

If the case of mobility through call data/detail records (CDR), health-related tweets or hate speech give us a powerful tool for refining public policies –mobility, health or human rights, respectively– the move towards political preferences detection takes us out the scope of the Administration or the Government and squarely in the field of Democracy and Governance. And let us insist on this point: «The value does not lie in each individual fragment of news and information, but rather in the mental portrait created by a number of messages over a period of time» (Rieder, 2012).

Put in another way: the new extra-representative digital participation can be understood both as a movement –with particular and well-defined actions– and as a culture – with its ideology and its overlying political program. It is this ideology, shared values and implicit political program which can now be made explicit through the handling of huge amounts of data, pattern recognition and inference of emergent behaviors

And slacktivism –or the slacktivist– is but a tiny but also precious piece of this puzzle. Because it is to the extent that a critical mass is reached of minimal and volatile actions, or of easily influenced individuals, that it is indeed possible to roll the snowball of viral participation (Watts & Dodds, 2007). If, after that, we can add the possibility of characterizing large aggregates of individuals according to their online behavior (Kosinski et al., 2013), we can not only infer emerging political trends through the identification of patterns of behavior, but we can also approximate their representation in the total population. And this is a crucial leap forward in comparison with usual aggregation of preferences emerging from political surveys or even polls.

Slacktivism lies in between two new ways of understanding collective action and decision-making. On the one hand, new forms of extra-representative participation initiated by highly cohesive cores of activists (Peña-López et al., 2013) or social hackers (Ruiz de Querol & Kappler, 2013). On the other hand, politics far away from the traditional leadership from modern democracies and more focused on capacity building and fostering emancipatory values, encouraging the shift from objective choice to subjective choice, and from subjective choice towards effective choice (Welzel et al., 2003).

2 http://www.floatingsheep.org/2012/11/mapping-racist-tweets-in-response-to.html

3 http://www.floatingsheep.org/2013/05/hatemap.html

7. VINDICATING SLACKTIVISM

In our exposition we have tried to present slacktivism under the topic of the iceberg. While the floating part is what is visible to the eyes, this is but a small part that can make us lose the overall perspective, minimizing its importance, and leading us to wreck.

Our claim of slacktivism is not made from the individual's point of view: as we have already acknowledged, slacktivism is in truth often made of actions just barely committed in themselves and even –and most times– a mere sequence of data generated automatically and passively. In this sense, and from the point of view of activism, we do not only understand but do share the ill reputation of slacktivism as the most evil brother of political engagement.

But most of the foundations of slacktivism are under the surface. Beneath the surface of institutions and formal political participation underlie new political practices not only extra-representative, but as new as invisible to the radar of modern democracy shaped around the scientific revolution and the industrial revolution. These new forms of doing or taking part in politics, in decentralized but cohesive way, individually-led but institutionalized on its outer face, must necessarily enter into the equations of institutional politics, and slacktivism is one of its most powerful variables.

The vindication of slacktivism has to be done, thus, from institutional politics, bringing up the value of casual or informal politics that occur in the periphery of the new social movements, in frivolous but significant friction with traditional practices – and, as we have seen often complementing each other rather than in opposition. Strictly speaking, and this is a major point, we believe that slacktivism does not actually take place in the periphery of new social movements in the sense of something marginal, but in the sense of something that is actually part of the whole, as smoke is part of the fire. In this sense, slacktivism is not weak engagement, but just a part of the new digital toolbox of political participation, which sometimes is more committed and sometimes is not, but it does not define the activist because, as evidence shows, we are facing a new kind of activism which is multimedia, crossmedia and transmedia. That is, slacktivism does not define the activist, but, in general, the activist individually uses slacktivism as yet another tool to reinforce a much more comprehensive and collective strategy of political engagement.

Before this landscape, we consider that monitoring, political pattern recognition, inference of tacit ideologies and proposals, or real-time politics are –or should be– new approaches to political action that are now not only possible but desirable. Setting aside this new toolbox, so much needed for understanding the new digital citizenship, is a sign of political stagnation as slacktivism is a sign that something is moving in society.

8. BIBLIOGRAPHY

Anduiza, E., Cristancho, C. & Cantijoch, M. (2012). «La exposición a información política a través de Internet». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 673-688. Berkeley: Berkeley Electronic Press. Retrieved February 14, 2013 from http://arbor.revistas.csic.es/index.php/arbor/article/viewFile/1493/1504

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven: Yale University Press.

Borge, R. & Cardenal, A.S. (2012). «Surfing the Net: A Pathway to Participation for the Politically Uninterested?». In *Policy & Internet, 3* (1). Berkeley: Berkeley Electronic Press. Retrieved April 01, 2011 from http://www.psocommons.org/policyandinternet/vol3/iss1/art3

Breindl, Y. & Gustafsson, N. (2011). «Leetocracy: Networked Political Activism or the Continuation of Elitism in Competitive Democracy». In Araya, D., Breindl, Y. & Houghton, T.J. (Eds.), *Nexus: New Intersections in Internet Research, Chapter 9*, 193-212. New York: Peter Lang.

Breindl, Y. (2012). «The Dynamics of Participation and Organisation in European Digital Rights Campaigning». In *eJournal of eDemocracy and Open Government, 4* (1), 24-44. Krems: Danube-University Krems. Retrieved March 13, 2013 from http://www.jedem.org/article/view/96

Cantijoch, M. (2009). *Reinforcement and mobilization: the influence of the Internet on different types of political participation*. Prepared for the seminar Citizen Politics: Are the New Media Reshaping Political Engagement? Barcelona, May 28th-30th 2009. Barcelona: IGOP.

Castells, M. (2009). *Communication power*. Cambridge: Oxford University Press.

Christensen, H.S. (2011). «Political activities on the Internet: Slacktivism or political participation by other means?». In *First Monday, February 2011, 16* (2). [online]: First Monday. Retrieved November 29, 2012 from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3336/2767

Colombo, C., Galais, C. & Gallego, A. (2012). «El uso de Internet y las actitudes políticas. Datos cuantitativos y cualitativos de España». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 751-766. Berkeley: Berkeley Electronic Press. Retrieved February 14, 2013 from http://arbor.revistas.csic.es/index.php/arbor/article/viewFile/1498/1509

De Marco, S. & Robles Morales, J.M. (2012). «Uso de los blogs políticos: análisis de algunos factores determinantes». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 689-705. Berkeley: Berkeley Electronic Press. Retrieved September 14, 2012 from http://arbor.revistas.csic.es/index.php/arbor/article/view/1494

Esty, D.C. & Rushing, R. (2007). *Governing by the Numbers: The Promise of Data-Driven Policymaking in the Information Age*. Washington, DC: Center for American Progress. Retrieved May 20, 2013 from http://www.americanprogress.org/wp-content/uploads/issues/2007/04/pdf/data_driven_policy_report.pdf

Fernández Prados, J.S. (2012). «Ciberactivismo: conceptualización, hipótesis y medida». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 631-639. Berkeley: Berkeley Electronic Press. Retrieved September 14, 2012 from http://arbor.revistas.csic.es/index.php/arbor/article/view/1490

Font, J., Navarro, C., Wojcieszak, M. & Alarcón, P. (2012). *¿»Democracia sigilosa» en España? Preferencias de la ciudadanía española sobre las formas de decisión política y sus factores explicativos*. Opiniones y actidudes, nº71. Madrid: Centro de Investigaciones Sociológicas. Retrieved December 03, 2012 from http://libreria.cis.es/static/pdf/OA71acc.pdf

Frias-Martinez, V., Virseda, J., Rubio, A. & Frias-Martinez, E. (2010). «Towards Large Scale Technology Impact Analyses: Automatic Residential Localization from Mobile Phone-Call Data». In *Proceedings of ICTD 2010*. 4th ACM/IEEE International Conference on Information and Communication Technologies and Development. London: IEEE. Retrieved May 17, 2013 from http://www.gg.rhul.ac.uk/ict4d/ictd2010/posters/ICTD2010 Frias-Martinez et al.pdf

Frias-Martinez, V. & Virseda, J. (2013). «Cell Phone Analytics: Scaling Human Behavior Studies into the Millions». In *Information Technologies and International Development, 9* (2 ICTD2012 Special Issue), 35-50. Cambridge: MIT Press. Retrieved June 11, 2013 from http://itidjournal.org/index.php/itid/article/view/1051

Fuster, M. & Subirats, J. (2012). «Crisis de representación y de participación. ¿son las comunidades virtuales nuevas formas de agregación y participación ciudadana?». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 641-656. Berkeley: Berkeley Electronic Press. Retrieved September 14, 2012 from http://arbor.revistas.csic.es/index.php/arbor/article/view/1491

Hibbing, J.R. & Theiss-Morse, E. (2002). *Stealth Democracy: Americans' Beliefs About How Government Should Work*. New York: Cambridge University Press.

Himanen, P. (2003). *L'ètica hacker i l'esperit de l'era de la informació*. Barcelona: Editorial UOC.

Hirschman, A.O. (1970). *Exit, Voice, and Loyalty*. Cambridge: Harvard University Press.

Hirschman, A.O. (1991). *The Rhetoric of Reaction*. Cambridge: The Belknap Press of Harvard University Press.

Horrigan, J.B., Garrett, R.K. & Resnick, P. (2004). *The internet and democratic debate*. Washington, DC: Pew Internet & American Life Project. Retrieved Fe-

bruary 14, 2013 from http://www.pewtrusts.org/uploadedFiles/wwwpewtrustsorg/Reports/Society_and_the_Internet/Pew_Internet_political_info_report_1004.pdf

Inglehart, R. (2008). «Changing Values among Western Publics from 1970 to 2006». In *West European Politics, January–March 2008, 31* (1-2), 130–146. London: Routledge. Retrieved February 12, 2013 from http://www.worldvaluessurvey.org/wvs/articles/folder_published/publication_559/files/values_1970-2006.pdf

Johnson, S. (2001). *Emergence. The connected lives of Ants, Brains, Cities and Software*. London: Penguin Books.

Kelly, J., Fisher, D. & Smith, M. (2005). *Debate, Division, and Diversity: Political Discourse Networks in USENET Newsgroups*. Paper prepared for the Online Deliberation Conference 2005. Palo Alto: Stanford University. Retrieved July 10, 2007 from http://www.coi.columbia.edu/pdf/kelly_fisher_smith_ddd.pdf

Kelly, J. (2008). *Pride of Place: Mainstream Media and the Networked Public Sphere*. Media Re:public Side Papers. Cambridge: Berkman Center for Internet and Society at Harvard University. Retrieved December 20, 2008 from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Pride of Place_MR.pdf

Kosinski, M., Stillwell, D. & Graepel, T. (2013). *Private traits and attributes are predictable from digital records of human behavior*. Washington, DC: Stanford University's HighWire Press. Retrieved March 12, 2013 from http://www.pnas.org/cgi/doi/10.1073/pnas.1218772110

Lanier, J. (2010). *You are Not a Gadget: A Manifesto*. London: Allen Lane.

Martínez Roldán, S. (2011). *Movimiento 15M: construcción del espacio urbano a través de la acción de las Multitudes Inteligentes*. Barcelona: UOC. Retrieved July 26, 2011 from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8582/1/smartinezrol_TFM_0711.pdf

Morozov, E. (2011). *The Net Delusion. The Dark Side of Internet Freedom*. New York: Public Affairs.

Morozov, E. (2013). *To save everything, click here. The folly of technologycal solutionism*. New York: PublicAffairs.

Mossberger, K., Tolbert, C.J. & McNeal, R.S. (2008). *Digital Citizenship. The Internet, society and participation*. Cambridge: The MIT Press.

Negroponte, N. (1995). *Being Digital*. London: Hodder & Stoughton.

Nonneke, B. & Preece, J. (2003). «Silent Participants: Getting to Know Lurkers Better». In Lueg, C. & Fisher, D. (Eds.), *From Usenet to CoWebs: Interacting with Social Information Spaces, Chapter 6*, 110-132. London: Springer.

Norris, P. (2001). *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge: Cambridge University Press.

Noveck, B.S. (2005). «A democracy of groups». In *First Monday, 10* (11). [online]: First Monday. Retrieved June 14, 2009 from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1289/1209

Obar, J.A., Zube, P. & Lampe, C. (2012). «Advocacy 2.0: An Analysis of How Advocacy Groups in the United States Perceive and Use Social Media as Tools for Facilitating Civic Engagement and Collective Action». In *Journal of Information Policy, 2*, 1-25. [online]: Pennsylvania State University. Retrieved December 21, 2012 from http://jip.vmhost.psu.edu/ojs/index.php/jip/article/view/80

Ogilvy Public Relations Worldwide & Center for Social Impact Communication at Georgetown University (2011). *Dynamics of Cause Engagement*. Arlington: Georgetown University. Retrieved November 29, 2012 from http://csic.georgetown.edu/research/215767.html

Padró-Solanet, A. (2010). *Internet and Votes: The Impact of New ICTs in the 2008 Spanish Parliamentary Elections*. Communication presented at the Internet, Politics, Policy 2010: An Impact Assessment conference, 16-17 September 2010. Oxford: Oxford Internet Institute.

Peña-López, I. (2011). «The disempowering Goverati: e-Aristocrats or the Delusion of e-Democracy». In *eJournal of eDemocracy and Open Government, 3* (1), 1-21. Krems: Danube-University Krems. Retrieved May 07, 2011 from http://www.jedem.org/article/view/50

Peña-López, I., Congosto, M. & Aragón, P. (2013). «Spanish Indignados and the evolution of 15M: towards networked para-institutions». In Balcells, J., Cerrillo-i-Martínez, A., Peguera, M., Peña-López, I., Pifarré, M.J., & Vilasau, M. (coords.) (2013). Big Data: Challenges and Opportunities. Proceedings of the 9th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 25-26 June, 2013. Barcelona: UOC-Huygens Editorial.

Rainie, L., Purcell, K. & Smith, A. (2011). *The social side of the internet*. Washington, DC: Pew Internet & American Life Project. Retrieved January 20, 2011 from http://www.pewinternet.org/Reports/2011/The-Social-Side-of-the-Internet.aspx

Rieder, B. (2012). «The refraction chamber: Twitter as sphere and network». In *First Monday, November 2012, 17* (11). [online]: First Monday. Retrieved November 21, 2012 from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/4199/3359

Robles Morales, J.M., Molina Molina, Ó. & De Marco, S. (2012). «Participación política digital y brech digital política en España. Un estudio de las desigualdades digitales». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 795-810. Berkeley: Berkeley Electronic Press. Retrieved September 14, 2012 from http://arbor.revistas.csic.es/index.php/arbor/article/view/1501

Ruiz de Querol, R. & Kappler, K. (2013). *Looking for the Social Hackers*. [mimeo].

Sádaba, I. (2012). «Participación política digital y brech digital política en España. Un estudio de las desigualdades digitales». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 781-794. Berkeley: Berkeley Electronic Press. Retrieved September 14, 2012 from http://arbor.revistas.csic.es/index.php/arbor/article/view/1500

Signorini, A., Segre, A.M. & Polgreen, P.M. (2011). «The Use of Twitter to Track Levels of Disease Activity and Public Concern in the U.S. during the Influenza A H1N1 Pandemic». In *PLOS ONE, 6* (5), e19467. San Francisco: Public Library of Science. Retrieved May 17, 2013 from http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0019467

Smith, A. (2013). *Civic Engagement in the Digital Age*. Washington, D.C.: Pew Internet & American Life Project. Retrieved April 25, 2013 from http://pewinternet.org/Reports/2013/Civic-Engagement.aspx

Tichenor, P.J., Donohue, G.A. & Olien, C.N. (1970). «Mass media flow and differential growth in knowledge». In *Public Opinion Quarterly, 34* (2), 159 - 170. Oxford: Oxford University Press.

Tiebout, C.M. (1956). «A Pure Theory of Local Expenditures». In *Journal of Political Economy, 64* (5), 416-424. Chicago: The University of Chicago Press.

Watts, D.J. & Dodds, P.S. (2007). *Influentials, Networks, and Public Opinion Formation*. Madison: University of Wisconsin.

Welzel, C., Inglehart, R. & Klingemann, H. (2003). «The theory of human development: A cross-cultural analysis». In *European Journal of Political Research, 42* (3), 341-379. Oxford: Blackwell. Retrieved April 20, 2007 from http://www.blackwell-synergy.com/doi/pdf/10.1111/1475-6765.00086

COMUNICACIONES SOBRE MOVIMIENTOS SOCIALES

SPANISH INDIGNADOS AND THE EVOLUTION OF 15M: TOWARDS NETWORKED PARA-INSTITUTIONS

Ismael Peña-López
Professor at the School of Law and Political Science of the Open University of Catalonia

Mariluz Congosto
Researcher at Universidad Carlos III de Madrid

Pablo Aragón
Researcher at Barcelona Media Foundation

ABSTRACT: The Arab Spring, the Spanish *Indignados*, the Occupy Movement (#jan25, #egypt, #arabspring, #15M, #29S, #occupywallst, #ows, #15O). In the last months the world has witnessed the emergence of networked citizen politics: besides institutions, but many times mimicking their nature; unlike traditional citizen movements, but very much alike in their essence. Networked citizen politics, characterized by decentralization, swarm-like action and an intensive use of Information and Communication Technologies, have been having a starring role in world-wide protests and movements, most of the times overtaking and circumventing the actions of governments, parliaments, political parties, labour unions, non-governmental organizations, mass media and all kinds of formal democratic institutions.

