



Retos y oportunidades del
**Entretenimiento
en línea**

Actas del VIII Congreso Internacional Internet, Derecho y Política
Universitat Oberta de Catalunya. Barcelona, 9-10 Julio, 2012

Challenges and Opportunities of
**Online
Entertainment**

Proceedings of the 8th International Conference on Internet, Law & Politics
Universitat Oberta de Catalunya. Barcelona, 9-10 July, 2012

COORDINADORES

Agustí Cerrillo i Martínez, Miquel Peguera
Ismael Peña-López, María José Pifarré de Moner,
Mònica Vilasau Solana

 **UOC**
Universitat Oberta
de Catalunya
www.uoc.edu


HUYGENS
EDITORIAL

Retos y oportunidades del entretenimiento en línea

Actas del VIII Congreso Internacional Internet,
Derecho y Política. Universitat Oberta de Catalunya,
Barcelona, 9-10 de julio de 2012

Challenges and Opportunities of Online Entertainment

*Proceedings of the 8th International Conference on Internet,
Law & Politics. Universitat Oberta de Catalunya,
Barcelona, 9-10 July, 2012*

2012



RETOS Y OPORTUNIDADES DEL ENTRETENIMIENTO EN LÍNEA

CHALLENGES AND OPPORTUNITIES OF ONLINE ENTERTAINMENT

© 2012, Los autores

© 2012, Huygens Editorial

La Costa, 44-46, át. 1^a

08023 Barcelona

www.huygens.es

ISBN: 978-84-695-4123-4

Impreso en España



Esta obra está bajo una llicència Attribution-NonCommercial-NoDerivs 3.0 Unported de Creative Commons.

Para ver una copia de esta licencia, visite

<http://creativecommons.org/licenses/by-nc-nd/3.0/>.

PRESENTACIÓN	15
--------------------	----

COMUNICACIONES SOBRE PROPIEDAD INTELECTUAL

CLOUD-BASED LOCKER SERVICES FOR MUSIC: OTHER INCOMING BATTLES IN THE ENDLESS WAR BETWEEN COPYRIGHT AND TECHNOLOGY?. <i>Aura Bertoni y Maria Lilla Montagnani</i>	25
1. Introduction.....	25
2. Models for online distribution of digital content	26
2.1. The first models for online distribution of digital content: the rise of downloading.....	26
2.2. The advertisement-based distribution and the rise of streaming	31
3. Cloud-based music services as new model of music distribution	34
3.1. The nature of cloud computing	34
3.2. The changing shape of digital music in the Cloud.....	36
4. New phase for online distribution of digital content: concluding remarks.	40
5. Bibliography.....	43

REMOVED COLLECTIVE LICENSING OF ON LINE MUSIC AND THE RECENT INITIATIVES IN THE EU. <i>Enrico Bonadio</i>	47
1. Introduction.....	47
2. The rationale of collective licensing and the reciprocal representation agreements.....	48
3. The second generation of reciprocal representation agreements.....	49
4. Towards a EU-wide licensing system in the on-line music field.....	52
4.1. The European Commission has recently addressed these issues	52
5. The European Commission Recommendation on collective cross-border management of copy right for legitimate online music services	53
6. Critical considerations of the «third option system».....	55
7. The aftermath of the Recommendation: the timid rise of EU licensing «platforms»	56
7.1. What happened after the Recommendation?	56
8. What will be the next step in the EU?	58
9. A possible global response: the Global Repertoire Database.....	59

COPYRIGHT INFRINGING CONTENT AVAILABLE ONLINE NATIONAL JURISPRUDENTIAL TRENDS. <i>Federica Casarosa</i>	61
1. Introduction.....	61
2. Between hosting and service provision – the regulatory framework for online intermediaries ...	62
3. In search of a common interpretation: the jurisprudence of french and italian courts on the conflicts between content producers and intermediaries.....	65

3.1. France.....	65
3.2. Italy.....	68
4. Comparative analysis.....	71
4.1. The content of the notice.....	72
4.2. The obligation to monitor	73
4.3. The distinction between active and passive host.....	74
5. Bibliography.....	75
EMULATION IS THE MOST SINCERE FORM OF FLATTERY: RETRO VIDEOGAMES, ROM DISTRIBUTION AND COPYRIGHT. <i>Benjamin Farrand</i>	77
1. Introduction.....	77
2. Emulators and roms: the legalities of re-engineering videogame past	78
2.1. A <i>prima facie</i> case of infringement? Copyright and videogame emulation	79
2.2. Good coders copy, great coders steal? Reverse engineering and the legality of emulators	82
2.3. Emulation, preservation, termination? A consideration of the impact of ROM distribution.....	85
3. Possible legal approaches to emulation.....	89
4. Bibliography.....	90
LA «LEY SINDE»: UNA OPORTUNIDAD PERDIDA PARA LA REGULACIÓN DEL OCIO ONLINE EN ESPAÑA. <i>Ercilia García Álvarez, Jordi López Sintas y Sheila Sánchez Bergara</i>	95
1. Introducción.....	95
2. Debate sobre la regulación de la propiedad intelectual online	97
3. Partes implicadas, intereses y derechos en la «Ley Sinde»	98
3.1. Cuestiones procesales con repercusiones para los derechos e intereses de las partes.....	101
4. Aplicación de la «Ley Sinde»: potenciales dificultades	103
5. La «Ley Sinde»: entre vótores y abucheos.....	105
6. Conclusiones.....	107
7. Bibliografía básica.....	108
THE DIGITAL CLOUD RECORDER: MODERN VCR OR NEW INTERMEDIARY? <i>Robin Kerremans...</i>	111
1. Introduction.....	111
2. Technologies, services and jurisdictions – a brief overview of cases aro und the world.....	112
2.1. TVCatchup (UK)	112
2.2. Wizzgo (FR).....	112
2.3. Cablevision (USA).....	113
2.4. TV Now (Australia).....	113
2.5. Relevant characteristics of DCR-services – Copyright question... ..	113
3. Fitting DCR into belgian copyright law: VCR-wise or cable-wise?	114
3.1. What is the legal status of the recording made by a DCR?	114
3.2. Exception for «temporary technical copies» as a safety net?	119
3.3. Does the use of the DCR imply a public or a private communication?	121
3.3.1. Scenario 1: Customer is «copier» and playback of copy is a «private communication»	121
3.3.2. Scenario 2: Service provider is «copier» and playback feature is a «communication to the public»	122

4. Conclusion.....	123
5. Bibliography.....	124
GUIDING PRINCIPLES FOR ONLINE COPYRIGHT ENFORCEMENT. <i>Andrew McDiarmid y David Sohn</i>	125
1. Introduction.....	125
2. Principles for Online Copyright Enforcement.....	126
2.1. Copyright enforcement should target true bad actors. Ratcheting up copyright protections across the board would impair legitimate business activity and chill technological innovation that drives free expression’.....	126
2.2. Existing policies establishing safe harbors for Internet intermediaries have been tremendously successful. Policymakers should avoid abandoning those policies in favor of imposing new network-policing roles on intermediaries.....	130
2.3. Rigorous cost-benefit analysis is essential in evaluating new policy proposals for addressing online copyright infringement. There needs to be a sober assessment of a policy’s likely effectiveness and its collateral impact on legitimate content and entities.....	132
2.4. There may be opportunities for progress through voluntary, collaborative approaches that do not involve government mandates. Such approaches must, however, be developed in a manner that ensures that consumer and innovation interests are strongly represented and protected ..	133
2.5. Online copyright policy should set a realistic goal: making participation in widespread infringement relatively unattractive and risky, compared to participating in lawful markets...	134
2.6. Enforcement alone cannot solve online infringement. Increased availability of compelling legal options for obtaining copyrighted works and public education about the consequences of infringement are essential to reducing online infringement.....	136
3. Case Study: Targeting Domain Names.....	137
3.1. Principle 1: Focus on bad actors.....	138
3.2. Principle 2: Avoid network-policing by intermediaries.....	139
3.3. Principle 3: Weigh costs versus benefits.....	140
3.4. Principles 4 Through 6.....	142
4. Conclusion.....	142
5. Bibliography.....	143
PIPA, SOPA, OPEN – THE END OF PIRACY OR PRIVACY? <i>László Németh</i>	147
1. Introduction.....	147
2. Acts, bills and proposals in the United States.....	148
2.1. The Basics.....	148
2.1.1. Network Architecture.....	148
2.1.2. Network Neutrality.....	149
2.1.3. Legislation.....	150
2.2. PIPA.....	151
2.3. SOPA.....	152
2.4. PIPA and SOPA – concerns, objections, protests.....	153
2.5. OPEN Act.....	156
3. The effects of SOPA and PIPA in the European Union.....	159
4. Conclusions.....	161
5. Bibliography.....	163
5.1. Books, Articles.....	163
5.2. Legal Bases.....	163