Taking the case of Spanish *Indignados*, the aim of this paper is to analyse the nature of networked citizen politics as an extra-representational kind of political participation after the usage of Twitter that has been made around the so called 15M movement. Firstly, users will be characterized, including a description on how movements propagate one onto another. Secondly, the paper will see what are the bonds between networked citizen movements and formal democratic institutions, how do they relate one with each other, especially the movements with political parties and mass media. It will also emphasize how networked citizen politics may use similar tools as the so mentioned Politics 2.0, but with very different purposes and, thus, results, and what is the result of the two clashing approaches.

Our analysis will show that different movements –i.e. 15M and 25S– act as a continuum for networked citizen politics that use the Internet as the support for new institutionalisms, and despite the lack of traditional organizations, people, practices and ideas are shared and used as foundations for further action. Notwithstanding, there almost is no inter-institutional dialogue with exceptions related with individuals belonging to minor and left-wing parties.

KEYWORDS: 15M, spanishrevolution, indignados, twitter, social network analysis, institutional politics.

1. INTRODUCTION

The Spring of 2011 will appear in the books of History as a period of worldwide unrest, revolts, uprisings and even revolutions, most of them lasting or replicating until

Fall or just left unended. In Spain, the Spanish *Indignados* took the *plazas* (squares) and camped on them the night of May 15th and for several weeks. The movement quickly spread all over the country, being Information and Communication Technologies (ICTs) crucial instruments for coordination, communication and (political) deliberation. Amongst all these technologies, Twitter played an important role both within the movement and, this is our guess, outside the movement, to get in touch with other citizen organizations, media, and formal democratic institutions: members of the parliament and political parties at large.

One of the main questions that have arisen have been whether these movements are as emergent as they seem, or have instead been designed, promoted, fostered and led by political parties or civil society organizations.

There is quite a lot of evidence that offline political activism is much related with online political activism, and that being online is also a good gateway for political participation. In this sense, Rainie et al. (2011) or the Institute for Politics, Democracy & the Internet (2004) have measured the strong relationship between being an online influential or an online politically committed person and their own offline political activity.

What we do not know is whether people that are politically active in their communities do the same thing once online, or if it is just the contrary. In this train of thought, Katz et al. (2001) found that «Internet users were more likely than non-users to engage in traditional political activity in the 1996 general election». This is a statement that could be difficult to validate if we were to look only at traditional parties, because as Norris & Curtice (2006) notice «the online population is most predisposed to engage in cause-oriented forms of activism, characteristic of petitioning, demonstrating, and contacting the media over single-issue politics and civic-oriented activities, such as belonging to voluntary associations and community organizations». And that is the very essence of the *Indignados* or 15M movement in Spain. Self-expression and other post-materialist values could be taking up with other survival-centered values, leading us to an intergenerational value change (Inglehart, 2008).

That said, if there is a change of values going hand in hand with a change in participation strategies, can it be stated that the *Indignados* movement, along others of the kind, are shifting or pushing political participation in the field of extra-representational participation (Cantijoch, 2005)? If that is so, how are democratic institutions such as governments, parliaments or political parties dialoguing with these extra-representational political ways of participation? What about media?

What is already a fact is that «technology [is enabling] more effective forms of collective action» (Noveck, 2005) and that it would be highly advisable to «explore ways to structure the law to defer political and legal decision-making downward to decentralized group-based decision-making».

Our hypothesis in this paper is that we have found, once again, evidence of new ways of extra-representational participation, a way of political participation that is a growing. Notwithstanding, there seem to be increasingly stronger liaisons between these movements and political parties –especially minor and left-wing ones– and media, the later intermediating between social movements and more disconnected institutions (governments, parliaments and major and right-wing parties). On the other hand, this dialogue is possible partly because of the process of pseudo-institutionalization of social movements: if we trace the evolution of such movements, despite their decentralization and lack of visible leadership, they show an emergent characteristic of flocking together and a behaviour that can be identified with formal institutions' from an outsider's point of view

2. FRAMEWORK

2.1. Internet and politics

Our first statement about Internet and politics or political participation and engagement is that they have a positive relationship. Borge & Cardenal (2012) found that «use of the Internet has a direct effect on participation independently of motivation». In other words, in addition to the set reasons that cause political participation, the Internet itself is increasing this willingness to participate online. In this sense, the Internet reinforces online participation.

This is a confirmation of other authors that dismissed former suspicion about the Internet alienating and isolating people from their community in general, and from politics in particular. On the contrary, «being involved in effortless political activities online does not replace traditional forms of participation, if anything, they reinforce off–line engagement» (Christensen, 2011).

Of course being online political participation requires a set of skills and capabilities (Peña-López, 2011) that does not only enable citizens to participate online, but that actually increase the probability of them doing it (Borge & Cardenal, 2012).

It is worth noticing, though, that even if the Internet has a positive impact on online participation and that this online participation correlates with offline participation, this does not necessarily mean that offline participation has to be understood as usual. In fact, it has already been found that a higher use of the Internet is not related with being more interested in a political campaign and not even be more prone to following official cyberpolitics (Sampedro et al., 2012). Online campaigns, thus, would be addressed not to the whole of the online population, but to the ones that have an influence, both online and offline.

Indeed, major media have not been replaced by online or independent media, and still have enormous influence in political matters, both online and offline (Sampedro et al., 2012). This is but yet another confirmation of the knowledge gap hypothesis

(Tichenor et al., 1970) as it has also been found by Anduiza et al. (2009), who show how the Internet is a knowledge gap amplifier when analyzing general elections in Spain. Nevertheless, the authors also find that a certain degree of serendipity is actually working: besides the negative impact of the Internet on equity of access to information and participation, it is also true that the Internet exposes people to politics in more ways and intensity than compared to offline channels. A consequence of that is that despite the cognitive gap increasing due to the impact of the Internet, the motivational gap actually decreases. In other words, the knowledge gap closes between politically interested citizens and those not interested.

Related to that, Cantijoch (2009) also analyzed the effects of the Internet on reinforcement and mobilization. She found, in addition to Aunduiza et al.'s (2009) findings that «institutionalised individuals are similarly increasing their likelihood of engaging in [online] activities in a mobilisation process», which confirms the mobilization hypothesis. The most interesting aspect to us, though, is how she also found a complementary impact to mobilization and how Internet would reinforce «pre-existing proclivity to engage in extra-representational modes of participation».

2.2. Spanish users and politics on the Internet

In addition to what has already been said, there are two main characteristics of Spanish online politics that still. Of course, there are exceptions to the general rule that we are presenting in the following lines –this research is partly about this issue– and the evolution of the Internet, Internet usage and online politics still is changing at a quick pace. But both characteristics are quite generally spread and will contribute in understanding the results of this research.

On the one hand, and put in a very simple way, citizens are using intensively the Internet and most especially the so-called web 2.0 and social media platforms and applications, while institutions are not (Peña-López, 2011). This is not exclusive from the political arena (it can be found in the many other institutions) but being politics such a conversational issue, it makes the question even more relevant. This non-usage of the web 2.0 or social media should not be understood as non-usage «at all», but as a mere technical usage without the underlying change of philosophy or ethos. For instance, when it comes to political blogging, it can be found that it is used in very unidirectional ways, campaign based and mainly for spreading the content from the party (Criado & Martínez Fuentes, 2009).

This subversion of the enormous potential of the Internet and the aim to control the message has created a sort of division between formal and informal online politics. If we add the rejection to formal politics, the increasing shift towards extra-representational participation and the motivational push of the Internet, it is not surprising that there is «a relatively small but statistically significant effect of political information exposure in the internet in the increase of the vote towards minor parties and the abstention»

(Padró-Solanet, 2010). In other words: a growing minority of Spaniards is moving away from formal politics partly pushed out by an intensive use of the Internet.

The second characteristic of online politics in Spain is that in general, socio-demographic characteristics explain most of the Internet use and online political activities among Spaniards (Robles Morales, 2008). But, regarding political ideology or positioning, Spanish Internet users are, significantly, more prone to be left wing than the average of the population (Robles Morales, 2008). This aspect has no explanation in classical theories –such as social class– and can only be indirectly explained by factors that we have already mentioned.

2.3. Twitter

If online politics are a reality in Spain –with the caveats noted above– Twitter is, arguably, already playing a major role in general elections in Spain (Izquierdo Labella, 2012). There are, though, some appreciations to be made on how Twitter is being used in politics in general and in Spanish politics in particular.

On the one hand, Twitter is becoming an easy, cheap and over all quick space where to broadcast opinion, unrest and concentrations in real time. In other words, there may not be «Twitter revolutions» but revolutions are definitely tweeted (Lotan, et al. (2011).

Besides coverage and broadcasting, Twitter is being useful to classify and concentrate users and their attention around specific topics. These topics are usually fed by mainstream media which passes it «to the masses indirectly via a diffuse intermediate layer of opinion leaders» (Wu, 2011).

The debate whether these flocks of people around topics are of the same feather is surely the most interesting part of it all. Wu (2011) warns about the risks of high levels of homophily being very high, as the classification of topics and the concentration around them is made by the users themselves, as it is them who explicitly opt-in who to follow (Wu, 2011). On the other hand, Kelly (2005) leaves an open door to some degree of ideological or political serendipity, as the openness of virtual spaces enables all kind of dialogues and «a range of policy preferences and ideological groundings –and they talk to each other».

In the case of Spain, Guadián Orta et al. (2012) have shown that the relationship between the citizen and the message actually works in both ways. On the one hand, an emergent social network is dynamically created around a specific topic, based on who is talking about it, who is following it, who replies or who forwards the message. On the other hand, the very message is shaped by the social network and its influence on it. At the end, message and network make up an *ad hoc* set that evolves together in time.

2.4. 15M

In a similar way, the *indignados* movement began with a call to camp on Puerta del Sol, a centric square in Madrid, on 15 May 2011 (Alcazan et al., 2012), just a week be-

fore the municipal elections. «15M demonstrators were younger, more educated [and] more likely to be women and unemployed» (Anduiza, Cristancho & Sabucedo; 2012). There also was a strong mobilization effect that brought onto the streets people that did not use to participate in demonstrations. The movement called for «real democracy, now» and in many cases asked for not voting major parties. One of the main characteristics of the movement was «their decentralized structure, based on coalitions of smaller organizations» (González-Bailón et al., 2011), with its back against political parties and, most of the times, against labour unions too.

Anduiza, Martín & Mateos (2012) characterized the participants in the 15M camps as having higher levels of political competence, deeply politicized ideals, and low levels of trust in institutions (especially political parties). In their analysis, they differentiated between non-sympathizers to the movement, sympathizers that did not participate and participants. And although still a preliminary analysis, their conclusions were that participants ended up voting more in the general elections of 20 November 2011, and that their vote went to minor parties, with a certain bias to the left wing.

Unlike other demonstrations, physical and virtual spaces, what happened in the plazas and what happened on the internet interacted and fed each other space with information, coordination and a sense of collective identity. Just like unrests in the Arab Spring, the hybridization of the virtual-urban space was crucial for the movement (Martínez Roldán, 2011; Castells, 2012). And Twitter played a major role in this hybridization.

3. EXTRA-REPRESENTATION OR A PROCESS OF INSTITUTIONALIZATION?

3.1. Research questions

It is relevant to know how the movements evolved along time, especially focusing on a double issue or question: did they dissolve or maintained after time, and would they become institution-like social structures or, on the contrary, would they maintain their extra-representational forms, based on networks or platforms.

There are, thus, two group of research questions that we face in this research: on the one hand, their characteristics –both individually and collectively– and how did these evolve along time; on the other hand, how did they relate, as a group, with other groups, especially institutions. In other words, we want to analyze their inner and their outer structure.

Regarding the former, we want to characterize the users: who they are, their gender, their socio-economic status and professional and political profile; what typologies can be drawn after them; what was their relationship with the territory, and be able to tell whether this is a urban phenomenon as most other industrial movements.

Concerning their evolution, we will analyze the movement at three moments in time: during 15 May 2011 (15 May) and the following days; during its first anniversary and the global movement of 12 May 2012 (12M15M); and during the events of 25 September 2012 (25S) where some influential actors from the movement lay siege in front of the Spanish Parliament until the general strike of 29 September (29S). We want to be able to tell how other citizen joined the *indignados* in their camps. We are interested in seeing the thread that goes through these three moments in time, how the different groups remained or changed, who where the long-term participants and, most important, why.

Regarding the second issue related with the relationships with other institutions (parties, media, labour unions), we want to know whether there was any contact between this kind of extra-representative politics and political institutions, and how did it evolve. Moreover, our intention is also to tell the capability of these movements to mobilize the citizenry compared to that of institutional politics. Summing up the previous questions, we would like to describe the relationships between the 15M and 29S and institutional politics, whether they share in common topics, liaisons, spaces. For instance, what was the role of media in telling the story and sharing viewpoints.

3.2. Hypotheses

Our hypotheses are as follows:

- H1: Extra-representative movements like the 15M, 12M15M, 25S or 29S are initiated by gathering a critical mass on social networking sites and evolve, on the outside, into a para-institution, while they keep an emergent and decentralized network-like structure on the inside.
- H2: Unlike institutions, that have a usually exclusive membership, citizen networks create para-institutions that share members among them.
- H3: The dialogue between political institutions and network para-institutions is weak, but existing, and concentrates on the left-side of the political arena.
- H4: When dialogue is non-existing, mass media act as the channel through which political institutions (normally on the right) and network para-institutions speak with each other.
- H5: Dialogue and lack of tension smoothes online participation. Lack of dialogue and tension sparks participation and boosts it beyond representational participation.

4. METHODOLOGY

To approach the phenomenon of the 15M, we analyse the messages that were sent on the Twitter social networking site. The election of the tool is not in the sense that the tool caused, framed or even explained the movement –a critique that Sádaba (2012)

raises– but in the sense that «the revolutions were tweeted» used by Lotan et al. (2011), as we will actually prove.

4.1. Data

Data were extracted from Twitter's API[1] which provides information of the time and space coordinates of each tweet, information on the sender (name and alias, bio), followers and friends. Table 1 shows the interval of time, selected hashtags, number of tweets and number of users for the three data sets.

Data set	Date of capture (from / until)	monitored words	Tweets	Users
15M	13-may-2011/ 31-may-2011	#15M, 15-M, #democraciarealya, #tomalacalle, #Nolesvotes, #spanishrevolution, #acampadasol, #acampadabcn, #indignados, #notenemosmiedo, #nonosvamos, #yeswecamp	1,444,051	181,146
12M-15M	01-may-2012 / 31-may-2012	#12M15M, #12M-15M, #12M, #15M, 15-M, 12-M, #spanishrevolution, #acampadasol, #acampadabcn, #indignados, #PrimaveraGlobal, #TomaLaCalle, #AnonOps, #hagamoscomoenislandia, #YoVoy12M, #desalojoSol, #volvemosalas5, #12mglobal, 14mMad, #Feliz15m, #Es15M	539,642	110,808
25S	16-aug-2012 / 31-oct-2012	25S, #25S, asalto al congreso,@ ocupaelcongreso, #ocupaelcongreso, ocupa el congreso, #tomaelcongreso, toma el congreso, 29-S, 29S, #29S, #voces25S, #vamos29S	1,394,114	289,001

Table 1: Data sets: hashtags

4.2. Demographical characterization

The policy of Twitter establishes that only a username and an email address are required. Some users complete their profile with their name, location, a brief biography and their website. We use these metadata to infer the attributes listed in Table 2.

1 https://dev.twitter.com/docs/streaming-apis/streams/public

Attribute	Inferred from	Complementary data
Gender	Name	Spanish Institute of Statistics (INE), male/female names[2]
Geography: Location	Location	Complemented by autonomous community and province after INE's table of municipalities and provinces[3]
Geography: Urban vs. local	Location	Madrid, Barcelona, Valencia, Sevilla, Bilbao, San Sebastián, A Coruña, Granada, Málaga, Salamanca, Valladolid are considered as urban. Rest as local.
Occupation level	Description	Classified as Manager-Executive, Professional, Support staff, Manual worker, Student
Tribe	Users	Classified by the authors after the user list as: • **Activists** (acampada, dry, pah, 25s) • **Media** • **Politicians** (pp, psoe, iunida, upyd, equo, ciu, erc, icv, compromis, pirata) • **Labour Unions** (ccoo, ugt).
Join	Timestamp	15M: Origin: May 13-14 Early: May 15-16 Boom: May 17-25 Late: May 26-31 25S: Origin: August 16-18 Early: August 19-September 24 Boom: September 25-30 Late: October 1-31

Table 2: Inferred attributes [23]

4.3. Evolution of the movements

To understand the evolution of the 15M movement through its information diffusion patterns, we study separately the different stages of the events, labeled as *Origin*, *Early*, *Boom* and *Late*. We denote as $V^r=\{v^r_1,\dots ,v^r_n\}$ all users that retweeted a user or were retweeted by a user at least once in the corresponding dataset of tweets. Then, we define a graph $G^r=G^r(V^r,E^r)$ comprising a set V^r of nodes and a set E^r of edges. There is an edge e^r_{ij} that connects user v^r_i with v^r_j if user v^r_i retweeted user v^r_j. Finally, we assign weight w^r_{ij} to every edge e^r_{ij} which is the number of times user v^r_i mentioned user v^r_j in the corresponding stage.