COMUNICACIONES SOBRE COMERCIO ELECTRÓNICO Y JUEGO ONLINE

¿CÓMO INFLUIRÁ LA NUEVA DIRECTIVA 2011/83/UE EN EL COMERCIO ELECTRÓNICO? <i>Zofia Bednarz</i>	167
1. Introducción.....	167
2. Propuesta de la directiva relativa a los derechos de los consumidores.....	168
2.1. Obstáculos al comercio electrónico transfronterizo	168
2.2. El significado de las consultas públicas.....	170
2.3. La acogida de la Propuesta de la Directiva.....	171
3. Directiva adoptada	172
3.1. Texto definitivo de la Directiva 2011/83/UE	172
3.2. La importancia de la Directiva para el comercio electrónico.....	173
3.3. Las novedades relativas al comercio electrónico establecidas por la Directiva	173
4. Consecuencias de la directiva para el comercio electrónico	175
4.1. Quién se verá afectado por la Directiva.....	175
4.2. Derechos acordados a los consumidores.....	175
4.3. La situación de empresas bajo la nueva normativa.....	177
4.4. La recepción de la Directiva por los Estados Miembros.....	178
5. Conclusiones	178
6. Bibliografía.....	179
 MYTHS AND TRUTHS OF ONLINE GAMBLING. <i>Margaret Carran</i>	181
1. Online gambling in context.....	181
1.1. Introduction.....	181
1.2. Snapshot of legal framework.....	182
2. Myths and truths of the internet gambling.....	184
2.1. Omnipresence of online gambling.....	185
2.2. Problem gambling	186
2.3. Online gaming experience	187
2.4. Solution?	188
3. Adolescents online – unique problem?.....	190
3.1. Prevalence rates.....	190
3.2. The real danger?.....	192
4. Conclusion.....	193
5. Bibliography.....	193
 LAS NUEVAS TECNOLOGÍAS Y EL BLANQUEO DE CAPITALES: <i>SECOND LIFE</i> , ENTRETENIMIENTO ONLINE Y MÉTODO DELICTIVO. <i>Covadonga Mallada Fernández</i>	199
1. Introducción	199
2. Métodos de blanqueo de capitales	203
3. Uso de internet y las nuevas tecnologías.....	203
3.1. Tarjetas anónimas y dinero electrónico.....	203
3.2. Las nuevas tecnologías y el blanqueo de capitales: <i>Second life</i>	205
4. Conclusiones	208
5. Bibliografía.....	209
 CAMBIAR LAS REGLAS DEL (VIDEO)JUEGO. MECANISMOS DE CONTROL CONTRACTUAL EN PLATAFORMAS DE ENTRETENIMIENTO ONLINE. <i>Antoni Rubí Puig</i>	211
1. Introducción	211

2. El asunto MDY Industries v. Blizzard Entertainment	212
2.1. Hechos	212
2.2. El conflicto entre las partes	213
2.3. La sentencia dictada en apelación	214
2.3.1. Responsabilidad ajena por infracción de derechos de autor (<i>Secondary Infringement</i>).....	215
2.3.2. Pretensiones derivadas de la Digital Millenium Copyright Act: elusión de medidas tecnológicas de protección.....	219
2.3.3. Inducción a la infracción contractual	221
3. Protagonismo del derecho de contratos.....	222
4. Bibliografía.....	224

EL SPAM SOCIAL O ENVÍO PROMOCIONAL NO SOLICITADO A TRAVÉS DE LAS REDES SOCIALES. <i>Trinidad Vazquez Ruano</i>	227
1. Aproximaciones sobre la materia.....	227
2. El denominado spam en redes sociales (<i>spamming 2.0</i>) o <i>Social Networking Spam</i>	229
3. La tutela de la información de carácter personal en las redes sociales.....	232
3.1. Presupuestos generales en materia de protección de datos	232
3.2. Especialidades de la tutela de los datos personales del usuario de una red social	235
4. Ideas finales. Posibles recomendaciones.....	236
5. Bibliografía.....	238
5.1. Referencias bibliográficas	238
5.2. Recursos normativos.....	238
5.3. Otros recursos	239

COMUNICACIONES SOBRE GOBIERNO Y POLÍTICAS REGULATORIAS

DEMOCRACIA ELECTRÓNICA, INTERNET Y GOBERNANZA. UNA CONCRECIÓN. <i>Fernando Galindo Ayuda</i>	243
1. Introducción	243
2. Democracia hoy	244
2.1. Los principios jurídicos fundamentales	244
2.2. El acceso a información como requisito democrático	245
2.3. Gobernanza	246
3. TIC y democracia.....	248
4. Democracia e internet	250
4.1. Internet y promoción de la democracia.....	250
4.1.1. Domicilios.....	250
4.1.2. Aplicaciones usadas.....	250
4.1.3. Conclusiones sobre el uso de Internet y democracia.....	251
4.2. La gobernanza de Internet	252
5. Uso de instrumentos técnicos y brecha digital	253
6. Acceso a información	254
7. Conclusión.....	258
8. Bibliografía.....	259

INTERNET CO-REGULATION AND CONSTITUTIONALISM: TOWARDS EUROPEAN JUDICIAL REVIEW. <i>Christopher T. Marsden</i>	261
1. Introduction: Examining the origins of co-regulation.....	261
2. Co-Regulation Defined.....	264
3. Towards a Nuanced Typology of Co-regulation.....	269
4. Constitutional Review and Co-regulation.....	271
5. Constitutional Protection by the European Charter of Fundamental Rights.....	276
6. Conclusion: Co-Regulation and Constitutionalism.....	280
REDEFINIENDO LA ISEGORÍA: OPEN DATA CIUDADANOS. <i>Helena Nadal Sánchez y Javier de la Cueva González-Cotera</i>	283
1. Introducción.....	283
2. La <i>isegoría</i>	285
3. La publicidad de lo político.....	287
4. La construcción ciudadana de <i>open data</i>	289
4.1. Supuestos de extracción y generación de datos.....	290
4.2. Los criterios <i>open data</i>	292
4.3. Criterios de demarcación para determinar la validez del dato.....	295
4. La <i>isegoría</i> , reformulada.....	297
5. Bibliografía.....	299
CONSTITUCIÓN 2.0 Y ESTADO DE E-DERECHO: A PROPÓSITO DEL PROCESO CONSTITUYENTE ISLANDÉS. <i>Pere Simón Castellano</i>	301
1. A modo de introducción: imperio de la Ley y Estado de Derecho en el universo 2.0.....	301
2. Cambio de paradigma en la efectividad del imperio de la Ley.....	304
2.1. La transparencia electrónica.....	304
2.1.1. Noción de transparencia y estado de la cuestión en España.....	304
2.1.2. Publicidad, transparencia y sometimiento de los poderes a la Ley en el Estado de Derecho.....	307
2.1.3. El empleo de las TICs a propósito de la transparencia.....	308
2.2. Participación ciudadana en la toma de decisiones legislativas.....	311
3. La Constitución 2.0 y el proceso constituyente islandés.....	315
4. Conclusiones.....	316
5. Bibliografía.....	317
COMUNICACIONES SOBRE PRIVACIDAD	
PNR AND SWIFT AGREEMENTS. EXTERNAL RELATIONS OF THE EU ON DATA PROTECTION MATTERS. <i>Cristina Blasi Casagran</i>	323
1. Introduction.....	323
2. Key issues of data transfers to third countries.....	324
3. Passenger Name Record agreements.....	325
4. EU PNR Directive.....	329
5. SWIFT Agreements.....	331
6. Creation of EU TFTS.....	333
7. Steps for the US-EU framework agreement on data protection.....	335
8. Conclusion.....	337
9. Bibliography.....	338

ONLINE ENTERTAINMENT IN CLOUD COMPUTING SURROUNDINGS. <i>Philipp E. Fischer y Rafael Ferraz Vazquez</i>	341
1. Introduction.....	341
2. Online entertainment- and cloud computing services.....	343
2.1. Online entertainment services	343
2.2. Cloud computing services.....	344
3. The concepts of privacy and data protection.....	346
4. Interfaces between cloud computing and online entertainment	346
4.1. A ccountability between controller and processor	346
4.2. Ubiquity and different data protection levels	347
4.3. Jurisdiction, applicable law and enforcement	348
4.3.1. Jurisdiction	348
4.3.2. Applicable law	348
4.3.3. Enforcement.....	349
4.4. Contract data processing	349
4.5. International data transfer	350
5. Finding a balance between the cloud, online entertainment and users' privacy.....	350
5.1. Data protection in Germany.....	350
5.2. Data protection in Spain	351
5.3. The European Data Protection Directive and its reform.....	352
5.4. International framework for data protection	353
6. Future solutions to existing problems	354
6.1. Solutions of the law	354
6.1.1. U.S.	354
6.1.2. E.U.....	354
6.1.3. Bilateral conventions	355
6.1.4. Multilateral conventions	356
6.2. Technical solutions	356
6.2.1. Self-certification and international standards	356
6.2.2. Privacy by design principles	357
6.3. Solutions of the private sector.....	360
7. Conclusion.....	361
8. Bibliography.....	361
EL RETO DE LA PROTECCIÓN DE DATOS DE LAS PERSONAS MAYORES EN LA SOCIEDAD DEL OCIO DIGITAL. <i>Isidro Gómez-Juárez Sidera y María de Miguel Molina</i>	367
1. Las personas mayores en la sociedad del ocio digital	367
1.1. Las personas mayores en la sociedad digital.....	367
1.2. Personas mayores y ocio digital	369
1.3. Estrategias para afrontar el reto de la protección de datos de las personas mayores	370
2. Protección de datos de las personas mayores en la sociedad del ocio digital.....	372
2.1. Brecha generacional digital y cultura de la protección de datos	372
2.2. La necesaria armonización del derecho de información	375
2.2.1. El valor instrumental del derecho de información respecto del principio del consentimiento	375
2.2.2. Respeto del contexto.....	377
2.2.3. Transparencia.....	378
2.3. Fomento de iniciativas de autorregulación y promoción de códigos de conducta	381
3. Conclusiones.....	383
4. Bibliografía.....	383

BALANCING INTELLECTUAL PROPERTY AGAINST DATA PROTECTION: A NEW RIGHT'S WAVERING WEIGHT. <i>Gloria González Fuster</i>	385
1. Introducing <i>Scarlet</i> and <i>Netlog</i>	386
1.1. <i>Scarlet v Sabam</i>	386
1.2. <i>Sabam v Netlog</i>	388
2. A new right in the making.....	388
2.1. The innovation of the Charter	389
2.2. Lack of straightforward reception in the case law	389
2.2.1. The moving object of data protection law	390
2.2.2. The right to respect for private life with regard to the processing of personal data	392
3. Balancing an elusive right	393
3.1. Disparate balancing operations in the context of EU data protection law	393
3.1.1. Deferring the balancing	394
3.1.2. Invalidity of EU law due to no insurance of fair balance	395
3.2. Balancing intellectual property against data protection (as a right).....	395
3.2.1. The right to personal data protection as the applicable right	396
3.2.2. A strong even if laconic assertion of the lack of fair balance	397
4. Concluding remarks	398
5. Bibliography.....	399

REMOVED HANDLING COOKIES WITHIN THE EUROPEAN UNION: MAKING THE COOKIES CRUMBLE?. <i>Eleni Kosta</i>	401
1. Introduction.....	401
2. The regulation of cookies in the eprivacy directive.....	402
2.1. The amendment of Article 5(3)	402
2.2. Information covered by Article 5(3) ePrivacy Directive.....	402
2.3. The new requirement for consent	403
3. Unravelling the new consent requirements	404
3.1. Early reactions against the new consent requirement	404
3.2. Analysis of the new requirement for consent.....	405
3.2.1. Conditions for valid consent.....	405
3.2.2. Exceptions from the consent requirement.....	405
3.2.3. Information to be provided.....	406
3.2.4. The essence of consent	408
3.2.5. Subscriber or user	409
3.3. The provision of consent via browser settings.....	409
3.3.1. Criticism against the provision of consent via browser settings.....	410
3.3.2. Conditions for providing consent via browser settings	411
3.4. A lternative mechanisms for provision of valid consent	412
3.5. The role of the European Commission.....	412
4. United Kingdom	413
5. Conclusions	415
6. Bibliography.....	415

THE EMERGING RIGHT TO BE FORGOTTEN IN DATA PROTECTION LAW: SOME CONCEPTUAL AND LEGAL PROBLEMS. <i>David Lindsay</i>	419
1. Introduction	419
2. Some paradoxes of privacy and digital identity	420
2.1. The problem of digital traces	421

2.2. Digital traces, freedom and self-development.....	422
2.3. Digital traces, Bauman and the paradoxes of identity formation	423
3. The case for a legal right to be forgotten	424
4. Background to the right to be forgotten in data protection law	425
4.1. EU Data Protection Reform and the Right to be Forgotten	425
4.2. A concise history of the deletion principle	426
4.3. The 1995 Data Protection Directive	428
5. The right to be forgotten in the proposed GDPR	430
5.1. The general framework of the proposed GDPR	430
5.2. The right to be forgotten in the proposed GDPR	430
5.3. Limitations on, and exceptions to, the proposed right to be forgotten	432
5.4. A pplication of the proposed right to be forgotten to SNS.....	434
5.4.1. The household exemption.....	434
5.4.2. Data Controller	435
6. Conclusion.....	436
7. Bibliography.....	438
NUEVOS RETOS DE LA REGULACIÓN JURÍDICA Y DEONTOLÓGICA DE LA PUBLICIDAD EN LAS REDES SOCIALES. <i>Esther Martínez Pastor y Mercedes Muñoz Saldaña</i>	443
1. Publicidad en la red, intimidad y datos personales. El reto del equilibrio	443
2. Los tres ejes para el equilibrio: la prestación del consentimiento; el derecho a la información y el derecho de oposición	444
2.1. Prestación del consentimiento	445
2.2. Derecho de Información.....	445
2.3. Derecho de oposición	447
3. La regulación como punto de partida y la corregulación como desarrollo de la autorregulación.	448
4. Bibliografía.....	450
NAMING AND SHAMING IN GREECE: SOCIAL CONTROL, LAW ENFORCEMENT AND THE COLLATERAL DAMAGES OF PRIVACY AND DIGNITY. <i>Lilian Mitrou</i>	453
1. Naming and shaming: an introduction.....	453
2. Shaming as sanction policy.....	455
2.1. Shaming Policies	455
2.2. Naming suspects and convicted sex offenders	456
2.3. Naming and Shaming Tax evaders.....	457
2.4. Shaming in the context of new security perceptions.....	458
3. Impact of shaming (s)a(n)ctions	459
3.1. Impact of shaming on reputation, privacy and dignity.....	459
3.2. Shaming and presumption of innocence.....	460
3.3. Impact of shaming in digital age.....	461
4. Conclusion.....	463
4.1. Is shaming appropriate, necessary and/or efficient?	463
4.2. Some concluding remarks.....	464
5. Bibliography.....	465
EL PODER DE AUTODETERMINACIÓN DE LOS DATOS PERSONALES EN INTERNET. <i>Ma Dolores Palacios González</i>	467
1. Introducción	467
2. La actual situación jurídica de la protección de datos en la Unión Europea.....	468

3. Datos personales y responsable del tratamiento	469
4. El principio general de la disponibilidad de los datos por el interesado	471
4.1. Consentimiento para el tratamiento de datos personales	471
4.2. Revocación del consentimiento y derechos de oposición y cancelación	474
5. Problemas concretos	476
5.1. Ejercicio de los derechos de oposición y/o cancelación frente a un buscador	476
5.2. Ejercicio de las facultades de revocación, oposición y/o cancelación frente a otros eventuales responsables del tratamiento.....	480
6. Conclusión.....	483
7. Bibliografía.....	483
REVIVING PRIVACY: THE OPPORTUNITY OF CYBERSECURITY. <i>Maria Grazia Porcedda</i>	485
1. Introduction.....	485
2. Organizational and technical challenges to privacy and data protection.....	487
2.1. Challenge n. 1: Surreptitious barter.....	488
2.2. Challenge n. 2: Cyber wrongdoings.....	489
2.2.1. What is really cybercrime?	490
3. Cybercrime and cybersecurity: threat or opportunity?	491
3.1. Notions of security (and privacy).....	492
3.1.1. The broad cybercrimes community: security vs. privacy.....	492
3.1.2. Narrow cybercrime communities.....	494
4. (Cyber)security and data privacy: a complementary goal	497
4.1. Rules complementary to cybercrime and the pursuit of cyber-security	497
4.2. Rules contributing to the prevention of crimes and cyber-security	498
4.3. Revision of data protection laws and cybercrime legislation	499
5. Conclusion.....	500
6. Bibliography.....	501
CONSERVACIÓN DE DATOS E ILÍCITOS EN MATERIA DE PROPIEDAD INTELECTUAL: UNA VISIÓN CONSTITUCIONAL DE LA DIRECTIVA 2006/24. <i>María Concepción Torres Díaz</i>	507
1. Planteamiento general.....	507
2. Aproximación a las Directivas 95/46 y 2002/58	509
2.1. Consideraciones a la Directiva 95/46.....	509
2.2. Consideraciones a la Directiva 2002/58.....	510
3. Aproximación a la Directiva 2004/48/CE.....	511
4. Aproximación a la Directiva 2006/24/CE.....	514
5. Análisis constitucional y derechos afectados.....	516
6. Consideraciones finales.....	519
7. Bibliografía.....	520