2 http://www.ine.es/daco/daco42/nombyapel/nombres_por_edad_media.xls

3 http://www.ine.es/jaxi/menu.do?type=pcaxis&path=/t20/e245/codmun&file=inebase

4.4. Relationship between the 15M and 29S and institutional politics

In order to analyse the relationship between the 15M movement, the political institutions and media, we generate graphs for the three periods: 15M, 12M15M and 25s. These graphs follows the same method that we defined in the above subsection but establishing edges between users based on mentions instead of retweets.

To quantify the influence of the tribes in each graph, through their connectivity, we use the k-core decomposition (Seidman, 1983) based on the in-degree of the nodes. Then, we group the k-index values of the users that form each tribe for computing the average and maximum value and the standard deviation.

Additionally, to understand the relationship between the tribes we remove the nodes which are not part of the pre-defined tribes and their edges. Then, we collapse the nodes which belong to the same tribe in super-nodes, one per tribe. Therefore, the edges of these new nodes express the mentions between users that form the adjacent tribes of an edge. We also remove the edges with a weight lower than 10 to ignore anecdotic interactions. Finally, we use the Louvain method (Blondel et al., 2008) for community detection in these new graphs and characterize the interactions between tribes at a macro-level.

4.4.1. K-index decomposition

K-core decomposition is a technique for the evaluation of potential influencers in different social networks (Kitsak et al., 2010). The k-core of a graph is the maximal sub-graph in which each vertex is adjacent to at least k other nodes of the sub-graph. In directed graphs as the ones of this study, then there exist two different k-core decompositions (for in- and out-degrees). A graph's node has a k-index equals to k if it belongs to the k-core but not to the (k +1)-core.

4.4.2. Community detection

The Louvain method is a greedy optimization algorithm to detect communities of nodes, also called modules, based in the modularity of the graph. The modularity is a function that quantifies a particular division of a graph into communities and obtains high values in graphs with dense edges between the nodes within communities and sparse edges between nodes in different communities.

5. RESULTS[4]

We analyse the behavioural patterns that emerge along time between and within the three events: 15M, its first anniversary (12M15M) and the events of the 25S.

5.1. Data: participation of users in the events

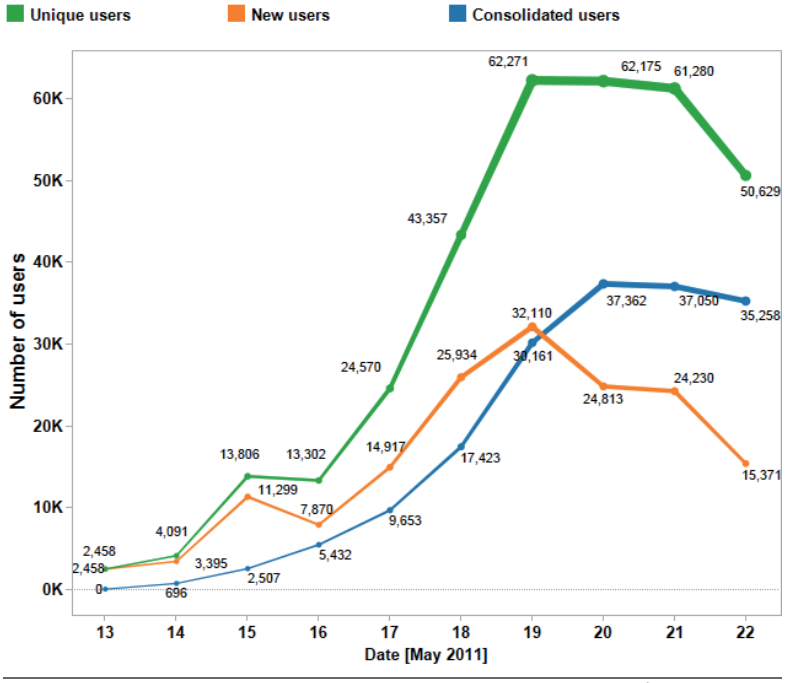


Figure 1: Participation of the users in 15M

First, we observe in Figure 1 that the 15m broke the general trend of immediateness of social movements: expectation and interaction lasted for days and even transcended one event into the other one[5]. Indeed, the number of total users on 15M (37,362) does not differ a lot from the estimated number of demonstrators on the streets. Thus, even if the movement was born online, it definitely went offline and Twitter acted as a communication platform between the participants.

4 The whole set of figures in higher resolution can be accessed at http://www.barriblog.com/idp2013/

5 Evolution of 12M-15M (http://t-hoarder.com/12M-15M/) and 25S (http://t-hoarder.com/25S/).

Regarding coincidence between the three events, Figure 2 confirms the volatility of Twitter in the political engagement of users in several periods. Only thee 3.22% of all participants took place in the three events, 16.30% participated in at least two of them and 83.70% only participated in one of them, following Pareto's Principle of participation.

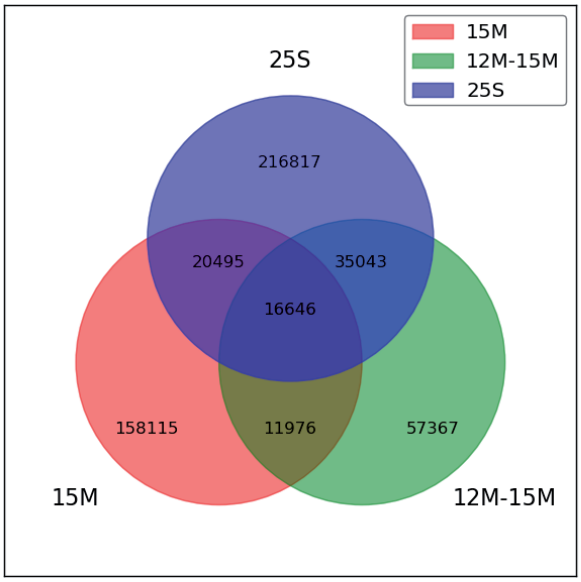
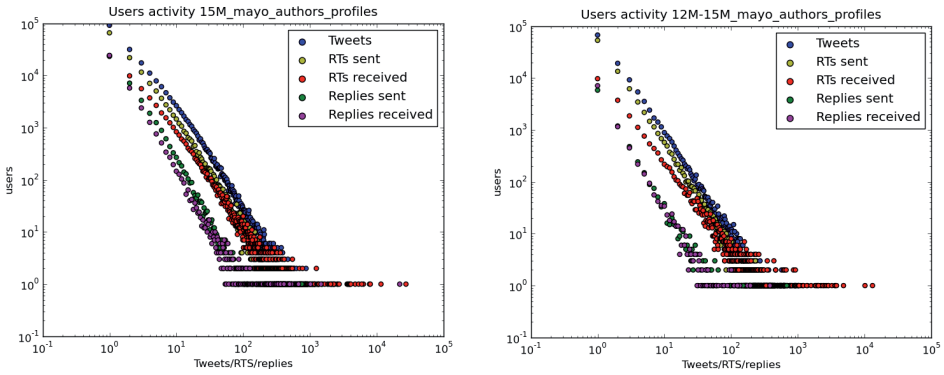


Figure 2: Participation of the users in the three events

Besides the different events, Figure 3 shows a Pareto's Power Law in the tweets, retweets and replies distributed by users. In other words, there is a low number of users that are very active while the rest shows much less activity. From now on, we denote as *Core* the subset of users that participated in the three events.



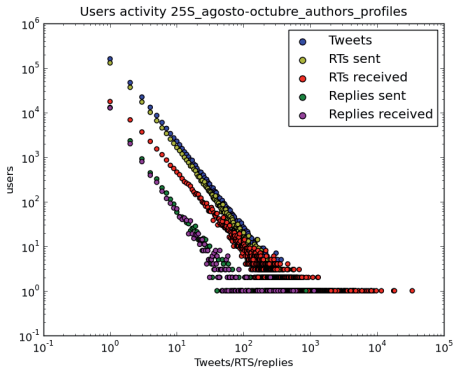


Figure 3: Tweets, retweets and replies by users during 15M, 12M15M and 25S

5.2. Demographical characterization

In this subsection, characterize the users who tweeted during the 15M, 12M15M and/or 25S events in terms of geographical location, gender, occupation, role and tribe.

5.2.1. Gender

Twitter provides no data for gender, and it has to be guessed by given names stated by users in their user names. Gender has been identified for about two-thirds of users. From 15M to 25S the percentage difference between men and women was cut by ten points. The Core group was mostly male.

Gender	Core %	15M %	12M15M %	25S %
Men	43.88	43.92	38.51	37.93
Women	23.12	23.78	26.74	27.44
Unknow	33	32.3	34.75	34.63

Table 3: Distribution of the users by gender

5.2.2. Geography

The geographical origin of the tweets was identified in almost a half of them, enough to know their distribution in the three events. Madrid, Catalonia, Andalusia and Valencia generated most of the messages. From 15M to 25S the percentage of tweets fell in the largest cities (Madrid and Barcelona) and instead the number of users with an unknown location increased. It is worth noting that people from the *Core* group provide their location most frequently (more than half, 53.08%) and they most belong to big cities, especially Madrid (16.73%).

Location	Core %	15M %	12M15M%	25S%
Andalusia	**6.61**	**4.82**	**6.22**	**6.44**
Aragon	1.77	1.22	1.50	1.12
Asturias	1.21	0.95	0.97	0.99
Balearics	0.71	0.61	0.55	0.44
Canary Islands	1.10	0.95	0.95	0.88
Cantabria	0.48	0.31	0.38	0.36
Castilla y Leon	2.64	1.99	2.27	2.23
Castilla la Mancha	0.85	0.71	1.00	1.16
Catalonia	**10.01**	**8.67**	**8.20**	**4.94**
Ceuta and Melilla	0.06	0.05	0.08	0.05
Valencian Community	**4.19**	**3.31**	**3.92**	**3.21**
Estremadura	0.93	0.67	0.92	0.93
Galicia	2.43	1.81	1.95	2.14
Rioja	0.21	0.17	0.18	0.17
Madrid	**16.73**	**10.87**	**10.74**	**9.25**
Murcia	1.47	1.06	1.35	1.31
Navarre	0.50	0.37	0.39	0.37
the Basque Country	1.16	0.97	0.86	0.98
unknown	**46.92**	**60.51**	**57.58**	**63.04**

Table 4: Distribution of users by geographical areas

When classified by urban or local origin, tweets show a trend towards decentralization from urban to local. As the *Core* group is more urban than local, the movement was initially mostly urban, but as it grows, so does decentralization.

Urban-Local	Core %	15M %	12M15M %	25S %
Urban	**25.96**	**18.81**	**18.25**	**13.95**
Local	23.25	18.25	20.93	20.38
Unknow	**50.79**	**62.94**	**60.82**	**65.67**

Table 5: Distribution of users by urban-local

5.2.3. Occupation level

We observed that the most common occupation level is «professional», though it showed a decreasing pattern in contrast to the participation of students. In the *Core* group the percentage of professionals was twice higher than on common users.

Level	Core %	15M %	12M15M %	25S %
Manager-Executive	0.94	0.96	0.73	**0.52**
Professional	**20.99**	13.93	14.02	**10.30**
Support staff	0.35	0.28	0.35	0.37
Manual worker	0.32	0.25	0.33	0.35
Student	3.93	3.08	5.3	**5.53**
Unknown	73.47	81.5	79.27	82.93

Table 6: Distribution of users by occupation level

5.2.4. Tribes

From the total set of users, a new categorization was made in tribes according to their general profiles: Activists, Media, Politicians and Unions. Evolution in time shows a greater involvement of unions at the expense of the Platforms and Media. Politicians do not present major changes with just a slight decrease in matters of presence.

Tribes	15M %	12M15M %	25S %
Activists	**17.03**	**13.74**	**11.72**
Media	**19.12**	**17.12**	**14.77**
Politicians	55.20	47.84	49.12
Unions	**8.65**	**21.29**	**24.39**

Table 7: Distribution of users by tribes

5.3. Evolution of the movements

We captured the formation and rise of 15M and 25S on Twitter. In both cases we find that the first users who participated and got notoriety were often overshadowed by others who joined later. We also note that at the *Boom* period there was a central core with many relevant users of different communities, but when the movement got into later stages, these groups took a distance from the main activities.

During the 15M movement, @democraciareal, the main convener, was quickly overtaken in the *Early* phase. On the other hand, the group that claimed free culture (@bufetalmeida, @julioalonso, @edans, etc...) was also overshadowed in the *Boom* stage. Two users that not existed in May 15, @AcampadaSol and @acampadabcn, were finally the most enduring users. Figure 4 to Figure 7 below portray the evolution of the relationships established during each stage of the 15M.

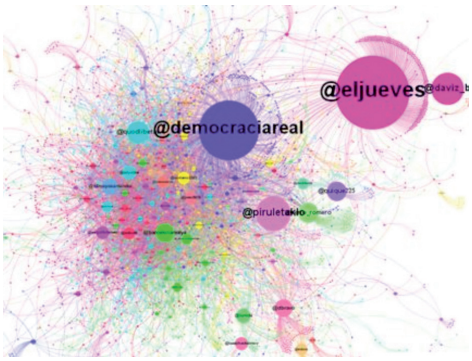


Figure 4: 15M- Map of RTs Origin

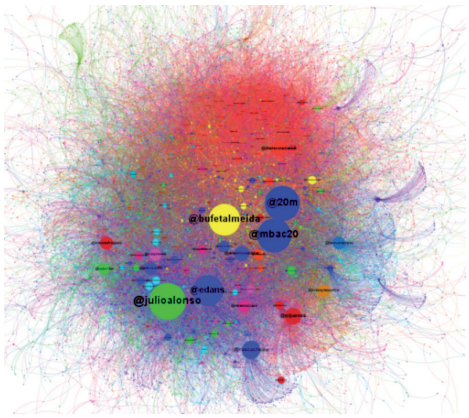


Figure 5: 15M- Map of RTs Early

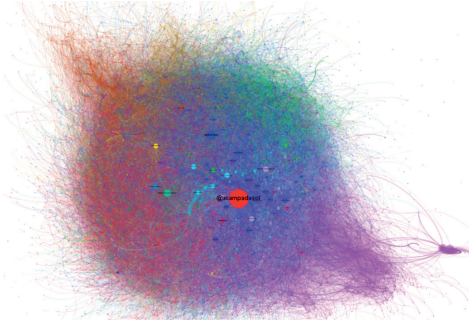


Figure 6: 15M Map of RTS Boom

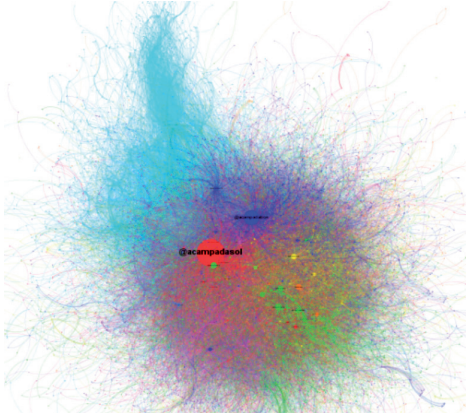


Figure 7: 15M- Map of RTs Late

As per the call for September 25 (Figure 8 to Figure 11) it can be seen that in the *Origin* stage there is no central node playing a coordinating role. Instead, the major roles are played by individual users and, later on, by the collective user @democraciareal. Though it has a important role in the diffusion of information, it is worth clarifying that it did not have a major role in terms of centrality.

During the *Early* stage from August 24 to September 24, a network around the call for a new event is created. The user @Coordinadora25S appears to, precisly, explicitly coordinate the movement, as do @OcupaelCongreso and @DemocraciaReal. Only two of the initial users are still on this stage.

On the *Boom* of the call –September 25 to 30– well defined communities have already appeared. Central nodes –in deep blue– are the platforms, with a strong relationship with media –painted in salmon. The periphery is populated by the political left

–red– and in the upper right corner –light blue the initial group, now not occupying the geographical center of the movement. At their side, in yellow, the *acampadas*.

Last, the *Late* stage maintains the spirit of the call of @coordinadora 25S and @democraciasreal, but now split in different communities.

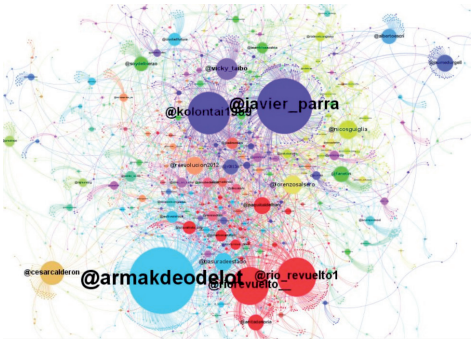


Figure 8: 25S- Map of RTs «Origin»

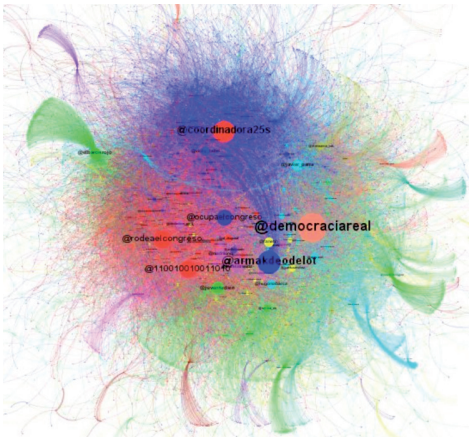


Figure 9: 25S- Map of RTs «Early»

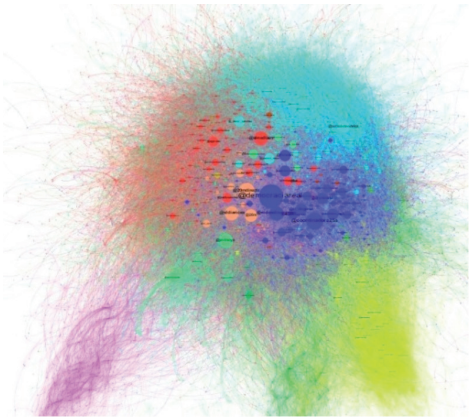


Figure 10: 25S- Map of RTs «Boom»

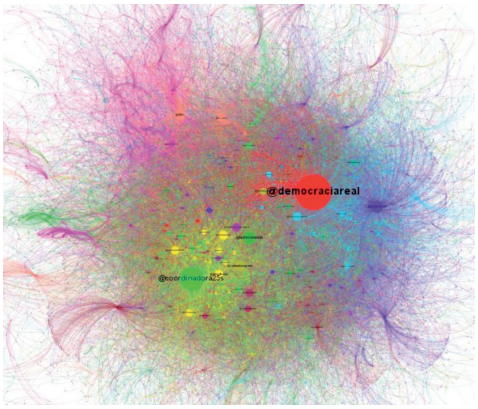


Figure 11: 25S- Map of RTs «Late»

5.4. Relationship between the 15M and 29S and institutional politics

In this subsection, we study the relationship among the 15M movement tribes, mass-media (channels, programs and journalists) and the democratic institutions (parties and trade unions) in the mention graphs. For this purpose we analyse the connectivity of each group, through the k-index decomposition, and the connections between groups, through the detection of communities.

5.4.1. K-index decomposition

Table 1 shows the maximum, the average and the standard deviation of the k-indices of the nodes which form each group in the three moments in time (15M, 12M15M and 25s).

In the 15M period, we observe that in almost every group there is at least one node with the maximum k-index (k_{max}=12), except for the parties CUP and COMPROMIS and the trade union CCOO. According to the average k-index, the 15M tribes (ACAMPADA, DRY, PAH) and MEDIA are distinguishably the best connected groups in this period (k_{avg}>=7). Then, we note that the parties with the highest average k-index are the three newest ones: EQUO, PIRATA and UPYD (k_{avg}>=3). The trade unions and the rest of the parties obtain the lowest average k-index values without any ideological ordering pattern (k_{avg}<3).

The results in the 12M15M period show that only the two main 15M tribes (ACAMPADA, DRY) and MEDIA contain a node with the maximum k-index (k_{max}=19). In this period, DRY emerges as the best connected group according to the average k-index (k_{avg}>=7), followed, by the two other 15M tribes (PAH, ACAMPADA) (k_{avg}>=7). The newest parties political parties PIRATA and EQUO are still the best connected ones (k_{avg}>=3.88) while UPYD shows greater disaffection in the anniversary period (k_{avg}>=1.45). We also observe that MEDIA do not play such an important role in this network when some left-wing parties (ICV, IUNIDA) and the trade unions (CCOO, UGT) get higher average k-index values.

In the 25S period many groups contain at least one with the maximum k-index value. However, we observe than in this period the average k-index value of the 25S group formed by the organizer accounts is significantly higher (k_{avg}=21.67) than the rest of the groups (k_{avg}<=10.34). After 25S group, the best connected groups are the two main 15M tribes (ACAMPADA, DRY) (k_{avg}>=9.65). The position of MEDIA in the ranking is considerably upper than its position in the previous period (k_{avg}=6.92) and EQUO remains as the best connected political party (k_{avg}=6.15).

Finally, we found that the standard deviation is notably higher in the best connected groups except for the 25S group, formed by just 6 accounts, in the last period. This indicates a greater diversity of values in high connected groups while in most parties the standard deviation is considerably lower because of the inactivity of most of their members during this period.

15M				12M15M				25S			
group	k_{max}	k_{avg}	k_{std}	**group**	k_{max}	k_{avg}	k_{std}	**group**	k_{max}	k_{avg}	k_{std}
acampada	12	7,6	4,11	dry	19	8,02	8	25s	22	21,67	0,75
media	12	7,31	4,28	pah	17	6,04	5,95	dry	22	10,34	8,8
dry	12	7,23	4,94	acampada	19	6	6,79	acampada	22	9,65	8,45
pah	12	7	5	pirata	17	4,3	3,85	media	22	6,92	7,53

15M			
equo	12	5,67	4,87
pirata	12	4,41	4,17
upyd	12	3,28	3,63
iunida	12	2,89	3,26
pp	12	2,51	2,78
psoe	12	2,09	2,76
icv	12	1,81	2,5
ugt	12	1,81	2,81
ciu	12	1,68	2,46
ccoo	7	1,36	1,85
cup	3	1,25	0,83
compromis	8	1,13	2,36
erc	12	0,97	1,87

12M15M			
equo	17	3,88	3,45
icv	13	3,2	3,28
iunida	16	3,18	3,26
ccoo	17	2,82	2,98
ugt	15	2,69	3,22
media	19	2,16	3,44
compromis	6	1,78	1,79
cup	6	1,53	1,79
upyd	5	1,45	1,13
psoe	17	1,19	1,75
erc	14	0,99	1,95
pp	5	0,54	0,88
ciu	3	0,5	0,7

25S			
equo	20	6,15	6,51
pah	22	5,14	6,48
iunida	22	5,11	6,74
ciu	13	4,16	5,2
pp	22	4,13	5,89
icv	22	3,77	5,73
pirata	22	3,11	5,61
psoe	20	2,48	4
upyd	21	2,16	3,98
compromis	18	1,84	4,55
cup	6	1,82	2,21
ccoo	22	1,53	3,28
ugt	22	1,4	3,07
erc	22	1,17	3,81

Table 8: Max k-index, average k-index and standard deviation of the k-indexes of the nodes that formed the analysed groups during the 15M, 12M15M and 25S periods.

5.4.2. Community detection

We also examine the relationships between groups, through the Louvain method for community detection, in the same three periods: 15M, 12M15M and 25S. Figure 12 shows the mention graph in the 15M period with two communities detected by the algorithm. The largest one is formed by the two main 15M tribes (ACAMPADA, DRY), MEDIA, left-wing parties (PIRATA, IUNIDA, EQUO, ICV, ERC) and the trade unions (CCOO, UGT). The second community is formed by the three major parties (PP, PSOE, CIU) accused of corruption by the platform *#nolesvotes*, core of the 15M movement in this period, and the liberal party UPYD.

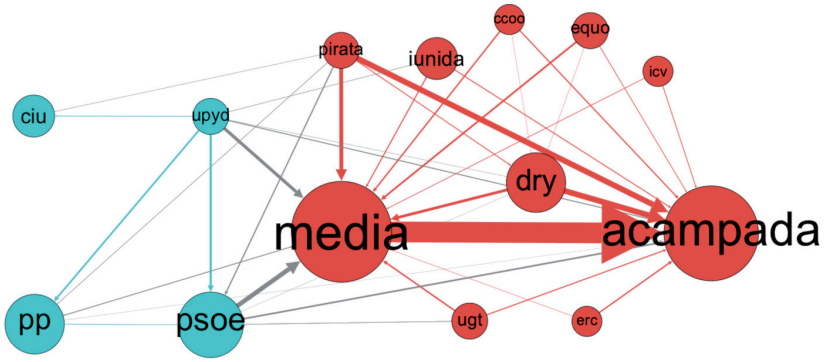


Figure 12: Mention graph of the analysed groups in the 15M period.
Note: The size corresponds to the in-degree of the node.

Figure 13 shows the three communities in the mention graph of 12M15M period. In this interval, when the first anniversary of the 15M movement was held, the three 15M tribes (ACAMPADA, DRY, PAH) form one community. MEDIA act as a hub in the second community formed by the trade unions (CCOO, UGT) and most of the political parties (PP, PSOE, UPYD, EQUO, PIRATA) except for two left-wing parties (IUNIDA, ICV) which appear in the third community.

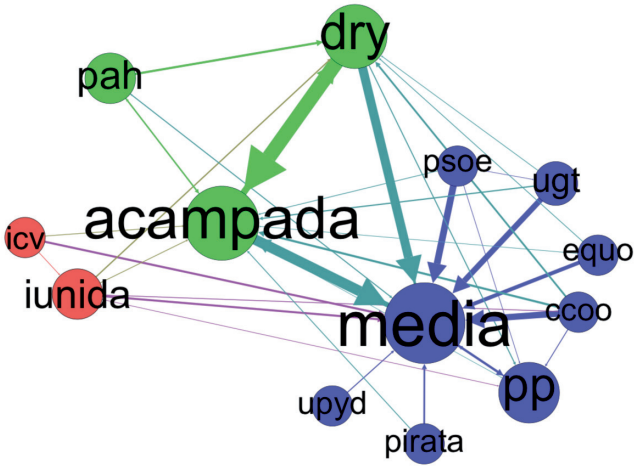


Figure 13: Mention graph of the analysed groups in the 12M15M period.
Note: The size corresponds to the in-degree of the node.

The three detected communities in the mention graph of the 25S period are showed in Figure 14. The 25s group form a community with the newest political parties (EQUO, UPYD, PIRATA, COMPROMIS) and PAH. The two main 15M tribes (ACAMPADA and DRY) are found in a community interacting with the three major parties accused of corruption by the platform *#nolesvotes* (PP, PSOE, CIU). Finally, some left-wing parties (IUNIDA, ICV, ERC), the trade unions (CCOO, UGT) and MEDIA form the third community.

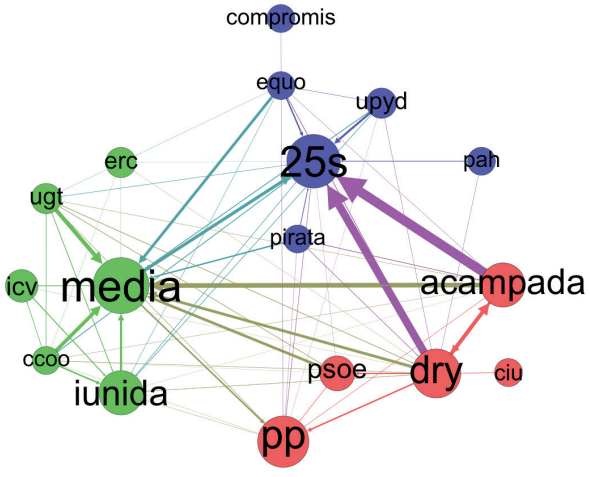


Figure 14: Mention graph of the analysed groups in the 25S period.
Note: The size corresponds to the in-degree of the node.

6. DISCUSSION

The movement of the 15M was clearly born and fostered on the Net and, later on, it did materialize in the offline world, in the *plazas*, in the *acampadas*. Initially born in big cities, they quickly spread out of urban areas to step on smaller cities and rural areas.

Totally lacking personal leaders, citizens flock around an idea or an explicit call to action and thus a movement emerges. A significant trademark of the movement is that a collective identity is created, an identity that quickly overshadows more or less relevant individuals that could very initially be identified. Collectivelly managed, «brands», mottos, collective users turn into real spokesman and intermediaries with other institutions such as governments, political parties, unions or media. This dialogue legitimates the collective without the need of visible individuals on the other side.

The profile of the initial participant is increasingly balanced men and women, and is a youngster, student, with a high educational level, and involved personally or professionally with communications, telecommunications or technology. This profile evolves with time into a more typical profile liked with activism, protests of demonstrations, as the increase of labour union members shows.

What ties the community –and its members– together is a strong sense of common goals, strengthened in sub-communities made up by common professional profiles, ideology or friendship.

6.1. Online vs. Offline

Unlike what common knowledge –and mainstream media messages– states, there is a strong bound between the online and the offline worlds of activism in the 15M movement. Despite the fact that the 15M and the subsequent events (12M15M, 25S) where initiated on the Net, they quickly moved offline to occupy physical public spaces. Our first hypothesis is not only validated by this observation, but also by what Aragón et al. (2012) already explained when comparing online and offline activity: growth of activity goes in parallel in both worlds, backed with political marketing and communication techniques.

We can state that these movements work as para-institutions, as they are assimilated as institutions on the outside –with explicit goals and targets, consolidated messages, collective identities that act as spokesmen– while they preserve a network-like organization on the inside, as the analysis of the inner communication clearly shows.

Indeed, the inner structure is nothing like the traditional structure of political parties, unions or other kind of citizen organizations. With free movement and possibility to participate, they use global digital networks in the most flexible way to enhance and enable any kind of participation (Castells, 2009), free in time, in space and in commitment. As we assumed in our hypotheses, members enter and leave the movement at will, or participate in different factions of it without major issues and, most important, without the movement even noticing –but the individuals, of course.

6.2. Relationship between the 15M and 29S and institutional politics

Reinforcing what has been stated before, despite the fact that many members enter or leave the movements, the movements themselves, taken as a whole, do survive like any other organization, hence their nature of para-institution. It is interesting to see how their collective identity evolves but persists along time and across the different calls and movements, from the 15M to 25S and through 12M15M. And this all happens with a most interesting characteristic: without any physical settlement of any kind.

These network para-institutions have close relationships amongst them –as it is shown comparing the different movements and calls of the 15M and 25S. In the same way, they feel closer to the organizations that have similar flexible structures, such as some media or other network parties such as the Spanish Pirate Party or the recently formed Equo.

Regarding this relationship with political parties and unions, besides this closeness to network parties, it is not surprising that these mostly protest movements have a fluid communication with left-wing parties and unions –though they are neither part of them nor can be confounded with them, which is also clear from data. Only a certain degree of confusion comes later, when the core of the movement begins to set aside and their space is taken by traditional actors of mobilization, mostly left-wing parties and unions. Most of the time, center and right-wing parties just keep a safety distance from the movement or even isolate themselves from all the buzz and debate.

It is true, then, that the dialogue between emergent citizen movement and traditional parties is weak and it varies depending on ideology and the maturity of the movement. As time passes, major and right-wing parties keep their isolation despite being constantly questioned by the movements, while minor parties try to get in the movement and media and left-wing parties have a decisive but cautious approach, benefitting from their political profile and relationship with independent activists (Elmer, et al., 2009).

6.3. Relationship with media

Is it beyond doubt that in many moments of the movement, and for many actors, media suppose the only link between the citizens and the institutions of the democracy: governments, many parties and the legislative power –the later not present in the debate, but constantly questioned about the actions it should undertake.

It is not surprisingly to see media as the intermediators of a network organization, as it was already shown by Adamic & Glance (2005) when analyzing the political blogosphere and the central role of media in bridging the two sides of the political debate.

But this «institutional journalism is threatened by the Internet» (Kelly, 2008) in the sense that once this mediation role disappears, political institutions and network

para-institutions can –as some of them do– speak one to each other and with the citizen with further mediation. We still see, notwithstanding, the mainstream media playing a major role and having a «strong symbiosis» (Kelly, 2008) between the citizen networks and other actors of the political arena. But, again, Kelly (2008) explains it for the blogosphere just the way it also happened in the 15M: »the growing networked public sphere is not just changing the relationship among actors in the political landscape: it is changing the kinds of actors found there, and changing what 'media' is actually doing».

6.4. Extra-representative participation

As we advanced in our last hypothesis, we can state, by comparing the actions online and offline of all democratic institutions and network movements that the cause behind participation is unrest. This is, of course, not a new finding, but the novelty are networks. When unrest cannot be channelled through representative participation –minor parties, unions, non-governmental organizations– as it was the case of 15M, extra-representative participation arises. And it does not arise in small clusters, but articulated globally by means of digital technologies. The tremendous democratic potential of Internet mobilization (Cristancho & Salcedo, 2009) is, undoubtedly, the reason behind past and actual protests, and behind the differences in organization design, behaviour and evolution.