CONSERVACIÓN DE DATOS E ILÍCITOS EN MATERIA DE PROPIEDAD INTELECTUAL: UNA VISIÓN CONSTITUCIONAL DE LA DIRECTIVA 2006/24

María Concepción TORRES DÍAZ

*Profesora de Derecho Constitucional de la Universidad de Alicante;
Premio Extraordinario en el Máster Oficial Sistemas y Servicios de la Sociedad de la Información,
especialidad jurídica (Universidad de Valencia)*

RESUMEN: El Tribunal Supremo de Suecia formuló una petición de decisión prejudicial al TJCE en el marco de un litigio entre las sociedades Bonnier Audio y otros y ePhone en relación con la oposición formulada por ePhone contra una solicitud de requerimiento judicial de revelación de información presentada por Bonnier Audio y otros, en aras de identificar a un determinado abonado. La petición pretende que el Tribunal de Justicia de las Comunidades Europeas se pronuncie sobre dos cuestiones prejudiciales. En primer lugar, si la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la presentación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones se opone a la aplicación de una disposición de derecho nacional basada en el artículo 8 de la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril, relativa al respeto de los derechos de propiedad intelectual, que permite que, a efectos de identificación de un abonado, se requiera en un procedimiento civil a un proveedor de acceso a Internet para que facilite al titular de un derecho de autor información relativa al abonado al que dicho proveedor de acceso asignó una dirección IP concreta, supuestamente utilizada para infringir dicho derecho. En segundo lugar, el Tribunal Supremo sueco plantea (también) si influye en la respuesta a la primera cuestión el hecho de que el Estado miembro no haya adoptado su Derecho interno a las disposiciones de la Directiva 2006/24. El planteamiento de sendas cuestiones prejudiciales resultan relevantes desde el punto de vista constitucional teniendo en cuenta los derechos susceptibles de verse afectados –a saber– intimidad personal, protección de datos, derechos de autor y, por extrapolación, secreto de las comunicaciones –todo ello en relación con la conservación de datos. Cuestiones que no son baladíes teniendo en cuenta las críticas que en su día suscitó la Directiva 2006/24. Críticas que supusieron un profundo cambio en los principios generales en materia de protección de datos y de secreto de las comunicaciones. Pero críticas que –al fin y al cabo– fueron justificadas por esa finalidad de garantizar que los datos conservados por los operadores estuvieran disponibles para las autoridades competentes con fines de investigación, detección y enjuiciamiento de delitos graves, esto es, estuvieran disponibles para luchar contra la criminalidad organizada y el terrorismo.

PALABRAS CLAVE: derechos de autor, conservación de datos, intimidad personal y derechos conexos, análisis constitucional.

1. PLANTEAMIENTO GENERAL

El Tribunal Supremo de Suecia (Högsta domstolen) formuló una petición de decisión prejudicial al TJCE en el marco de un litigio entre las sociedades Bonnier Audio y otros (Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget Aktiefbolag

y Storyside AB) y ePhone en relación con la oposición formulada por ePhone contra una solicitud de requerimiento judicial de revelación de información presentada por Bonnier Audio y otros, en aras de identificar a un determinado abonado. La petición pretende que el Tribunal de Justicia de las Comunidades Europeas se pronuncie sobre dos cuestiones prejudiciales. En primer lugar, si la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la presentación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones se opone a la aplicación de una disposición de derecho nacional basada en el artículo 8 de la Directiva 2004/48/CE del Parlamento Europeo y del Consejo, de 29 de abril, relativa al respeto de los derechos de propiedad intelectual, que permite que, a efectos de identificación de un abonado, se requiera en un procedimiento civil a un proveedor de acceso a Internet para que facilite al titular de un derecho de autor información relativa al abonado al que dicho proveedor de acceso asignó una dirección IP concreta, supuestamente utilizada para infringir dicho derecho. En segundo lugar, el Tribunal Supremo sueco plantea (también) si influye en la respuesta a la primera cuestión el hecho de que el Estado miembro no haya adoptado su Derecho interno a las disposiciones de la Directiva 2006/24. El planteamiento de sendas cuestiones prejudiciales resulta relevante desde el punto de vista constitucional teniendo en cuenta los derechos susceptibles de verse afectados –a saber– intimidad personal, protección de datos, derechos de autor y, por extrapolación, secreto de las comunicaciones –todo ello en relación con la conservación de datos. Cuestiones que no son baladíes teniendo en cuenta las críticas que en su día suscitó la Directiva 2006/24. Críticas que supusieron un profundo cambio en los principios generales en materia de protección de datos y de secreto de las comunicaciones. Pero críticas que –al fin y al cabo– fueron justificadas por esa finalidad de garantizar que los datos conservados por los operadores estuvieran disponibles para las autoridades competentes con fines de investigación, detección y enjuiciamiento de delitos graves, esto es, estuvieran disponibles para luchar contra la criminalidad organizada y el terrorismo.

Partiendo de las anteriores consideraciones la presente comunicación pretende reflexionar sobre una serie de cuestiones: ¿Qué cabe entender por delitos graves a tenor de la Directiva 2006/24? ¿La infracción de derechos de propiedad intelectual entrarían dentro de esa conceptualización? ¿Quiénes son las autoridades competentes a las que alude la Directiva 2006/24? ¿Estaría justificado que en el marco de un procedimiento civil se requiera a un proveedor de acceso que facilite a un titular de derechos de autor los datos de identificación de un abonado? ¿Estaría justificada la aplicación de la Directiva 2006/24 en el caso planteado teniendo en cuenta que las dudas surgen en el marco de un litigio cuya protección es esencialmente civil o de derecho privado? ¿Qué riesgos conllevaría –desde el punto de vista de los derechos fundamentales– la extensión y/o generalización a los litigios civiles de la aplicación de una norma que nació en el seno de la lucha antiterrorista? Y es que –pendientes de la sentencia que (en su día) falle el TJCE– son muchas las dudas que suscita esta cuestión, máxime cuando se advierte que la Directiva 2006/24 puede ser utilizada para perseguir ilícitos de propiedad intelectual que exceden –y mucho– de los fines previstos en la mentada Directiva.

2. APROXIMACIÓN A LAS DIRECTIVAS 95/46 Y 2002/58

2.1. Consideraciones a la Directiva 95/46

Antes de entrar a analizar propiamente las Directivas 2006/24/CE y 2004/48/CE considero oportuno realizar algunas consideraciones generales a la Directiva 95/46/CE¹ 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. Y es que la Directiva referenciada tiene como objeto –a tenor de lo dispuesto en su artículo 1– que los Estados miembros garanticen la protección de las libertades y los derechos fundamentales de las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. La Directiva recoge una serie de definiciones como las de datos de carácter personal, tratamiento de datos personales, fichero de datos personales, responsable del tratamiento, encargado de tratamiento, tercero, destinatario y consentimiento del interesado. Su ámbito de aplicación está recogido en su artículo 3 cuando señala que «Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero». A sensu contrario, el párrafo 2 de dicho precepto precisa que las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario como el tratamiento de datos que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en materia penal, así como las actividades efectuadas por una persona física en el ejercicio de actividades exclusivamente personales o domésticas. La Directiva recoge una serie de principios relativos a la calidad de los datos que es preciso tener en cuenta. Entre esos principios –precisa– que los datos deben ser tratados de manera leal y lícita, deben ser recogidos con fines determinados, explícitos y legítimos de tal forma que no sean tratados posteriormente de manera incompatible con dichos fines, deben ser exactos y deben estar actualizados, además, deben conservarse de tal forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se tratan ulteriormente. Junto a estos principios la Directiva alude (también) a una serie de principios relativos a la legitimación del tratamiento de datos. Su artículo 7 dispone que los Estados miembros dispondrán que el tratamiento de datos sólo puede efectuarse si el interesado ha dado su consentimiento de forma inequívoca, si es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, si es necesario