As Font et al. (2012) explained for Spain, there is an unmet need for participation which formal politics just cannot fulfil. The need for more participation, the critical mass built in (a) urban areas and (b) through the Net, plus the extremism due to socioeconomic causes has led the citizens to find their ways around traditional institutions. Indeed, when the citizenry trusts not politicians but their own peers (Font et al., 2012), the substrate for building a strong network has just been set.

It is undecided wether «movement-parties» –defined as non-programmatic and non-bureaucratic parties– will benefit from their advantage in exploiting the interactive potential of the internet for political mobilization (Cardenal, 2013) and thus be able to interact and work with these new network para-institutions. We have already seen that, as time goes by, the igniting core leaves room to the mass for participation and, in the long term, is somewhat complemented by traditional actors.

The question is whether the movement will ever be replaced by or will merge with these actors. So far, we have witnessed the movement emerge as a collective representative and wait for other actors –media, left-wing parties, unions– to appear on the new political arena. It is soon to tell whether these network para-institutions will disappear after the current socio-economic conjuncture, will complete the evolution to a formal institution (as some splinters of the movement actually did) and become a party or an incorporated lobby, will vanish into the bigger programme of a major party or union or,

on the contrary, will be the seed of a new political paradigm based on network-centric organization models.

7. BIBLIOGRAPHY

Adamic, L.A. & Glance, N. (2005). «The political blogosphere and the 2004 U.S. election: divided they blog». In *LinkKDD '05: Proceedings of the 3rd international workshop on Link discovery*, 36-43. New York: ACM.

Alcazan, Monty, A., Axebra, Quodlibetat, Levi, S., SuNotissima, TakeTheSquare & Toret (2012). *Tecnopolítica, Internet y R-Evoluciones. Sobre la Centralidad de Redes Digitales en el #15M*. Barcelona: Icaria.

Anduiza, E., Gallego, A. & Jorba, L. (2009). *The Political Knowledge Gap in the New Media Environment: Evidence from Spain*. Prepared for the seminar Citizen Politics: Are the New Media Reshaping Political Engagement? Barcelona, May 28th-30th 2009. Barcelona: IGOP.

Anduiza, E., Martín, I. & Mateos, A. (2012). «Las consecuencias electorales del 15M en las elecciones generales de 2011». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756). Barcelona: UAB. Retrieved March 27, 2013 from http://democracia.uab.cat/images/publications/anduizaetal.pdf

Anduiza, E., Cristancho, C. & Sabucedo, J.M. (2012). «Mobilization through Online Social Networks: the political protest of the indignados in Spain». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756). Barcelona: UAB. Retrieved March 27, 2013 from http://s3.amazonaws.com/academia.edu.documents/18107452/Mobilization_through_online_social_networks_for_web.pdf?AWSAccessKeyId=AKIAIR6FSIMDFXPEERSA&Expires=1364401083&Signature=rV9E0upqgjLyc32mv6AoGJvVvuo=

Aragón, P., Kappler, K., Kaltenbrunner, A., Neff, J.G., Laniado, D. & Volkovich, Y. (2012). *Tweeting the campaign. Evaluation of the Strategies performed by Spanish Political Parties on Twitter for the 2011 National Elections*. Internet, Politics, Policy 2012: Big Data, Big Challenges?. Barcelona: Barcelona Media Foundation. Retrieved January 09, 2013 from http://microsites.oii.ox.ac.uk/ipp2012/sites/microsites.oii.ox.ac.uk.ipp2012/files/aragon_et_al_0.pdf

Blondel, V. D., Guillaume, J. L., Lambiotte, R., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment*, *2008*(10), P10008. Bristol: IOP Publishing Ltd.

Borge, R. & Cardenal, A.S. (2012). «Surfing the Net: A Pathway to Participation for the Politically Uninterested?». In *Policy & Internet, 3* (1). Berkeley: Berkeley Electronic Press. Retrieved April 01, 2011 from http://www.psocommons.org/policyandinternet/vol3/iss1/art3

Cantijoch, M. (2009). *Reinforcement and mobilization: the influence of the Internet on different types of political participation*. Prepared for the seminar Citizen Politics: Are the New Media Reshaping Political Engagement? Barcelona, May 28th-30th 2009. Barcelona: IGOP.

Cardenal, A.S. (2013). «Why mobilize support online? The paradox of party behaviour online». In *Party Politics, 19* (1), 83–103. London: SAGE Publications.

Castells, M. (2009). *Communication power*. Cambridge: Oxford University Press.

Castells, M. (2012). *Redes de indignación y esperanza*. Madrid: Alianza Editorial.

Christensen, H.S. (2011). «Political activities on the Internet: Slacktivism or political participation by other means?». In *First Monday, February 2011, 16* (2). [online]: First Monday. Retrieved November 29, 2012 from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3336/2767

Criado, J.I. & Martínez Fuentes, G. (2009). «¿Hacia la conquista política de la blogosfera? Blogging electoral en la campaña de los comicios municipales del 2007». In *IDP. Revista de Internet, Derecho y Ciencia Política*, (8). Barcelona: Universitat Oberta de Catalunya. Retrieved October 05, 2009 from http://idp.uoc.edu/ojs/index.php/idp/article/viewFile/n8_criado_martinez/n8_criado_esp

Cristancho, C. & Salcedo, J. (2009). *Assessing Internet Mobilization - Integrating Web Analysis and Survey Data*. Prepared for the seminar Citizen Politics: Are the New Media Reshaping Political Engagement? Barcelona, May 28th-30th 2009. Barcelona: IGOP.

Elmer, G., Langlois, G., Devereaux, Z., Ryan, P.M., McKelvey, F., Redden, J. & Curlew, A.B. (2009). ««Blogs I Read»: Partisanship and Party Loyalty in the Canadian Political Blogosphere». In *Journal of Information Technology & Politics, 6* (2), 156 – 165. London: Routledge.

Font, J., Navarro, C., Wojcieszak, M. & Alarcón, P. (2012). *¿»Democracia sigilosa» en España? Preferencias de la ciudadanía española sobre las formas de decisión política y sus factores explicativos*. Opiniones y actidudes, nº71. Madrid: Centro de Investigaciones Sociológicas. Retrieved December 03, 2012 from http://libreria.cis.es/static/pdf/OA71acc.pdf

González-Bailón, S., Borge-Holthoefer, J., Rivero, A., & Moreno, Y. (2011). The dynamics of protest recruitment through an online network. Scientific reports, 1.

Guadián Orta, C., Rangel Pardo, F.M. & Llinares Salas, J. (2012). *Análisis de Redes de Influencia en Twitter*. II Congreso Español de Recuperación de Información (CERI 2012). Valencia: Universitat Politècnica de València. Retrieved August 20, 2012 from http://users.dsic.upv.es/grupos/nle/ceri/papers/ceri2012_guardian.pdf

Inglehart, R. (2008). «Changing Values among Western Publics from 1970 to 2006». In *West European Politics, January–March 2008, 31* (1-2), 130–146. London:

Routledge. Retrieved February 12, 2013 from http://www.worldvaluessurvey.org/wvs/articles/folder_published/publication_559/files/values_1970-2006.pdf

Institute for Politics, Democracy & the Internet (2004). *Political Influentials Online in the 2004 Presidential Campaign*. Washington, DC: The George Washington University. Retrieved October 15, 2008 from http://www.ipdi.org/UploadedFiles/political%20influentials.pdf

Izquierdo Labella, L. (2012). «Las redes sociales en la política española: Twitter en las elecciones de 2011». In *Estudos em Comunicação, Maio 2012, 11*, 139-153. Covilhã: Universidade da Beira Interior. Retrieved January 21, 2013 from http://www.ec.ubi.pt/ec/11/pdf/EC11-2012Mai-07.pdf

Jensen, M.J. (2009). *Political Participation, Alienation, and the Internet in the United States and Spain*. Prepared for the seminar Citizen Politics: Are the New Media Reshaping Political Engagement? Barcelona, May 28th-30th 2009. Barcelona: IGOP.

Katz, J.E., Rice, R.E. & Aspden, P. (2001). «The Internet, 1995-2000: Access, Civic Involvement, and Social Interaction». In *American Behaviorial Scientist, 45* (3), 405-419. London: SAGE Publications.

Kelly, J., Fisher, D. & Smith, M. (2005). *Debate, Division, and Diversity: Political Discourse Networks in USENET Newsgroups*. Paper prepared for the Online Deliberation Conference 2005. Palo Alto: Stanford University. Retrieved July 10, 2007 from http://www.coi.columbia.edu/pdf/kelly_fisher_smith_ddd.pdf

Kelly, J. (2008). *Pride of Place: Mainstream Media and the Networked Public Sphere*. Media Re:public Side Papers. Cambridge: Berkman Center for Internet and Society at Harvard University. Retrieved December 20, 2008 from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Pride of Place_MR.pdf

Kitsak, M., Gallos, L., Havlin, S., Liljeros, F., Muchnik, L., Stanley, H.E. & Makse, H.A. «Identifying influential spreaders in complex networks». In *Nature Physics*, 6 (11), 888-893. London: Nature Publishing Group. arXiv:1001.5285, 2010

Lotan, G., Graeff, E., Ananny, M., Gaffney, D., Pearce, I. & Boyd, D. (2011). «The Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions». In *International Journal of Communication, 5*, 1375–1405. Los Angeles: USC Annenberg Press. Retrieved September 27, 2011 from http://ijoc.org/ojs/index.php/ijoc/article/view/1246/613

Martínez Roldán, S. (2011). *Movimiento 15M: construcción del espacio urbano a través de la acción de las Multitudes Inteligentes*. Barcelona: UOC. Retrieved July 26, 2011 from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/8582/1/smartinezrol_TFM_0711.pdf

Mislove, A., Lehmnan, S., Ahn, Y.A., Onnela, J. & Rosenquist, J.N. (2011). «Understanding the Demographics of Twitter Users». In *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*. Barcelona: AAAI Press.

Norris, P. & Curtice, J. (2006). «If You Build a Political Web Site, Will They Come? The Internet and Political Activism in Britain». In *International Journal of Electronic Government Research, 2* (2), 1-21. Hershey: IGI Global.

Noveck, B.S. (2005). «A democracy of groups». In *First Monday, 10* (11). [online]: First Monday. Retrieved June 14, 2009 from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1289/1209

Padró-Solanet, A. (2009). *The Strategic Adaptation of Party Organizations to the New Information and Communication Technologies: A Study of Catalan and Spanish Parties*. Paper prepared for presentation at the Workshop 20: «Parliaments, Parties and Politicians in Cyberspace» ECPR Joint Sessions Lisbon, April 14-19 2009. Lisbon: ECPR. Retrieved June 17, 2009 from http://intradociep.upmf-grenoble.fr/Spip//IMG/pdf/ECPR2009Padro-Solanet.Padró-Solanet, A. (2010). *Internet and Votes: The Impact of New ICTs in the 2008 Spanish Parliamentary Elections*. Communication presented at the Internet, Politics, Policy 2010: An Impact Assessment conference, 16-17 September 2010. Oxford: Oxford Internet Institute.

Peña-López, I. (2011). «Striving behind the shadow – The dawn of Spanish politics 2.0». In van der Hof, S. & Groothuis, M. (Eds.), *Innovating Government. Normative, policy and technological dimensions of modern government, Chapter 8*, 129-147. The Hague: TMC Asser Press.

Peña-López, I. (2011). «The disempowering Goverati: e-Aristocrats or the Delusion of e-Democracy». In *eJournal of eDemocracy and Open Government, 3* (1), 1-21. Krems: Danube-University Krems. Retrieved May 07, 2011 from http://www.jedem.org/article/view/50

Rainie, L., Purcell, K. & Smith, A. (2011). *The social side of the internet*. Washington, DC: Pew Internet & American Life Project. Retrieved January 20, 2011 from http://pewinternet.org/Reports/2011/The-Social-Side-of-the-Internet.aspx

Robles Morales, J.M. (2008). *Ciudadanía Digital. Un acercamiento a las causas de la ideología de los internautas españoles*. Research seminar held on July, 3rd, 2008 in Barcelona, Universitat Oberta de Catalunya. [mimeo].

Robles Morales, J.M., Molina Molina, Ó. & De Marco, S. (2012). «Participación política digital y brech digital política en España. Un estudio de las desigualdades digitales». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 795-810. Berkeley: Berkeley Electronic Press. Retrieved September 14, 2012 from http://arbor.revistas.csic.es/index.php/arbor/article/view/1501

Sampedro, V., López Rey, J.A. & Muñoz Goy, C. (2012). «Ciberdemocracia y cibercampaña: ¿Un matrimonio difícil? El caso de las Elecciones Generales en España en 2008». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 657-672. Berkeley: Berkeley Electronic Press. Retrieved September 14, 2012 from http://arbor.revistas.csic.es/index.php/arbor/article/view/1492

Sádaba, I. (2012). «Participación política digital y brech digital política en España. Un estudio de las desigualdades digitales». In *Arbor. Ciencia, Pensamiento y Cultura, 188* (756), 781-794. Berkeley: Berkeley Electronic Press. Retrieved September 14, 2012 from http://arbor.revistas.csic.es/index.php/arbor/article/view/1500

Seidman, S. B. (1983). Network structure and minimum degree. *Social networks*, *5*(3), 269-287.

Tichenor, P.J., Donohue, G.A. & Olien, C.N. (1970). «Mass media flow and differential growth in knowledge». In *Public Opinion Quarterly, 34* (2), 159 - 170. Oxford: Oxford University Press.

Traficantes de Sueños (Ed.) (2004). *¡Pásalo! Relatos y análisis sobre el 11-M y los días que le siguieron*. Madrid: Traficantes de Sueños.

Wu, S., Hofman, J.M., Mason, W.A. & Watts, D.J. (2011). *Who Says What to Whom on Twitter*. New York: Yahoo! Research. Retrieved March 30, 2011 from http://research.yahoo.com/files/twitter-flow.pdf

EL ESTUDIO DE LA MOVILIZACIÓN SOCIAL EN LA ERA DEL *BIG DATA*

Jorge L Salcedo M
Investigador Grupo Democracia Elecciones y Ciudadanía UAB
Consultor Universitat Oberta de Catalunya

Camilo Cristancho
Investigador Grupo Democracia Elecciones y Ciudadanía
Universitat Autónoma de Barcelona

RESUMEN: Los procesos de movilización social han sido una cuestión central de la investigación en las ciencias sociales, tanto en las preguntas centrales por el comportamiento de los actores como por la lógica de los procesos comunicativos y de difusión de información. Sin embargo, la aproximación empírica al análisis de procesos de difusión ha presentado tradicionalmente grandes dificultades metodológicas. Antes del desarrollo de la Web era muy difícil estudiar redes de influencia, contenidos y el rol de los actores con el fin de identificar de manera precisa la dirección de los procesos de difusión en un evento de movilización social de grandes dimensiones (Watts et al 2012). Adicionalmente, los estudios con soporte empírico que existían estaban fuertemente sesgados por concentrarse en eventos de movilización exitosos. Con el desarrollo de las redes sociales online y en particular de Twitter, investigadores de diferentes disciplinas tienen la oportunidad de explicar estos fenómenos. De esta manera, existen múltiples perspectivas sobre el fenómeno, las cuales han generado una amplia literatura y proveen un abundante repertorio de instrumentos para estudiar los fenómenos de difusión. El estudio de este tipo de dinámicas no está exento de desafíos metodológicos, diferentes preguntas por resolver y nuevos interrogantes que han surgido a la luz de hallazgos recientes. Consideramos relevante identificar principios teóricos comunes en la investigación realizada hasta el momento para conectar el amplio espectro de hallazgos sobre los procesos de movilización. Pretendemos buscar conexiones entre el trabajo de las ciencias de la computación y las diferentes aproximaciones teóricas de las ciencias sociales y por ello proponemos este artículo de compilación y futuras líneas de investigación. Revisamos el estado del arte sobre los estudios de movilización vía Twitter con el fin de identificar los diferentes métodos utilizados hasta ahora, los límites a los que se han enfrentado los investigadores en aproximaciones de *Big data* y los resultados propuestos. El análisis se basa en artículos publicados en revistas de alto impacto y en textos presentados en conferencias de múltiples disciplinas. Una de nuestras principales conclusiones es que aproximaciones como las del *Big Data* dentro de la movilización social nos ofrecen nuevas explicaciones de los fenómenos de difusión de información, no obstante entre los estudiosos de la movilización social se categorizan diferentes formas de difusión que al intentar recurrir al *Big Data* para su explicación se convierten en un desafío e incluso evidencia los límites de esta novedosa aproximación.

PALABRAS CLAVE: Movilización social, *Big Data*, difusión, redes sociales.

1. INTRODUCCIÓN

1.1. Objetivos

La pregunta por la movilización social ha sido una cuestión central en las ciencias sociales (Givan, Roberts, y Soule 2010; McAdam 1983; Myers 1997; Porta y Tarrow 2012), la cual ha empezado a revisarse a la luz de los procesos de movilización que se dan en las redes sociales online (Bennett y Segerberg 2012; González-Bailón et al. 2011; Khamis y Vaughn 2011). Las dinámicas de la información en estas redes han cambiado radicalmente y por ello generan preguntas de gran interés para los científicos sociales y los estudiosos de las comunicaciones y de la computación. Junto con los posibles efectos y cambios en los comportamientos de los actores generados por estas nuevas formas de comunicación, surgen nuevas posibilidades metodológicas. El registro de la actividad en los medios sociales permite el seguimiento del rastro digital de las comunicaciones y comportamientos. De esta forma se convierte en una fuente de información de una enorme riqueza para una aproximación académica y plantea nuevos retos metodológicos.

El objetivo de este artículo es hacer una revisión de algunos de los estudios recientes más relevantes sobre la difusión en las redes sociales con el fin de buscar conexiones entre el trabajo que integra enfoques de las ciencias de la computación y las diferentes aproximaciones teóricas de las ciencias sociales. Se busca identificar puntos comunes en la investigación realizada hasta el momento e identificar sus aportes a la luz de las teorías relevantes de los procesos de movilización. De tal forma, se pretende hacer un recuento de qué sabemos hasta el momento sobre la difusión en la movilización social y proponer futuras líneas de investigación.

En una primera parte presentamos una breve definición de difusión, la cual exploraremos con mayor detalle en el cuerpo del texto. Igualmente precisamos los conceptos de medios sociales y *Big Data*. En un siguiente apartado expondremos el creciente interés de los estudios de difusión y medios sociales entre la comunidad académica, y las características que hacen de Twitter un medio especialmente atractivo para los estudios de difusión. A continuación presentamos los documentos que analizamos para establecer este Estado del arte, junto con sus criterios de selección. En la parte central del texto proponemos un dialogo entre las ciencias de la computación y las ciencias sociales y exponemos desde el enfoque de *Big Data* qué preguntas y explicaciones acerca de difusión se han establecido y cómo pueden conectarse con las preguntas centrales de los estudios de movilización tradicionales de las ciencias sociales. Finalmente plateamos una serie de preguntas y aspectos que consideramos están por resolver. Éstos se plantean como futuras líneas de investigación.

1.2. Algunos conceptos clave

El interés de los científicos sociales sobre el tema de difusión surge hace más de tres décadas, cuando Everett Rogers en la primera edición de su libro en 1962 realizo su

estudio sobre difusión de las innovaciones tecnológicas (Rogers 2010). En éste explicaba cómo el proceso de difusión se podía representar como una curva con forma de S, en donde la innovación primero sería aceptada por un pequeño grupo o elite y logrando la aceptación de ellos; seguía una rápida absorción entre un largo número de seguidores y se estabilizaba cuando alcanzaba un nivel cercano a la capacidad de una población dada de absorber la innovación. En términos de Strang y Meyer (1993) la difusión implica que la adopción previa de un rasgo o una práctica en una población altera la probabilidad de adopción para el resto de los no adoptantes. Dentro de los procesos de movilización social todo lo concerniente a lograr la movilización ha sido conceptualizado como un problema de difusión (Kim y Bearman 1997; Strang y Soule 1998).Todo el proceso de movilización y finalmente de difusión se transmite de un miembro de la población a otro a través de canales directos o indirectos del conjunto social. (Rogers 2010). Entre los canales directos están todas las redes interpersonales que existen entre individuos y organizaciones. Entre los indirectos están el compartir atributos similares o formas culturales, donde los medios de comunicación facilitan la difusión.

Entre los canales que en la actualidad han tomado un mayor protagonismo en la movilización social y la difusión de la protesta están los medios sociales (Gilad Lotan et al. 2011; Papacharissi y de Fatima Oliveira 2012). Diferentes hechos cómo la llamada Primavera Árabe, el Movimiento Indignado, El movimiento Occupy Wall Street, entre otros, son ejemplos del rol fundamental de los medios sociales en la difusión de información. Entendemos como medio social a las tecnologías web y móviles que se utilizan para convertir la comunicación en un diálogo interactivo (Hansen, Shneiderman, y Smith 2010). Algunos ejemplos de este tipo de tecnología son Facebook (una red social), Twitter (un servicio de micro-blogging) o YouTube (portal para compartir vídeos), sin embargo, hay miles de ejemplos adaptados a diferentes propósitos y audiencias. En la actualidad los medios sociales son los servicios con mayor crecimiento dentro de Internet (Bellenghem Steven Van 2011).

El creciente uso de los medios sociales implica un masivo volumen de datos personales volcados a la red, en el que día a día un mayor número de personas dejamos nuestro rastro cuando utilizamos estos servicios[1]. Los registros de la actividad se convierten entonces en un repositorio de datos de grandes dimensiones, el cual está al alcance de los científicos sociales para estudiar la sociedad. El masivo y creciente uso de la Red permite el conocimiento de fenómenos sociales a partir de lo que observamos en la red, un fenómeno al que autores como Rogers(2009) han denominado *online groundedness*. Un ejemplo es la posibilidad de inferir la inminencia de una epidemia de gripe si en un

1 Cada vez que realizamos una llamada, o que nos conectamos a internet, que creamos un perfil y utilizamos una red social o de microblogging estamos dejando rastros de nuestro comportamiento, de nuestras preferencias y opiniones que son almacenados y con los conocimientos y medios necesarios que son cada vez más accesibles pueden ser analizados.

conjunto de regiones de manera simultánea hay un pico de búsquedas en Google sobre antigripales, la cualcoincide con la búsqueda de los síntomas y tratamientos para la misma (Ginsberg et al. 2009, Butler 2013).

Esos rastros que dejamos en la red nos sirven para inferir fenómenos sociales es donde surge la relevancia del enfoque de *Big Data* para las ciencias sociales. «*Big Data*» es un término que pareciera centrar la atención sólo en el volumen de datos pero más allá del tamaño de nuestra de base datos, el valor del *Big Data* está es en las conexiones con otros datos del ámbito individual o grupal y los patrones que podemos identificar en su análisis (Boyd y Crawford 2011). *Big Data* surge como una nueva forma de aproximarse al conocimiento y en nuestro caso particular, a cómo se desarrollan los procesos de movilización y difusión. La observación y análisis de datos de medios sociales es un ejercicio que se adecúa perfectamente a las ventajas de los enfoques de *big data* en la medida en que éste permite analizar datos del momento exacto en los que se inicia una movilización en la red, qué camino sigue un mensaje y las características de la red.

1.3. Documentos para el análisis

Dado el volumen de artículos escritos sobre difusión de información en Twitter, concentramos nuestra atención en los primeros diez resultados de búsqueda en Google académico. Usamos diferentes términos de búsqueda con múltiples términos relacionados (difussion AND «Social Media»; difussion AND Twitter; Difussion AND «Social Networks»; Difusssion and Web 2.0; Difussion and «Social Movements», Difussion AND Mobilization, Difussion AND «Political Mobilization») los resultados para cada una de las búsquedas se filtraron bajo el criterio de relevancia[2.] El periodo de búsqueda fue 2007-2013 para en un primer momento obtener la bibliografía más actualizada. Esta búsqueda la hemos complementado con un proceso de bola de nieve localizando aquellos documentos citados como de alta relevancia por las primeras fuentes obtenidas a través de Google Académico sin limitarnos al periodo de búsqueda.

Proponemos una tipificación de los temas centrales en los artículos que hemos determinado como de mayor relevancia con el fin de ordenar nuestra revisión comparativa, tal como se propone en la tabla 2.

2 La relevancia para Google Académico sigue criterios muy parecidos a los de la mayoría de índices de impacto científico, para consultar con mayor detalle dirigirse a http://scholar.google.com/intl/en/scholar/about.html (01/03/2013) o a http://uiuc.libguides.com/content.php?pid=57231&sid=419094 (01/03/2013)

Tabla 2. Artículos revisados y propuesta de clasificación

Autores y artículo	**Preguntas**	**Difusión** **- Dinámicas de adopción / viralidad** **- Rutas de difusión** **- Masa crítica** **- Alcance** **- Velocidad**	**Atributos de la red**	**Atributos de los Nodos influyentes** **- poder/influencia** **- interno o externo a las redes** **- influencia contextual o global**	**Contenidos / memes** **- Novedad** **- concentración** **-Límites de atención**
Weng, L., Flammini, A., Vespignani, A., & Menczer, F. (2012) Competition among memes in a world with limited attention	Cuál es el rol de los límites de la atención en los usuarios en los procesos de difusión? Cuáles son los memes que logran captar la mayor atención? Afecta la competencia por la atención la popularidad, diversidad o tiempo de vida de los memes?				Los temas de mayor supervivencia dependen de los medios tradicionales y de sucesos reales. Pocos asuntos acaparan toda la atención.
González-Bailón, S., Borge-Holthoefer, J., Rivero, A., & Moreno, Y. (2011) The dynamics of protest recruitment through an online network	¿Cómo se relacionan los medios digitales con la difusión de la protesta? Cuál es el rol de los medios sociales en las procesos de difusión en convocatorias a la acción política y en organizar la acción colectiva? Cómo son los patrones de reclutamiento en la red social Twitter?		Topología de red de reclutamiento es heterogénea Centralidad no es requisito	Éxito de difusión requiere centralidad del nodo	
Goel, S., Watts, D. J., & Goldstein, D. G. (2012) The structure of online diffusion networks	Con qué frecuencia aparecen cascadas de información masivas en los procesos de difusión y qué proporción de la difusión se explica por procesos de dispersión virales frente a otro tipo de procesos	Sólo 10% de difusión es viral o logra grandes cascadas. Importancia de estudiar parámetros de bajo nivel de contagio que es la mayoría.			

Autores y artículo	**Preguntas**	**Difusión** **- Dinámicas de adopción / viralidad** **- Rutas de difusión** **- Masa crítica** **- Alcance** **- Velocidad**	**Atributos de la red**	**Atributos de los Nodos influyentes** **- poder/influencia** **- interno o externo a las redes** **- influencia contextual o global**	**Contenidos / memes** **- Novedad** **- concentración** **-Límites de atención**
Asur, S., Huberman, B. A., Szabo, G. & Wang, C. (2011) Trends in social media: Persistence and decay	¿Cuáles son los factores que contribuyen a la creación y evolución de tendencias? ¿Cómo es la distribución del número de tuits a través de los trending topics? De qué depende la persistencia de las tendencias? ¿Cuál es el impacto de los usuarios en la persistencia de tendencias en Twitter?				Medios sociales amplifican medios tradicionales. Atención a un tema es muy corta se privilegia:, Novedad. Eco en medios tradicionales.
Watts, D. J., & Dodds, P. S. (2007) Influentials, networks, and public opinion formation 3	¿En qué medida juegan un rol crítico grupos particulares de actores influyentes en formar y dirigir la opinión pública?	La mayoría de cascadas dependen de una masa crítica de individuos influenciables más que de un actor altamente influyente.		Explotar la influencia de manera excesiva lleva a la perdida de la misma	
Myers, S. A., Zhu, C., & Leskovec, J. (2012) Information diffusion and external influence in networks	¿Cómo interactúa la información transmitida por los medios masivos con la influencia personal que se da en los medios sociales? ¿Cuál es el nivel y tipo de interacción entre los medios sociales y los medios tradicionales para favorecer la movilización y un mayor alcance de la difusión?		Un 30% de la difusión depende de los medios tradicionales o de efectos externos a la red social		
Huberman, B., Romero, D., & Wu, F. (2008)e Social networks that matter: Twitter under the microscope 3	¿Cuál es la naturaleza de las redes sociales que finalmente importan a los usuarios de Twitter?		El proceso determinante de uso es una red difusa e implícita que existe de forma paralela con los nexos oficiales de amigos y seguidores		

Autores y artículo	**Preguntas**	**Difusión** **- Dinámicas de adopción / viralidad** **- Rutas de difusión** **- Masa crítica** **- Alcance** **- Velocidad**	**Atributos de la red**	**Atributos de los Nodos influyentes** **- poder/influencia** **- interno o externo a las redes** **- influencia contextual o global**	**Contenidos / memes** **- Novedad** **- concentración** **-Límites de atención**
Colbaugh, R., & Glass, K. (2010) Early warning analysis for social diffusion events	¿Qué tipo de relaciones se presentan entre los actores que se movilizan?	Un proceso temprano de difusión entre comunidades es un indicador fiable que la difusión implicará un número sustancial de individuos	Unos pocos vinculos entre comunidades pueden lograr que la difusión de una comunidad se replique		
Leskovec, J., Backstrom, L., & Kleinberg, J. (2009) Meme-tracking and the dynamics of the news cycle	¿Cómo el seguimiento de memes entre medios tradicionales y sociales permite identificar los ciclos de noticias?	Existe un retraso típico de 2,5 horas entre el pico de atención de un meme en medios tradicionales y en medios sociales			La mayoría de memes surgen en medios tradicionales
Cha, M., Haddadi, H., Benevenuto, F., & Gummadi, K. P. (2010) Measuring user influence in twitter: The million follower fallacy	¿Quién o quiénes son los actores principales en los procesos de difusión de un evento?			1.Alto nivel de seguidores no implica ser influyente en términos de retweets y menciones. 2. Los actores más influyentes lo son en varios temas. 3. La influencia no es espontanea se gana posicionándose en un tema.	
Wu, F. & Huberman, B. J. (2010) A persistence paradox	¿Cuáles son los principales temas y marcos asociados a un proceso de difusión en torno a un evento o asunto?	La novedad de un tema determina la velocidad de difusión			La atención decae con la pérdida de novedad de los temas
Romero, D. M., Meeder, B. & Kleinberg, J. (2011) Differences in the Mechanics of Information Diffusion Across Topics: Idioms, Political Hashtags, and Complex Contagion on Twitter	¿Cómo se difunden diferentes tipos de información on-line? ¿De qué manera se difunden los hashtags en redes definidas por la interacción de usuarios de Twitter?			Influencia en la generación de contenido de alta resonancia entre seguidores causa la propagación y aumento de popularidad	

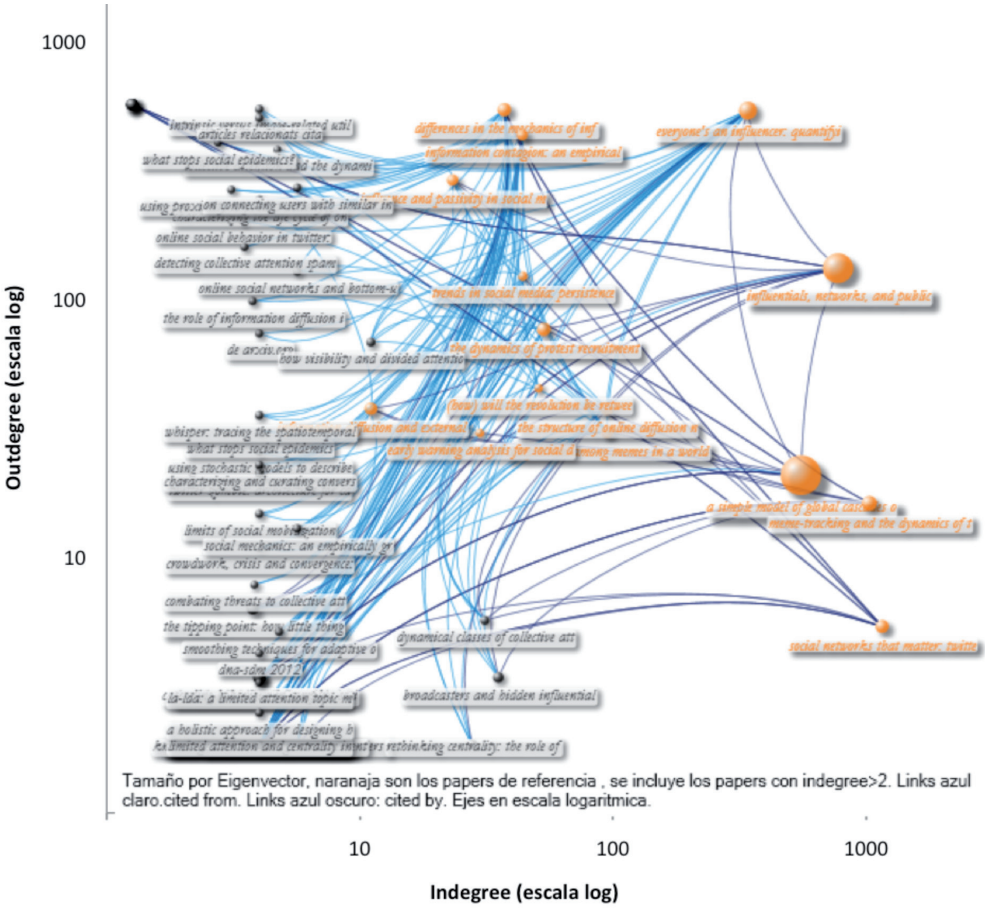
Autores y artículo	**Preguntas**	**Difusión** **- Dinámicas de adopción / viralidad** **- Rutas de difusión** **- Masa crítica** **- Alcance** **- Velocidad**	**Atributos de la red**	**Atributos de los Nodos influyentes** **- poder/influencia** **- interno o externo a las redes** **- influencia contextual o global**	**Contenidos / memes** **- Novedad** **- concentración** **-Límites de atención**
Romero, D. M., Galuba, W., Asur, S. & Huberman, B. A. (2011) Influence and passivity in social media	¿Qué determina la atención y la influencia de los usuarios de Twitter?			Correlación débil entre popularidad e influencia. Para ser influyente es necesario obtener popularidad y superar la pasividad	
Wu, F., & Huberman, B. A. (2007) Novelty and collective attention	¿Cómo se propaga la atención a eventos novedosos y eventualmente desaparece en poblaciones grandes? (DIGG)				
Starbird, K., & Palen, L. (2012) (How) will the revolution be retweeted?: information diffusion and the 2011 Egyptian uprising.	¿Cómo se difunde información a través de Twitter en procesos de protesta en especial a través de retweets?				Los retweets identifican información novedosa
Bakshy, E., Hofman, J. M., Mason, W. A. & Watts, D. J. (2011) Everyone's an Influencer: Quantifying Influence on Twitter	Cuáles son los atributos y la influencia relativa de los usuarios de Twitter en eventos de difusión?			Los usuarios comunes pueden ser tan influyente como los líderes de opinión Importancia de campañas boca a boca	
Watts, D. J. A (2002) Simple model of global cascades on random networks 4	¿Cómo pueden explicarse atributos genéricos de las cascadas en términos de la conectividad de la red en la cual la influencia se transmite entre individuos?	La novedad de los contenidos aumenta la velocidad de difusión			La novedad de los contenidos se agota con el tiempo y pierde atención
Lerman, K. & Ghosh, R. (2010) Information contagion: an empirical study of the spread of news on digg and twitter social networks	¿Cómo afecta la estructura de la red las dinámicas de dispersión de información?	Los usuarios siguen las acciones de amigos y la hacen visible a sus propios amigos y seguidores			