1 Véase 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. Puede consultarse en la siguiente dirección url: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:ES:PDF>, (fecha de consulta: 15/11/2011). Véase (también) la LO 15/1999, de 13 de diciembre en la siguiente dirección url: <http://www.boe.es/boe/dias/1999/12/14/pdfs/A43088-43099.pdf>, (fecha de consulta: 15/11/2011).

para el cumplimiento de una obligación jurídica, si es necesario para proteger el interés vital del interesado, si es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero o a quien se comuniquen los datos o, por último, si es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos. La Directiva recoge el derecho de información al interesado tanto cuando los datos se hayan recabado del propio interesado como cuando se hayan recabado de terceros. Asimismo recoge el derecho de oposición del interesado así como aspectos relacionados con la confidencialidad y la seguridad en el tratamiento de datos personales. A los objetos de esta comunicación conviene resaltar como la Directiva 95/46/CE obliga a los Estados miembros a garantizar la protección de los derechos y libertades de las personas físicas en relación con el tratamiento de datos personales estableciendo principios rectores que determinan la legalidad de dicho tratamiento.

2.2. Consideraciones a la Directiva 2002/58

La Directiva 2002/58/CE² 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 (Directiva sobre la privacidad y las comunicaciones electrónicas) tiene como objetivo garantizar un nivel equivalente de protección de las libertades y derechos fundamentales y, en particular, el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas, así como la libre circulación de tales datos y de los equipos y servicios de comunicaciones electrónicas. A los objetos de esta comunicación conviene prestar especial atención a la dicción literal del artículo 5.1 de la Directiva referenciada. Precepto que dispone textualmente,

«Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad».

De la dicción literal del precepto extractado se observa como las únicas excepciones al principio de confidencialidad son las que se aplican a favor de las personas autorizadas legalmente, en el sentido del artículo 15, apartado 1 y las relativas al almacenamiento técnico

2 Véase 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. Puede consultarse en la siguiente dirección url: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:ES:PDF>, (fecha de consulta: 12/10/2011).

necesario para la conducción de una comunicación. Con respecto al apartado 1 del artículo 15 cabe señalar como dispone textualmente,

«Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión».

Por su parte el apartado 1 del artículo 6 de la Directiva referenciada prevé que los datos de tráfico almacenados deberán eliminarse o hacerse anónimos cuando ya no sean necesarios a los efectos de la transmisión de una comunicación, sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 de dicho artículo y en el artículo 15, apartado 1 de dicha Directiva. Señala textualmente el apartado 1 del artículo 6,

«Sin perjuicio de lo dispuesto en los apartados 2, 3 y 5 del presente artículo y en el apartado 1 del artículo 15, los datos de tráfico relacionados con abonados y usuarios que sean tratados y almacenados por el proveedor de una red pública de comunicaciones o de un servicio de comunicaciones electrónicas disponible al público deberán eliminarse o hacerse anónimos cuando ya no sean necesario a los efectos de la transmisión de una comunicación».

Partiendo de las anteriores consideraciones, y en virtud de lo expuesto, cabe colegir que los Estados miembros podrán adoptar medidas legales para limitar el alcance de la obligación de garantizar la confidencialidad de los datos de tráfico cuando tal limitación constituya una medida necesaria, proporcionada y apropiada, en una sociedad democrática, para proteger la seguridad nacional (defensa y seguridad pública), la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas³.

3. APROXIMACIÓN A LA DIRECTIVA 2004/48/CE

La Directiva 2004/48/CE⁴ del Parlamento Europeo y del Consejo de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual recoge una serie de considerandos de especial interés a los objetos de la presente comunicación. Señala

3 Véase el apartado 1 del artículo 13 de la Directiva 95/46.

4 Véase la Directiva 2004/48/CE del Parlamento Europeo y del Consejo de 29 de abril de 2004, relativa al respecto de los derechos de propiedad intelectual. Puede consultarse en la siguiente dirección url: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:157:0045:0086:ES:PDE>, (fecha de consulta: 22/10/2011).

la –en su considerando primero– como la realización del mercado interior ha supuesto la eliminación de las restricciones a la libre circulación así como la eliminación de las distorsiones de la competencia, al tiempo que se crea un entorno favorable a la innovación y la inversión. En este contexto, la protección de la propiedad intelectual resulta imprescindible no sólo para la promoción de la innovación y de la creación, sino también para el desarrollo del empleo y la competitividad. En la misma línea se pronuncia el considerando segundo cuando resalta como la protección de la propiedad intelectual debe permitir que el inventor o creador obtenga un beneficio legítimo de su invención o creación. En este sentido, se hace preciso garantizar una difusión amplia de las obras, ideas y conocimientos nuevos, no debiendo ser un obstáculo para la libertad de expresión, para la libre circulación de la información, ni para la protección de los datos personales, inclusive en Internet. No obstante matiza –el considerando tercero– que «sin medios eficaces de tutela⁵ de los derechos de propiedad intelectual, la innovación y la creación se desincentivan y las inversiones se reducen. Por consiguiente, es preciso garantizar que el Derecho sustantivo de propiedad intelectual, que actualmente forma parte en gran medida del acervo comunitario, se aplique de manera efectiva en la Comunidad». Especial atención cabe prestar al considerando número diez. Considerando que recoge el objetivo de la presente Directiva y señala que no es otro que «aproximar dichas legislaciones [las legislaciones de los Estados miembros] para garantizar un nivel de protección de la propiedad intelectual elevado, equivalente y homogéneo en el mercado interior». Se observa como el objeto no es establecer normas armonizadas sobre cooperación judicial, competencia judicial, reconocimiento y ejecución de las decisiones en materia civil y mercantil, ni tratar de la legislación aplicable, sino que su objeto queda delimitado en su artículo 1 cuando señala como la presente Directiva «se refiere a las medidas, procedimientos y recursos necesarios para garantizar el respeto de los derechos de propiedad intelectual». El artículo 2 de la Directiva alude al ámbito de aplicación y precisa –en su apartado 2– que afectará a los derechos de autor sin perjuicio de disposiciones específicas relativas al respeto de los derechos y a las excepciones establecidas por la legislación comunitaria, en particular en la Directiva 91/250/CEE, concretamente en su artículo 7, o en la Directiva 2001/29/CE, concretamente en sus artículos 2 a 6 y 8. Por su parte la Directiva no afectará –según lo recogido en el apartado 3 del artículo 2– a las disposiciones comunitarias que regulan el Derecho sustantivo de propiedad intelectual, la Directiva 95/46/CE, la Directiva 1999/93/CE y la Directiva 2000/31/CE, en general, y los artículos 12 a 15 de esta última en particular. Tampoco afectará a las obligaciones internacionales de los Estados miembros ni a ninguna disposición nacional de los Estados miembros relativa a los procedimientos o sanciones penales con respecto a las infracciones de los derechos

5 Sobre los medios de tutela de los derechos de propiedad intelectual habrá que estar a lo dispuesto en los convenios internacionales en materia de propiedad intelectual tales como el Convenio de París para la protección de la propiedad industrial, el Convenio de Berna para la protección de las obras literarias y artísticas y la Convención de Roma sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión.

de propiedad intelectual. El artículo 3 recoge una serie de disposiciones generales entre las que cabe destacar una obligación general en la que se insta a los Estados miembros a que establezcan las medidas, procedimientos y recursos necesarios para garantizar el respeto de los derechos de propiedad intelectual a los que se refiere la presente Directiva. El precepto precisa que dichas medidas serán justas y equitativas así como efectivas, proporcionadas y disuasorias y se aplicarán del tal modo que se evite la creación de obstáculos al comercio legítimo y se ofrezcan salvaguardias contra su abuso.

Sin perjuicio de lo expuesto conviene prestar especial atención al artículo 8 en donde se recoge el derecho a la información. El párrafo 1 de dicho precepto dispone textualmente,

«Los Estados miembros garantizarán que, en el contexto de los procedimientos relativos a una infracción de un derecho de propiedad intelectual y en respuesta a una petición justificada y proporcionada del demandante, las autoridades judiciales competentes puedan ordenar que faciliten datos sobre el origen y las redes de distribución de las mercancías o servicios que infringen un derecho de propiedad intelectual el infractor o cualquier persona que: a) haya sido hallada en posesión de las mercancías litigiosas a escala comercial; b) haya sido hallada utilizando servicios litigiosos a escala comercial; c) haya sido hallada prestando a escala comercial servicios utilizados en las actividades infractoras o d) haya sido designada por la persona a que se refieren las letras a), b) o c) como implicada en la producción, fabricación o distribución de dichas mercancías o en la prestación de dichos servicios».