A partir de los documentos incluidos en la tabla 2, realizamos un análisis de redes, utilizándolos como semillas para identificar referencias comunes entre ellos. Primero listamos las referencias de todos los documentos (out degree) y en segundo lugar, identificamos todos los documentos que citan nuestros documentos de interés en Google Académico (indegree). Los objetivos de este análisis son confirmar la relevancia de los documentos incluidos en la tabla número 2 e identificar los artículos más influyentes en términos de su nivel de su centralidad de vector propio dentro del tema de difusión y *Big Data*. Con este indicador podemos identificar la influencia del artículo por la relevancia de la citas que ha recibido dentro de los artículos más relevantes del tema. Este análisis de redes de referencia va más allá del simple número de citas que recibe cada artículo, en cuanto reconoce la importancia de ser citado por un documento altamente popular frente a serlo por uno prácticamente desconocido y poco citado.

La red obtenida está compuesta por 2878 artículos (nodos) y 3553 referencias (aristas) – Gráfico 1. Es una red compacta, con la separación máxima entre los dos artículos más alejados en la red es de cinco grados. Los cinco artículos más influyentes en el tema en orden de importancia de acuerdo a su nivel de eigenvector son: «A simple model of global cascades on random networks», «Influentials, networks, and public opinion formation», «Everyone's an influencer: quantifying influence on twitter», «Meme-tracking and the dynamics of the news cycle» y «The dynamics of protest recruitment through an online network». A partir de los resultados del análisis, podemos confirmar que los artículos que seleccionamos inicialmente (nodos color naranja) son centrales dentro del tema de estudio (delimitado por los términos de búsqueda «difusión» y «social media»). Adicionalmente, podemos identificar cuatro artículos nuevos que reciben un alto nivel de referencias conjuntas: se trata de artículos de los mismos autores (Broadcasters and Hidden Influentials… - Gonzáles et al.) o de artículos relacionados a nivel temático (Dynamical classes of Collective Action, Rethinking centrality: the role of dynamical processes in social network analysis, y How visibility and divided attention constrain social contagion).

Las redes de referencias conjuntas indican además una afinidad temática y disciplinar dentro de los artículos elegidos. Esto confirma nuestro interés por buscar conexiones entre los estudios de las ciencias de la computación interesados principalmente en las estructuras de las redes y las dinámicas de la información y los estudios sociológicos y politológicos que estudian procesos y casos particulares en la movilización social. Esta confirmación nos permite proceder con la revisión de la literatura con mayor certeza sobre el conjunto de artículos elegidos para nuestro propósito.

Gráfico 1. Ego networks de 18 artículos influyentes en difusión y *big data*. Mayo 2013



Fuente: Diseño propio a partir de los artículos de la tabla 1 y sus referencias en Google Académico.

2. REVISIÓN DE LA LITERATURA

2.1. Enfoques y preguntas

2.1.1. Limitaciones de los enfoques tradicionales

En los estudios de movilización tradicionales[3], y puntualmente de difusión, era muy difícil establecer de manera precisa cómo los procesos de difusión virales se dan en múltiples pasos (Watts y Dodds 2007) Sin los registros de la actividad online, resultaba imposible observar la red de difusión y las únicas formas de recrear la red era entrevistando a líderes activistas o encuestando personas que hubiesen participado en la movilización o mediante análisis históricos de contenido en prensa como la investigación pionera de McAdam (1983). Estos métodos de obtención de información presentan diferentes sesgos y pérdida de información. Años antes del desarrollo de Twitter y cuando la Web no presentaba las tasas de penetración de uso actuales[4], autores especializados en estudios de protesta como Myers y Olivers (1998) ya señalaban las dificultades metodológicas de acceder a datos precisos, y en particular datos que tuviesen información del tipo de relación entre los individuos que se movilizaban, la dirección que presentaba el flujo de información y en qué momento exacto se había presentado el proceso de difusión. Esta información permitiría establecer por lo menos la red de difusión y la secuencia cronológica del proceso.

Otro sesgo en los estudios que recurren a métodos tradicionales es que la mayoría de estos se han concentrado en eventos de movilización exitosos (Watts y Dodds 2007), dado que el seguimiento sólo era posible para eventos de grandes dimensiones y cubrimiento detallado, eventos que el investigador pudiese conocer de su existencia y obtener un registro de este. Es el caso de las reivindicaciones de derechos civiles por la población afro (McAdam 1983), los movimientos transnacionales antiglobalización (Tarrow y Della Porta 2005) o las protestas de los veranos calientes en Estados Unidos (Myers 1997) entre otros. No obstante, los factores que supuestamente explicaban el éxito de este tipo de eventos sólo representaban a los eventos exitosos, pero no una muestra representativa que permitiera contrastar si estos mismos factores se presen-

3 Con estudios de difusión tradicionales hacemos referencia a aquellas investigaciones usualmente desarrolladas antes de alcanzar los niveles de penetración de usuarios de la Web y medios sociales actuales de occidente y que entre sus técnicas de obtención de datos recurrían a entrevistas o encuestas entre los actores involucrados en el evento movilizador. Técnicas muy valiosas para obtener información sociodemográfica, de la percepción del evento por parte del entrevistado, de las razones para movilizarse y de las estrategias y técnicas utilizadas para movilizar. No obstante, dependían de la buena memoria y honestidad del entrevistado para identificar con precisión de quien había recibido información sobre la movilización y a quién le habían transmitido información sobre la misma.

4 Fundamentalmente en países de la OCDE, en todos la tasa de penetración de Internet supera el 50% de la población. (Internet World Stats 2011).

taban en iniciativas de movilización y difusión que no habían llegado a tener ningún tipo de trascendencia. Ante estos desafíos metodológicos, el análisis de fenómenos de difusión a través de medios sociales y en particular Twitter con el enfoque de *Big Data* ha permitido dar respuesta tanto a preguntas clásicas de la literatura de movimientos sociales, así como abordar nuevos interrogantes y ofrecer explicaciones más precisas a aspectos de los fenómenos de movilización.

2.1.2. Preguntas clásicas abordadas desde el enfoque de Big Data

Las preguntas clásicas de la literatura en el estudio de la difusión y la protesta han ido evolucionando y podrían centralizarse en ¿quién o quiénes son los actores principales en los procesos de difusión de un evento? (Cha et al. 2010; Myers, Zhu, y Leskovec 2012) ¿Qué tipo de relaciones se presentan entre estos actores? (Colbaugh y Glass 2010; Starbird y Palen 2012) o ¿Cuáles son los principales temas y marcos asociados al proceso de difusión entorno a un evento o asunto? (Asur et al. 2011).

2.1.3. Nuevas preguntas, nuevas explicaciones a antiguos fenómenos

La capacidad de precisar en estas cuestiones permite abordar otras preguntas tales como ¿Cuál es la frecuencia en que se presentan fenómenos virales de transmisión de información?, ¿Qué tan frecuentes son las grandes cascadas en los procesos de difusión?, ¿Cuál es el nivel de adopción que estas representan?(Goel, Watts, y Goldstein 2012), ¿Qué temas y memes logran captar una mayor atención? (Weng et al. 2012) ¿Cuál es el rol de los medios sociales y en especial de Twitter en el proceso de difusión en convocatorias a la acción política y en organizar la acción colectiva? (González-Bailón et al. 2011) ; ¿Cuál es el nivel y tipo de interacción entre los medios sociales y medios tradicionales para favorecer la movilización y un mayor alcance de la difusión? (Myers, Zhu, y Leskovec 2012)

En cuanto a aspectos de la movilización que es posible explicar de una forma más precisa con el enfoque de *Big Data* está el análisis de la estructura y dinámica que presentan las redes de difusión (Goel, Watts, y Goldstein 2012), comparar los tipos de contenidos que se difunden para establecer que contenidos tienen mayor aceptación que otros(Leskovec, Backstrom, y Kleinberg 2009; Weng et al. 2012), también es posible comparar iniciativas de difusión exitosas con iniciativas de difusión inadvertidas (Goel, Watts, y Goldstein 2012; Wu et al. 2011) Exitosas en términos de la amplia movilización y eco que alcanzan, e iniciativas inadvertidas por su bajo impacto movilizador y mediático. A las iniciativas inadvertidas de movilización sólo es posible acceder a través del registro en medios sociales cómo Twitter.

2.2. Aproximaciones teóricas de las ciencias sociales

Los procesos de difusión han jugado un rol determinante dentro de las teorías de movilización en los estudios de movimientos sociales. La difusión de diferentes tipos de

información hace parte de cualquiera de líneas centrales de estudio con enfoques racionalista, estructuralista y culturalista o de psicología social.

Estas líneas han dominado las teorías de movilización en las ciencias sociales, con diferentes énfasis en las disciplinas de la sociología, la psicología social, las comunicaciones y la ciencia política. En la movilización de recursos (McCarthy & Zald, 1977; Zald & McCarthy, 1979) las organizaciones juegan el rol central en la coordinación de la acción colectiva al proveer los incentivos para que los individuos formen parte de las causas comunes. El desarrollo y comportamiento de los actores se estudia como una interacción entre factores internos a las organizaciones/movimientos (Liderazgo, recursos, organización) y las instituciones y circunstancias en las cuales se desarrollan (Oportunidades políticas, represión social, grupos de presión,…). Es una visión que se enfoca en el paradigma racionalista y busca explicar de qué manera se centraliza el control de recursos de un grupo para sobrellevar los costos individuales de la participación. De esta manera, las organizaciones juegan un rol centra en los procesos de difusión al asumir los roles de construcción de redes, planeación logística de las acciones de grupo e intermediación.

Una condición central para la movilización es la existencia de redes interpersonales densas, en cuanto éstas aportan la estructura para los incentivos colectivos. Varios estudios de caso identifican la relevancia de los vínculos entre organizaciones como alternativa a la importancia de los actores centrales. (Colbaugh y Glass 2010; Strang y Soule 1998) De esta manera, la teoría de movilización de recursos también abarca enfoques estructuralistas y se alinea con estudios como los de Passy que aportan evidencia sobre la importancia de la fortaleza de los vínculos para explicar la participación de individuos conectados en comparación con quienes se encuentran aislados, de igual forma resalta la importancia de vínculos débiles para un mayor alcance de la difusión de la movilización (Passy 2003)

El enfoque de estructuras puede verse como un complemento de las explicaciones centradas en las motivaciones individuales y grupales y los procesos de identificación desde una aproximación de la psicología. Permite comprender los niveles agregados y aporta explicaciones sobre los procesos de influencia y socialización. El enfoque de marcos de acción colectiva (Benford & Snow, 2000) se centra en la producción de contenidos y marcos de interpretación que proveen significados centrales en la definición de los grupos, sus posibilidades de acción y legitiman sus acciones. La importancia de las prácticas retóricas y discursivas es parte integral de los procesos comunicativos. Por esta razón se complementa con el estudio de las estructuras en las cuales se dan procesos comunicativos tales como la difusión de información.

El enfoque culturalista comprende las teorías de la identidad social (Turner, Oakes, Haslam, & McGarty, 1994). Éstas proveen explicaciones en términos de procesos de grupo en contraposición a los enfoques de colectivos de individuos. Los conceptos de identidades de grupo, pertenencia y las diferencias entre «nosotros y ellos» aportan una

visión distinta de la manera como se dan las interacciones sociales. La identidad social juega un rol diferente a la identidad individual. En este sentido, esta perspectiva resulta fundamental para comprender los procesos de influencia que se dan de manera masiva, los procesos de liderazgo grupal (Reicher et al. 2005), las interacciones individuales que determinan la identidad grupal (Postmes et al. 2005) y las dinámicas que determinan las estructuras de red, tales como la polarización.

3. FUTURAS LÍNEAS DE INVESTIGACIÓN

En esta sección presentamos cuestiones comunes en la investigación sobre procesos de difusión en movimiento sociales y medios sociales. A partir de estos temas y hallazgos comunes proponemos futuras líneas de investigación basadas en los enfoques de *Big Data* sobre las cuestiones de dinámicas de difusión, estructura de las redes, atributos relevantes de los nodos en los procesos de difusión y propiedades de los contenidos.

Con respecto a las dinámicas de difusión, los hallazgos sobre los procesos de cascadas de información aportan evidencia contraria a la importancia que se ha otorgado a los medios sociales como espacios de transformación de las dinámicas tradicionales (Goel, Watts & Goldstein 2012). Las dinámicas de difusión de información en medios sociales no respaldan las interpretaciones más optimistas sobre el rol de Twitter en las protestas que han llevado a la ocupación de las plazas públicas en los últimos años alrededor del mundo.

En cuanto a los hallazgos sobre las propiedades de las redes de movilización, el uso de registros de actividad en los medios sociales y las aproximaciones de *Big Data* serán útiles para identificar dinámicas de interacción que den cuenta de hallazgos estructurales consistentes entre estudios de caso (McAdam 2003). De la misma forma, establecer de manera rigurosa los atributos relevantes de las redes para los procesos de difusión permite un mejor entendimiento del comportamiento de los actores y de los factores en un nivel meso. Una cuestión de especial interés es la importancia de las conexiones formales y las estructuras sociales estables en contraposición con las redes efectivas de interacción. Si las redes estables se han identificado ampliamente como el escenario propicio para el desarrollo de la actividad contenciosa (McCarthy, 1996), al igual que la fortaleza de los vínculos (Patsy, Gould 2003), la capacidad movilizadora de los medios sociales puede establecerse a partir del análisis de dinámicas de difusión en redes dispersas e informales.

Esa lógica es igualmente válida para los atributos de los individuos. Los enfoques de *Big data* permiten establecer la incidencia de la posición de los individuos en la red en su capacidad de influencia en los procesos de difusión. La capacidad de establecer que usuarios comunes pueden ser tan influyentes como los líderes de opinión (Bakshy et al 2011), o que ciertas posiciones en la red favorecen mayores tasas de difusión (González-Bailón et al. 2011) son hallazgos de gran relevancia para probar en diferentes asuntos y contextos de movilización.

Los estudios que han abordado los contenidos como elemento central de los procesos de difusión y las estructuras de redes tienen a su vez una relevancia directa en el estudio de los marcos de acción colectiva. Los avances en el estudio sobre la economía de la atención generan respuestas a cuestiones clásicas como la prominencia de los asuntos como factores determinantes para la movilización. Aunque los límites de atención se vuelvan un tema especialmente relevante en las redes sociales online, el estudio de los procesos de marcos de interpretación se ha desarrollado desde su origen en referencia a los marcos mediáticos. La identificación de factores exógenos y especialmente la difusión que tienen los memes en medios tradicionales (Weng et al 2012; Asur 2011 y Wu et al. 2010) conlleva una revisión del rol de las organizaciones y de su interacción con los líderes mediáticos en los medios sociales.

A pesar del éxito ante las nuevas preguntas y la cantidad de investigaciones producidas en relación al tema de difusión y enfoque de *Big Data* en medios sociales, desde la literatura de movimientos sociales se precisa que la difusión va más allá de la simple transmisión de información. Earl (2010) propone diferentes clases de difusión en la movilización social: 1-la difusión de información, 2-la difusión de tácticas y formas de protesta y 3- la difusión de la protesta en sí misma a otras poblaciones, cómo una forma de resolver un problema desafiando guiones, esquemas y prácticas en determinado contexto. Uno de nuestro argumentos centrales es que un eje común entre las investigaciones que han utilizado el enfoque de *Big Data* con los estudios sobre movilización, es qué los primeros centran su atención en la difusión de información. El conjunto de preguntas, nuevas explicaciones e interrogantes que se ofrecen desde *Big Data* se centran en esta clase difusión. Los papers identificados como de mayor influencia siguen esta tendencia.

Depende del tipo de difusión que estemos analizando la aproximación de *Big Data* parece ofrecer más o menos resultados. En el mejor de nuestros conocimientos, la aproximación de *Big Data* no parece haber abordado el estudio de los procesos de difusión de segunda y tercera clase. Lo que Earl denomina como difusión de segundo orden. Su énfasis en los procesos informativos responde al enfoque en prácticas comunicativas. La difusión de segunda y tercera clase no es algo que se transmita cómo la información de un mensaje pues implica un periodo de aprendizaje y adaptación para que el grupo que se moviliza pueda interiorizar las prácticas y tácticas que ha observado en otros escenarios (Earl 2010; Oliver y Myers 1998)

Las investigaciones que involucran la difusión de segundo orden con aproximaciones como las de *Big Data* tienen todavía fuertes limitaciones, por lo menos a la luz de la tecnología actual. Un ejemplo es lograr recrear de forma exacta los diferentes pasos que sigue la transmisión de prácticas y estrategias entre un grupo a otro. Un enfoque metodológico tradicional podrá realizar un estudio longitudinal, identificando en los dos o más grupos bajo observación prácticas comunes pero que difieran en el tiempo, y de acuerdo al orden temporal de las mismas asumir su causalidad. Pero contrario a los estudios de *Big Data* en difusión de la información, está la duda de poder establecer con precisión quien enseño a

quien, o si a pesar de darse una práctica en un evento en otro orden temporal esta no sea resultado de una iniciativa individual, una coincidencia que se parezca a la práctica del otro grupo. Para dar respuesta a estas cuestiones resultaría más sencillo y tal vez eficiente entrevistar a los diferentes organizadores y contrastar sus respuestas para poder identificar un proceso de intercambio y aprendizaje de un grupo a otro, que analizar masivamente todo la información que esté disponible en la red sobre ellos. En este sentido, los enfoques de *Big Data* presentarían limitaciones para analizar la difusión de segundo orden.

4. DESAFÍOS METODOLÓGICOS

En estudios por ejemplo sobre memes y en general que involucren difusión de contenidos, tener en cuenta el contexto es fundamental, por ejemplo en lo que corresponde a ciertos usos del lenguaje, a dialectos, sarcasmo o ironías que a luz de la tecnología actual todavía es un reto en determinar por un ordenador el doble sentido con el que el lenguaje puede utilizarse. Evidentemente para cada caso particular los algoritmos se podrán ajustar y determinar que palabras claves presentadas de cierta manera pueden tener un significado diferente de su definición literal, lo que significa que el criterio del investigador y su experiencia tienen un rol crítico.

Un aspecto que tampoco debemos olvidar es el importante y subjetivo ejercicio de interpretación que exigen los datos, tal como exponen Boyd y Crawford (2011) se presenta la falsa creencia que por el hecho de manejar grandes volúmenes de datos , los científicos sociales nos acercamos más al anhelo del cuantitativismo de las mal llamadas ciencias exactas. Más cuando uno de los desafíos centrales está en la difusión de prácticas, contenidos, y formas de aprendizaje que difícilmente pueden ser ajenas de la lectura del científico que interpreta las observaciones.

En esta línea los investigadores debemos ser capaces de dar cuenta de los sesgos en la interpretación de los datos Todos los investigadores somos intérpretes de datos. Un modelo puede ser matemáticamente sólido, un experimento puede parecer válido, pero tan pronto como investigador trata de comprender lo que significa, el proceso de interpretación ha comenzado. Las decisiones del diseño que determinan lo que se medirá también se derivan de la interpretación y a veces esto se nos olvida.

En este sentido tal como lo plantea Boyd and Crawford (2011) es necesario un mayor dominio de las técnicas de obtención y análisis de datos en *Big Data* por parte de los científicos sociales, para poder contribuir en el desarrollo y crítica a este enfoqué. Además es esencial la aproximación multi-método dejando a un lado divisiones artificiales entre enfoques cuantitativos o cualitativos, en la medida en que el enfoque de *Big data* es integrador y exige los dos enfoques para diferenciar procesos de difusión como aquellos que mencionamos de diferentes aproximaciones. En este aspecto existe una amplia veta por explorar.

Por otra parte hay aspectos de carácter técnico, económico y legal para acceder como en los inicios de Twitter a grandes bases de datos y en general datos de los diferentes medios sociales. Primero las restricciones cada vez mayores de las diferentes API[5] para acceder a los datos y donde la obtención de los mismos puede llegar a tener problemas en momentos de mayor movilización, segundo los problemas de muestreo que se ve afectado por el tipo de API que utilicemos (Gonzalez-Bailon et al. 2012) cómo de la características de la red de datos que finalmente obtengamos (De Choudhury et al. 2010). Si no tenemos conocimiento de las características de la población y un adecuado acceso a los datos (por el API que utilicemos y la red que logremos obtener), no tendremos garantía de contar con una muestra representativa. De igual forma una muestra con un gran volumen de datos no es garantía de representatividad. Un conjunto de datos puede tener millones de observaciones, pero esto no quiere decir que sea aleatoria y representativa. Lo que llevará a problemas de validez en el momento de aspirar a extrapolar nuestros posibles descubrimientos más allá de la muestra con la que contemos.

Esto exige la comprensión del origen, las propiedades y los límites de nuestro conjunto de datos, independientemente de su tamaño. Tener en cuenta que por ejemplo a pesar del éxito que pueda presentar servicios como Twitter en términos de su tasas de crecimiento, ciertos medios sociales son más utilizados por determinadas franjas de la población o en ciertas regiones del mundo medios sociales que son muy populares en otras no lo son. Sumado a esto la división digital (Norris 2001) que se presenta entre diferentes regiones consecuencia de diferentes niveles de educación e ingresos, así como la división digital entre generaciones de una misma región. En este sentido es crucial saber de dónde provienen nuestros datos así como conocer y dar cuenta de las deficiencias de los mismos. Además si nuestra investigación requiere de acceder a datos históricos, en el caso de Twitter sólo unas pocas empresas como Gnip o Datasift los suministran a un coste económico que no todos los investigadores pueden asumir. En términos de cuestiones legales, es necesario esperar que se levante el embargo sobre los Tweets históricos que Twitter ha cedido a la biblioteca del Congreso de los Estados Unidos.

Un último aspecto legal y de ética en la investigación es la necesidad de garantizar el criterio de anonimidad en datos personales para evitar el acceso de terceras partes. Sin embargo un exceso de protección de los datos puede generar otro problema: la garantía de replicar procedimientos y resultados en la academia. Un principio esencial del desarrollo científico y más en un enfoque tan reciente y novedoso como el de *Big Data*.

5 Application Programming Interface

REFERENCIAS

Asur, S., B. A. Huberman, G. Szabo, y C. Wang. 2011. «Trends in social media: Persistence and decay». En *5th International AAAI Conference on Weblogs and Social Media*, http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2815/3205 (22 de noviembre de 2012).

Bellenghem Steven Van. 2011. *Social media around the world 2011*. Insites consulting. http://www.slideshare.net/stevenvanbelleghem/social-media-around-the-world-2011 (28 de noviembre de 2011).

Bennett, W. Lance, y Alexandra Segerberg. 2012. «THE LOGIC OF CONNECTIVE ACTION». *Information, Communication & Society*: 1-30.

Boyd, D., y K. Crawford. 2011. «Six provocations for big data». http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431 (17 de octubre de 2012).

Cha, Meeyoung, Hamed Haddadi, Fabricio Benevenuto, y Krishna P. Gummadi. 2010. «Measuring user influence in twitter: The million follower fallacy». En *4th international aaai conference on weblogs and social media (icwsm)*, , 8. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM10/paper/download/1538/1826 (18 de febrero de 2013).

De Choudhury, M., Y. R. Lin, H. Sundaram, K. S. Candan, L. Xie, y A. Kelliher. 2010. «How does the data sampling strategy impact the discovery of information diffusion in social media». En *Proceedings of the 4th International AAAI Conference on Weblogs and Social Media*, , 34-41. http://www.aaai.org/ocs/index.php/ICWSM/ICWSM10/paper/viewFile/1521/1832 (25 de octubre de 2012).

Colbaugh, Richard, y Kristin Glass. 2010. «Early warning analysis for social diffusion events». En IEEE, 37-42. https://xpv.uab.cat/xpl/,DanaInfo=.aifgh1urvznJtqrsO48y+articleDetails.jsp?arnumber=5484778 (28 de febrero de 2013).

Earl, Jennifer. 2010. «The Dynamics of Protest-Related Diffusion on the Web». *Information, Communication & Society* 13(2): 209-25.

Gilad Lotan, Erhardt Graeff, Mike Ananny, Devin Gaffney, Ian Pearce, y danah boyd. 2011. «The Arab Spring| The Revolutions Were Tweeted: Information Flows during the 2011 Tunisian and Egyptian Revolutions». *International Journal of Communication; Vol 5 (2011)*. http://www.ijoc.org/ojs/index.php/ijoc/article/view/1246/643 (1 de enero de 2011).

Ginsberg, Jeremy, Matthew H. Mohebbi, Rajan S. Patel, Lynnette Brammer, Mark S. Smolinski, y Larry Brilliant. 2009. «Detecting Influenza Epidemics Using Search Engine Query Data». *Nature* 457(7232): 1012-14.

Givan, Rebecca Kolins, Kenneth M Roberts, y Sarah Anne Soule. 2010. *The diffusion of social movements: actors, mechanisms, and political effects*. Cambridge; New York: Cambridge University Press.

GlobalWebIndex. 2012. «World social media users». http://globalwebindex.net/thinking/social-platforms-gwi-8-update-decline-of-local-social-media-platforms/ (6 de marzo de 2013).

Goel, Sharad, Duncan J. Watts, y Daniel G. Goldstein. 2012. «The structure of online diffusion networks». En *Proceedings of the 13th ACM Conference on Electronic Commerce*, EC '12, New York, NY, USA: ACM, 623-38. http://doi.acm.org/10.1145/2229012.2229058 (16 de noviembre de 2012).

González-Bailón, Sandra, Javier Borge-Holthoefer, Alejandro Rivero, y Yamir Moreno. 2011. «The Dynamics of Protest Recruitment Through an Online Network». *Scientific Reports* 1. http://www.nature.com/srep/2011/111215/srep00197/full/srep00197.html (12 de noviembre de 2012).

Gonzalez-Bailon, Sandra, Ning Wang, Alejandro Rivero, Javier Borge-Holthoefer, y Yamir Moreno. 2012. «Assessing the Bias in Communication Networks Sampled from Twitter». *SSRN eLibrary*. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2185134 (10 de diciembre de 2012).

Hansen, Derek, Ben Shneiderman, y Marc A. Smith. 2010. *Analyzing Social Media Networks with NodeXL: Insights from a Connected World*. Morgan Kaufmann.

Khamis, S., y K. Vaughn. 2011. «Cyberactivism in the Egyptian Revolution: How Civic Engagement and Citizen Journalism Tilted the Balance». *Arab Media & Society* 13.

Kim, Hyojoung, y Peter S. Bearman. 1997. «The Structure and Dynamics of Movement Participation». *American Sociological Review* 62(1): 70-93.

Leskovec, Jure, Lars Backstrom, y Jon Kleinberg. 2009. «Meme-tracking and the dynamics of the news cycle». En *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD '09, New York, NY, USA: ACM, 497-506.

McAdam, Doug. 1983. «Tactical Innovation and the Pace of Insurgency». *American Sociological Review* 48(6): 735-54.

Myers, Daniel. 1997. «Racial Rioting in the 1960S: An Event History Analysis of Local Conditions». *American Sociological Review* 62(1): 94-112.

Myers, Seth A., Chenguang Zhu, y Jure Leskovec. 2012. «Information diffusion and external influence in networks». En *Proceedings of the 18th ACM SIGKDD international conference on Knowledge discovery and data mining*, , 33-41. http://dl.acm.org/citation.cfm?id=2339540 (14 de febrero de 2013).

Norris, Pippa. 2001. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*. Cambridge: Cambridge University Press.

Oliver, Pamela E., y Daniel J. Myers. 1998. «Diffusion Models of Cycles of Protest as a Theory of Social Movements». *National Defense University*. http://www.ssc.wisc.edu/~oliver/PROTESTS/ArticleCopies/isaf.pdf (15 de febrero de 2013).

Papacharissi, Zizi, y Maria de Fatima Oliveira. 2012. «Affective News and Networked Publics: The Rhythms of News Storytelling on #Egypt». *Journal of Communication* 62(2): 266-82.

Passy, F. (2003). Social networks matter. But how?. Social movements and networks: Relational approaches to collective action, 21-48.

Porta, Donatella della, y Sidney Tarrow. 2012. «Interactive Diffusion The Coevolution of Police and Protest Behavior With an Application to Transnational Contention». *Comparative Political Studies* 45(1): 119-52.

Postmes, Haslam, & Swaab. (2005). Social influence in small groups: An interactive model of social identity formation. European Review of Social Psychology, 16(1), 1-42.

Reicher, S., Haslam, S. A., & Hopkins, N. (2005). Social identity and the dynamics of leadership: Leaders and followers as collaborative agents in the transformation of social reality. The Leadership Quarterly, 16(4), 547-568.

Rogers, Everett M. 2010. *Diffusion of Innovations, 4th Edition*. Simon and Schuster.

Rogers, R. 2009. «The End of the Virtual Digital Methods». En University of Amsterdam, 1-37. http://www.govcom.org/publications/full_list/oratie_Rogers_2009_preprint.pdf.

Romero. , Galuba, W., Asur. & Huberman, B. (2011). Influence and passivity in social media. Machine Learning and Knowledge Discovery in Databases, 18-33.

Romero, Meeder., & Kleinberg. (2011, March). Differences in the mechanics of information diffusion across topics: idioms, political hashtags, and complex contagion on twitter. In Proceedings of the 20th international conference on World wide web (pp. 695-704). ACM.

Starbird, Kate, y Leysia Palen. 2012. «(How) will the revolution be retweeted?» En ACM Press, 7. https://xpv.uab.cat/,DanaInfo=.admBdgrFvzp+citation.cfm?id=2145204.2145212&coll=DL&dl=ACM&CFID=285782505&CFTOKEN=40726355 (28 de febrero de 2013).

Strang, David, y John W. Meyer. 1993. «Institutional Conditions for Diffusion». *Theory and Society* 22(4): 487-511.

Strang, David, y Sarah A. Soule. 1998. «Diffusion in Organizations and Social Movements: From Hybrid Corn to Poison Pills». *Annual Review of Sociology* 24: 265-90.

Tarrow., y Della Porta. 2005. «Transnational Protest and Social Activism: An Introducction». En *Transnational Protest and Global Activism*, eds. Donatella della Porta y Sidney G Tarrow. Lanham [etc.]: Rowman & Littlefield Publishers, 1-20.

Turner., Oakes, Haslam, & McGarty (1994). Self and collective: Cognition and social context. Personality and social psychology bulletin, 20, 454-454.

Watts, Duncan J., y Peter Sheridan Dodds. 2007. «Influentials, Networks, and Public Opinion Formation». *Journal of Consumer Research* 34(4): 441-58.

Weng, L., A. Flammini, A. Vespignani, y F. Menczer. 2012. «Competition Among Memes in a World with Limited Attention». *Scientific Reports* 2. http://www.nature.com/srep/2012/120329/srep00335/full/srep00335.html (8 de noviembre de 2012).

Wu, Shaomei, Jake M. Hofman, Winter A. Mason, y Duncan J. Watts. 2011. «Who says what to whom on twitter». En *Proceedings of the 20th international conference on World wide web*, WWW '11, New York, NY, USA: ACM, 705-14. http://doi.acm.org/10.1145/1963405.1963504 (16 de noviembre de 2012).

Big Data: Retos y Oportunidades

Actas del *IX Congreso Internacional Internet, Derecho y Política (IDP 2013)*

ISBN: 978-84-695-8160-5

Para citar la obra, por favor, utilicen las siguientes referencias indistintamente:

Balcells Padullés, J., Cerrillo-i-Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J. & Vilasau Solana, M. (coords.) (2013). *Big Data: Retos y Oportunidades*. Actas del IX Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 25-26 junio, 2013. Barcelona: UOC-Huygens Editorial.

Balcells Padullés, J., Cerrillo-i-Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J. & Vilasau Solana, M. (coords.) (2013). *Big Data: Challenges and Opportunities*. Proceedings of the 9th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 25-26 June, 2013. Barcelona: UOC-Huygens Editorial.

http://edcp.uoc.edu/symposia/idp2013/proceedings/

UOC Universitat Oberta de Catalunya www.uoc.edu

HUYGENS EDITORIAL