Por su parte el párrafo 2 del mismo precepto recoge que los datos a los que se refiere el apartado 1 incluirán los nombres y direcciones de los productores, fabricantes, distribuidores, suministradores y otros poseedores anteriores de las mercancías o servicios, así como de los mayoristas y minoristas destinatarios así como información –en su caso– sobre las cantidades producidas, fabricadas, entregadas, recibidas o encargadas, así como sobre el precio obtenido por las mercancías o servicios de que se trate.

A los objetos de la presente comunicación –y por lo que respecta a la protección de datos– conviene significar el contenido del párrafo 3 del artículo 8. Según esta disposición, los apartados 1 y 2 antes referenciados, que regulan el acceso a datos que puedan estar relacionados con infracciones a un derecho de propiedad intelectual, se aplicarán sin perjuicio de otras disposiciones legales y reglamentarias que regulen el tratamiento de datos personales. Dispone textualmente,

«Los apartados 1 y 2 se aplicarán sin perjuicio de otras disposiciones legales que: a) concedan al titular derechos de información más amplios; b) regulen la utilización de los datos que se comuniquen con arreglo al presente artículo en procedimientos civiles o penales; c) regulen la responsabilidad por abuso del derecho de información; d) ofrezcan la posibilidad de negarse a facilitar datos que obliguen a la persona a la que se refiere el apartado 1 a admitir su propia participación o la de sus parientes cercanos en una infracción de un derecho de propiedad intelectual, o e) rijan la protección de la confidencialidad de las fuentes de información o el tratamiento de los datos personales».

De lo expuesto se observa como la Directiva indica que hay que respetar las disposiciones legales y reglamentarias que regulan el tratamiento de datos personales pero no especifica que datos pueden ser conservados, ni la finalidad de su conservación, ni su duración o las personas que pueden acceder a los mismos en caso de infracción de derechos de propiedad intelectual. Por tanto, estamos ante una omisión importante teniendo en cuenta la cuestión suscitada en la cuestión prejudicial planteada.

4. APROXIMACIÓN A LA DIRECTIVA 2006/24/CE

Con respecto a la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones tiene como cometido - según su artículo 1 apartado 1,

«(...) armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro».

Su párrafo segundo señala cuáles son los datos sobre los que se aplicará la Directiva siendo éstos los datos de tráfico y de localización sobre personas físicas y jurídicas y los datos relacionados necesarios para identificar al abonado o usuario registrado. No obstante, precisa el precepto que no se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.

Partiendo de la dicción literal del precepto anteriormente reseñado resulta importante aludir a los distintos considerandos que se incluyen y que tratan de justificar la aprobación de la misma. El considerando primero alude a 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 los datos personales y a la libre circulación de estos datos. El considerando segundo se hace eco de 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. También es importante tener en cuenta las Conclusiones del Consejo de Justicia e Interior de 19 de diciembre de 2002 en donde se destaca la importancia de los datos relativos al uso de las comunicaciones electrónicas como instrumentos para la prevención, investigación, detección y enjuiciamiento de delitos. Junto a esto, la Declaración sobre la lucha contra el terrorismo⁶, adoptada por el Consejo Europeo el 25 de marzo de 2004, tuvo entre otros objetivos examinar las medidas para establecer normas sobre la conservación por los prestadores de servicios de datos de tráfico de las comunicaciones.

Siguiendo con el contenido de la Directiva 2006/24/CE conviene precisar como resalta la importancia de los datos de tráfico y localización para la investigación, detección y enjuiciamiento de delitos, según demuestra la investigación y la experiencia práctica de varios Estados miembros, existiendo la necesidad de asegurar a escala europea que los datos generados o tratados, en el marco de la prestación de servicios de comunicaciones, por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública

6 Vease la Declaración sobre la lucha contra el terrorismo, adoptada por el Consejo Europeo, de 25 de marzo de 2004. Puede consultarse en la siguiente dirección url: <http://www.realinstitutoelcano.org/especiales/atentados/docs/declarterrorUE25304.pdf>, (fecha de consulta: 22/11/2011).

de comunicaciones se conserven durante un determinado período de tiempo con arreglo a las condiciones establecidas en la presente Directiva. En vista de lo expuesto, queda patente la importancia de la conservación de datos en las comunicaciones electrónicas en vista de futuras investigaciones y enjuiciamiento de delitos.

Partiendo de las consideraciones anteriores conviene resaltar como los objetivos de la Directiva 2006/24/CE son, por un lado, armonizar las obligaciones de los proveedores de conservar determinados datos en el ámbito europeo y, por otro, asegurar que éstos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la normativa nacional de cada Estado miembro. Ahora bien ¿qué cabría entender por delitos graves? Según señala la Directiva dentro de la conceptualización de delitos graves se encuentran el terrorismo y la delincuencia organizada. Esta precisión no es baladí si se tiene en cuenta los riesgos para la privacidad y para el secreto de las comunicaciones que las medidas establecidas en la Directiva comentada son susceptibles de generar. En este sentido resulta importante aludir también a la Carta Europea de Derechos Humanos, concretamente a sus artículos. 7 y 8, en donde se reconocen los derechos de respeto de la vida privada y familiar y de protección de datos de carácter personal.

En cuanto al articulado de la Directiva 2006/24/CE cabe señalar que está formada por 17 artículos. El artículo 1 enmarca el objeto y el ámbito de aplicación de la Directiva. El artículo 2 recoge una serie de definiciones importantes, el artículo 3 delimita la obligación de conservar datos. El artículo 4 regula el acceso a los datos, esto es, quiénes serán los autorizados para acceder a los mismos. El artículo 5 recoge el elenco de datos que deben conservarse. El artículo 6 determina el lapso de tiempo en el que deberán ser conservados los datos. El artículo 7 recoge una serie de principios mínimos de seguridad que deberán observar los proveedores de servicios de comunicaciones electrónicas de acceso público. El artículo 8 regula los requisitos de almacenamiento para los datos conservados. El artículo 9 regula las autoridades de control, etc. Sin ánimo de profundizar en el articulado de la Directiva –a los objetos de esta comunicación– conviene apuntar una serie de críticas en cuanto al profundo cambio en los principios generales en materia de protección de datos y secreto de las comunicaciones que comporta. Cambios que tienen como finalidad garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves. A tenor de lo expuesto, se observa como se concede a los Estados amplias facultades de control que han sido ampliamente criticadas por las instancias que velan por la adecuada protección de datos personales ya que supone contravenir los principios, hasta el momento asentados, sobre esta materia. Todo ello fue fruto de la preocupación por la seguridad y la necesidad de dotar a los Estados de los máximos instrumentos para luchar contra el terrorismo. Como señala VILASAU⁷,

«(...) la adopción de una medida sobre retención de datos ha comportado la valoración de distintos intereses en juego contrapuestos. Frente al interés de las autoridades en la retención para luchar de forma más eficaz contra el terrorismo y otras formas de delincuencia organizada, se halla el derecho

7 VILASAU, M. (2006). La Directiva 2006/24/CE sobre conservación de datos de tráfico en las comunicaciones electrónicas: seguridad v. privacidad. IDP, Revista de Internet, Derecho y Política, nº 3, UOC. Recuperado fecha de consulta 10/05/2007, en <http://www.uoc.edu/ojs/index.php/idp/article/view/398>.

fundamental de los ciudadanos a la protección de sus datos. Además, hay que añadir los intereses de los proveedores de servicios de comunicaciones electrónicas en que no les atribuyen más cargas económicas derivadas de las nuevas obligaciones».

De lo expuesto hasta este momento cabría colegir que la finalidad de la Directiva 2006/24/CE queda bastante clara. Una finalidad que –a priori– quedaría fuera de aplicarse al caso objeto de comentario. Y es que conviene recordar que según su artículo 1 –anteriormente citado– busca garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro. Por el contrario, el asunto principal del caso planteado es un procedimiento civil y los datos no los solicita a una autoridad nacional sino a unos particulares.

5. ANÁLISIS CONSTITUCIONAL Y DERECHOS AFECTADOS

Partiendo de las consideraciones expuestas en los apartados anteriores resulta factible realizar algunas consideraciones desde el punto de vista constitucional. Y es que los derechos susceptibles de verse afectados invitan a una reflexión desde esta óptica de análisis. En este sentido, en cuanto a derechos afectados cabría señalar el derecho a la intimidad y la protección de datos, el derecho al secreto de las comunicaciones sin olvidar los derechos de autor. Derechos –todos ellos– de relevancia constitucional que derivan de su propia ubicación sistemática en nuestra Carta Magna. Ubicación que les otorga una serie de características propias y unas garantías de tutela y protección reforzadas⁸. Y es que hablamos de derechos recogidos en la sección 1ª del capítulo 2º del Título I de la Constitución española. Derechos dotados de una doble dimensión subjetiva⁹ y objetiva¹⁰ y derechos cuya constitucionalización les hace tributarios de una serie de caracteres como su aplicabilidad directa, su vinculación a todos los poderes públicos y a la ciudadanía¹¹ y su protección jurisdiccional.

Con respecto al derecho a la intimidad está recogido en el artículo 18.1 CE junto con el derecho al honor y la propia imagen. Desde el punto de vista constitucional se busca resguardar de la acción y el conocimiento ajenos un ámbito propio y reservado de cada sujeto, que se considera necesario para mantener una calidad mínima de vida humana. Por su parte, el derecho a la protección de datos se encuentra en el apartado 4 del artículo 18 CE. Se ha configurado como un derecho autónomo –a pesar de que esta cuestión ha sido y es ampliamente debatida– que otorga a sus titulares un poder de disposición sobre los propios datos. El secreto de las co-

8 Sobre las garantías véase el artículo 53 CE.

9 Con respecto a la dimensión subjetiva de los derechos fundamentales y/o constitucionales deriva de su relación con la dignidad humana (art. 10.1 CE) y se concretan en facultades que garantizan un ámbito libre de intervención y actuación frente a eventuales injerencias o intromisiones.

10 Con respecto a la dimensión objetiva cabría precisar que genera la obligación de los poderes públicos de contribuir a la efectividad de los derechos en su desarrollo, interpretación y aplicación.

11 Véase el artículo 9.1 de la Constitución española. Dicho precepto dispone «*Los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento jurídico*».

municaciones¹² protege tanto el proceso de comunicación como el contenido de la misma. Partiendo de esta definición se puede señalar que el secreto de las comunicaciones garantiza tanto el proceso de comunicación como el conocimiento antijurídico de las comunicaciones ajenas. Además, el derecho también protege la identidad subjetiva de los interlocutores. Con respecto a los derechos de autor véase lo preceptuado en el artículo 20.1.b) cuando señala «Se reconocen y protegen los derechos (...) b) A la producción y creación literaria, artística, científica y técnica (...)». De la dicción literal de este precepto cabría colegir que se reconoce el derecho a crear libremente en el ámbito artístico y a producir en el ámbito científico. También protege el objeto del proceso creador y el derecho a difundir el contenido de lo creado y/o producido.

A tenor de todo lo anterior y teniendo en cuenta la petición de decisión prejudicial formulada ante el TJCE por el Tribunal Supremo de Suecia en el marco del litigio entre las sociedades Bonnier Audio y otros y iPhone –y desde el ámbito constitucional– es necesario traer a colación referentes importantes en aras de intentar delimitar cuál es el escenario del que partimos y cuál es el escenario al que se podría llegar. Referentes como la STEDH de 2 de agosto de 1984, caso Malone, en donde el TEDH reconoce expresamente la posibilidad de que el artículo 8 de la Convención Europea de Derechos Humanos pueda resultar vulnerado por el empleo de un artificio técnico –comptage– que permite registrar cuáles han sido los números telefónicos marcados sobre un determinado aparato aunque no el contenido de la comunicación misma. Referentes como la STJUE, de 29 de enero de 2008, caso Promusca, en donde el Tribunal de Justicia de la Unión Europea declaró que no existe una obligación a los Estados miembros de imponer el deber de comunicar datos personales con objeto de garantizar la protección efectiva de los derechos de autor en el marco de un procedimiento civil. No obstante, conviene significar como el TJCE instó a los Estados miembros a que adaptaran su ordenamiento jurídico interno en aras de garantizar un justo equilibrio entre los distintos derechos fundamentales protegidos por el ordenamiento jurídico comunitario. El TJCE precisó –además– que son las autoridades y órganos jurisdiccionales de los Estados miembros a los que compete interpretar el derecho nacional de conformidad con las Directivas comunitarias. Interpretación que debe evitar conflictos entre derechos fundamentales y principios generales de Derecho comunitario, entre los que cita el principio de proporcionalidad¹³. En cualquier caso –a los objetos de esta comunicación– resulta interesante señalar como el TJCE ve compatible con el Derecho comunitario que los Estados miembros excluyan la comunicación de datos de tráfico personales para la persecución

12 Sobre el secreto de las comunicaciones véase PULIDO QUECEDO, M. (2006). *La noción de «secreto de las comunicaciones postales» ex art. 18.3 CE*. Repertorio Aranzadi del Tribunal Constitucional, núm. 16/2006, Pamplona. Véase también NARVÁEZ RODRÍGUEZ, A. (1999). *Intervenciones telefónicas*. En Repertorio Aranzadi del Tribunal Constitucional, vol II, Pamplona: Aranzadi. Sobre esta materia resulta interesante (también) JIMÉNEZ CAMPOS, J. (1987). *La garantía constitucional del secreto de las comunicaciones*. En Revista Española de Derecho Constitucional, nº 20, pp. 42 y ss.

13 Sobre la proporcionalidad resulta interesante citar la Sentencia del Tribunal Constitucional Alemán de 2 de marzo de 2010 en donde el máximo intérprete constitucional declaró inconstitucional la Ley de conservación de datos por la que se transpone la Directiva 2006/24/CE. Sobre la proporcionalidad resulta interesante – entre otros – el FJ 5 de la STC 66/1995, de 8 de mayo.

por vía civil de infracciones de derecho de autor. Y es que no podemos olvidar que esos datos de tráfico son susceptibles de socavar derechos fundamentales como la intimidad, protección de datos y el secreto de las comunicaciones. Vulneración que se produciría para resolver cuestiones civiles –caso de Promusicae– en donde estamos ante un intercambio de ficheros de música a través de redes p2p sin ánimo de lucro que no constituyen delito.

Junto a los referentes anteriores conviene señalar (también) las sentencias de nuestro intérprete constitucional sobre el valor jurídico de las interceptaciones de las comunicaciones cuando éstas consisten en indagar en los listados de llamadas telefónicas a través de las compañías telefónicas o mediante el acceso a los registros de llamadas de los móviles. Y es que el Tribunal Constitucional en una reiterada jurisprudencia¹⁴ ha venido señalando que el derecho al secreto de las comunicaciones como derecho fundamental consagra la libertad de las comunicaciones y su secreto, estableciendo –en este último sentido– la interdicción de la interceptación o del conocimiento antijurídico de las comunicaciones ajenas. Por tanto, el bien jurídico protegido es la libertad de las comunicaciones. Libertad que se vería socavada tanto si se produjera una interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje con conocimiento o no del mismo, o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado. Además, conviene precisar como la delimitación jurídica del ‘secreto de las comunicaciones’ cubre no sólo el contenido de la comunicación sino también la identidad subjetiva de los interlocutores, de ahí que se haya afirmado que la entrega de los listados de llamadas telefónicas por las compañías telefónicas a la policía, sin consentimiento del titular del teléfono, requiera resolución judicial y lo mismo cabría apuntar con respecto al acceso al registro de llamadas memorizadas en el terminal de un móvil.

Otro aspecto importante sobre el que prestar especial atención –al hilo de la cuestión prejudicial planteada por el Tribunal Supremo de Suecia– es el relativo a la relevancia jurídica del número IP un aspecto no menor y que obliga a tener en cuenta tanto la Consulta 1/1999 de la Fiscalía General del Estado como los Informes de la Agencia Española de Protección de Datos sobre direcciones IP¹⁵ y sobre cesión de datos a las Fuerzas y Cuerpos de Seguridad del Estado¹⁶, sin olvidar los documentos de Trabajo del GdT 29 entre los que destaca el Documento de Trabajo sobre Privacidad en Internet. Y es que un análisis de los mismos determina que la consideración de la dirección IP como dato personal obliga a que la interceptación de los datos de tráfico requiera de un abordaje específico dado su carácter sensible. Un abordaje que entronca directamente en nuestro ordenamiento jurídico interno con la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Norma que contiene un objeto limitado en cuanto a la regulación

14 Véase –entre otras– la STC 230/2007, de 5 de noviembre de 2007. Interesantes resultan también la STC 70/2002, de 3 de abril de 2002 y la STC 114/1984, de 29 de noviembre de 1984.

15 Véase –entre otros– el Informe 327/2003, de la Agencia Española de Protección de Datos, sobre carácter de dato personal de la dirección IP.

16 Véase el Informe 213/2004, de la Agencia Española de Protección de Datos, sobre cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad.

de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. Partiendo de ese objeto limitado que recoge la Ley 25/2007 en su artículo 1 –que supone la transposición de la Directiva 2006/24/CE– resulta cuestionable que se obligue a un proveedor de acceso a Internet para que facilite al titular de un derecho de autor información relativa al abonado al que dicho proveedor asignó una dirección IP concreta.

6. CONSIDERACIONES FINALES

Teniendo en cuenta las consideraciones planteadas al inicio de la presente comunicación y lo dispuesto en los distintos puntos desarrollados a lo largo de la misma cabría resaltar esa visión constitucional que se extrapola de las cuestiones planteadas. Visión que viene determinada por los propios derechos susceptibles de verse afectados y que han sido objeto de planteamiento en la cuestión prejudicial ante el TJCE por parte del Tribunal Supremo de Suecia en el marco del litigio entre las sociedades Bonnier Audio y otros y ePhone en relación con la oposición formulada por ePhone contra una solicitud de requerimiento judicial de revelación de información presentada por Bonnier Audio y otros, en aras de identificar a un determinado abonado. Y es que a tenor del contenido de las Directivas objeto de análisis –a saber– la Directiva 2006/24/CE así como la Directiva 2004/48/CE –parece difícil que pudiera extrapolarse una cierta obligación por parte de ePhone de revelar los datos de identificación del abonado ante el requerimiento realizado por Bonnier y otros en el marco de un procedimiento civil. Cuestión distinta sería que esa cesión de datos se enmarcara en una investigación, detección o enjuiciamiento de delitos graves. No obstante, la cuestión no resulta sencilla máxime teniendo en cuenta el desarrollo normativo interno en Suecia del artículo 8 de la Directiva 2004/48/CE que permite que a efectos de identificación de un abonado (efectivamente) se requiera, en un procedimiento civil, a un proveedor de acceso a Internet para que facilite al titular de un derecho de autor información relativa al abonado al que dicho proveedor de acceso asignó una dirección IP. Desarrollo normativo que –a mi juicio– colisiona con el contenido de la Directiva 2006/24/CE de conservación de datos. Directiva que nació con una finalidad muy determinada que justifica –no sin ciertas dudas en materia de una posible vulneración del derecho al secreto de las comunicaciones– la conservación de datos por parte de los proveedores de servicios de la sociedad de la información con fines de investigación, detección y enjuiciamiento de delitos graves. En cualquier caso, la cuestión está sub júdice¹⁷ y habrá que estar a la resolución del TJCE en aras de analizar los

17 Conviene reseñar que una vez finalizado el texto de la comunicación se ha hecho pública la Sentencia del Tribunal de Justicia de 19 de abril de 2012 («Derechos de autor y derechos afines –Tratamiento de datos por Internet –Vulneración de un derecho exclusivo – Audiolibros a los que se posibilita el acceso gracias a un servidor FTP a través de Internet mediante una dirección IP proporcionada por el

argumentos jurídicos que fundamenten una solución al caso planteado y que nos permitan atisbar hacia dónde se camina en esta materia.

7. BIBLIOGRAFÍA

ARENAS RAMIRO, M. (2007). El derecho a la protección de datos personales como garantías de las libertades de expresión e información. En COTINO HUESO, L. (coord.). Libertad en Internet. La red y las libertades de expresión e información. Valencia: Tirant Lo Blanch.

Consulta 1/1999, de la Fiscalía General del Estado, de 22 de enero de 1999.

Documentos de Trabajo del GdT 29 sobre Privacidad en Internet, de 21 de noviembre de 2000.

GÓMEZ SÁNCHEZ, Y. (2005). Derecho Constitucional Europeo. Derechos y libertades. Madrid: Sanz y Torres.

Informe 327/2003, de la Agencia Española de Protección de Datos, sobre carácter de dato personal de la dirección IP.

Informe 213/2004, de la Agencia Española de Protección de Datos, sobre cesión de la dirección IP a las Fuerzas y Cuerpos de Seguridad.

operador de Internet – Requerimiento al operador de Internet para que facilite el nombre y la dirección del usuario de dirección IP») en el asunto C-461/10, Bonnier Audio AB y otros frente a Perfect Communication Sweden AB. La sentencia analiza las directivas referenciadas en esta comunicación y declara que la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, debe interpretarse en el sentido de que no se opone a la aplicación de una normativa nacional, basada en el artículo 8 de la Directiva 2004/48 del Parlamento Europeo y del Consejo, de 29 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual, que, a efectos de la identificación del abonado a Internet o de un usuario de Internet, permite que se requiera judicialmente a un proveedor de acceso a Internet para que comunique al titular de un derecho de autor la identidad del abonado a quien se ha asignado una determinada dirección IP que supuestamente ha servido para la vulneración de dicho derecho, puesto que tal normativa es ajena al ámbito de aplicación *ratione materiae* de la Directiva 2006/24. Además, precisa el TJCE que carece de interés en el procedimiento principal el hecho de que el Estado miembro interesado no haya adaptado aún su ordenamiento interno a la Directiva 2006/24. El TJCE precisa que las Directivas 2002/58 y 2004/48 deben interpretarse en el sentido de que no se oponen a una normativa nacional que permita al órgano jurisdiccional nacional que conozca de una acción por la que se solicite un requerimiento judicial de comunicación de datos de carácter personal ponderar, en función de las circunstancias de cada caso y con la debida observancia de las exigencias derivadas del principio de proporcionalidad. Se observa como la decisión del TJCE difiere de las consideraciones finales plasmadas en esta comunicación. Lo que – sin duda – nos invita a reflexionar sobre esa deriva que se advierte cuando se extiende la aplicación de unas medidas nacidas en el seno de la lucha antiterrorista a litigios de naturaleza civil. Y es que ¿no estaremos ante nuevas formas de control estatal?

- JIMÉNEZ CAMPOS, J. (1987). La garantía constitucional del secreto de las comunicaciones. En *Revista Española de Derecho Constitucional*, nº 20, pp. 42 y ss.
- MARTÍNEZ MARTÍNEZ, R. (2004). Una aproximación crítica a la autodeterminación informativa. Madrid: Thomson-Civitas.
- NARVÁEZ RODRÍGUEZ, A. (1999). Intervenciones telefónicas. En *Repertorio Aranzadi del Tribunal Constitucional*, vol II, Pamplona: Aranzadi.
- PULIDO QUECEDO, M. (2006). La noción de «secreto de las comunicaciones postales» ex art. 18.3 CE. En *Repertorio Aranzadi del Tribunal Constitucional*, núm. 16/2006, Pamplona: Aranzadi.
- VILASAU, M. (2006). La Directiva 2006/24/CE sobre conservación de datos de tráfico en las comunicaciones electrónicas: seguridad v. privacidad. IDP. En *Revista de Internet, Derecho y Política*, nº 3, UOC. Recuperado fecha de consulta 10/05/2007, en <http://www.uoc.edu/ojs/index.php/idp/article/view/398>.



Retos y oportunidades del entretenimiento en línea.
*Actas del VIII Congreso Internacional Internet, Derecho y Política
(IDP 2012)*

ISBN: 978-84-695-4123-4

Para citar la obra, por favor, utilicen las
siguientes referencias indistintamente:

Cerrillo i Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J.,
& Vilasau Solana, M. (coords.) (2012). *Retos y oportunidades del entretenimiento en línea.*
Actas del VIII Congreso Internacional, Internet, Derecho y Política. Universitat Oberta
de Catalunya, Barcelona 9-10 Julio, 2012. Barcelona: UOC-Huygens Editorial.

Cerrillo i Martínez, A., Peguera, M., Peña-López, I., Pifarré de Moner, M.J., & Vilasau Solana,
M. (coords.) (2012). *Challenges and Opportunities of Online Entertainment.* Proceedings of
the 8th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya,
Barcelona 9-10 July, 2012. Barcelona: UOC-Huygens Editorial.

<http://edcp.uoc.edu/symposia/idp2012/proceedings/>