LA GOBERNANZA DE INTERNET

EN ESPAÑA 2015

IGF SPAIN

FORO DE LA GOBERNANZA DE INTERNET EN ESPAÑA

LA GOBERNANZA DE INTERNET

EN ESPAÑA 2015

IGF SPAIN

FORO DE LA GOBERNANZA DE INTERNET EN ESPAÑA

Con el apoyo de:

Telefónica Fundación Telefónica

Google

orange

Fundación Vodafone España

Gobierno de España · Ministerio de Industria, Energía y Turismo

red.es

ETSIT UPM

POLITÉCNICA

Esta obra ha sido editada por el Foro de Gobernanza de Internet en España (IGF Spain)

Coordinador del Foro de Gobernanza de Internet en España (IGF Spain):

Jorge Pérez Martínez

Coordinadora de la obra:

Silvia Serrano Calle

Maquetación y diseño:

Marina González Llorca

Primera edición: Junio 2015
Libro digital en esta URL

Edita:

Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.
Ciudad Universitaria, s/n 28040-Madrid

ISBN: 978-84-7402-408-1

www.igfspain.com

Contenido

Capítulo 5: Identidad en red de niñ@s y jóvenes 122

Presentación

El 17 de mayo de 1865, veinte delegaciones de diferentes países europeos, entre los que se encontraba España, firmaron en París el primer Convenio de la Unión Telegráfica Internacional. Hoy día forman la Unión Internacional de Telecomunicaciones (UIT), 193 países miembros y más de 700 entidades del sector privado e instituciones académicas pertenecientes a todas las partes del globo. Hace 150 años surgió la imperiosa necesidad de la cooperación internacional para aprovechar el inmenso valor social y económico que suponía el perfeccionamiento de los medios técnicos que permitían enviar mensajes, entonces telegramas, a través de las fronteras artificiales creadas por los hombres. Acababa de nacer una de las primeras organizaciones internacionales multilaterales de la historia cuyo modelo se extendería a todos los ámbitos de las relaciones internacionales entre países soberanos con diferentes culturas y constituciones políticas. Mediante acuerdos y tratados internacionales estas organizaciones multilaterales se enfrentarían a los problemas globales de cada momento y al reto de aprovechar las ventajas de la globalización en un contexto de ausencia de soberanía global.

Cuando celebramos el 150 aniversario de la UIT la historia se repite. Internet, el corazón de las comunicaciones electrónicas del mundo globalizado actual, busca con urgencia un modelo de gobierno que permita preservar y garantizar una Red de Redes única, abierta, descentralizada y segura tal como la concibieron sus creadores. Los debates sobre el control y gobernanza de Internet, que tuvieron lugar durante la preparación y el desarrollo de la Cumbre Mundial de la Sociedad de la Información (CMSI) convocada por La Naciones Unidas en dos fases (Ginebra 2003 y Túnez 2006), pusieron de manifiesto la incapacidad de gobernar la Red de Redes desde modelos multilaterales y por tanto la necesidad de buscar otros modelos que involucrasen, a todas las partes interesadas (*multistakeholder*). Así, además de los gobiernos, en la gobernanza de Internet tendrían que participar las organizaciones técnicas que deciden sobre los recursos críticos de Internet, los agentes económicos que proporcionan las infraestructuras, servicios y contenidos de la Internet comercial, y los representantes de la sociedad civil que defienden a los usuarios. A propuesta de la CMSI, la ONU convocó en 2006 el Foro de la Gobernanza de Internet (IGF), una de las primeras entidades internacionales de naturaleza auténticamente *multistakeholder*. Desde entonces el IGF ha sido el principal lugar de encuentro en el que el conjunto de las partes interesadas han debatido sus puntos de vista sobre los problemas globales de Internet y han compartido sus experiencias sobre la búsqueda de soluciones a estos problemas mediante la colaboración de todos los agentes concernidos.

Siguiendo el ejemplo del IGF mundial, muchos países y regiones han ido creando sus propios foros de debate para analizar los problemas de Internet en sus respectivos ámbitos geográficos. Nuestro país fue uno de los primeros países en involucrarse en este proceso con el lanzamiento a finales del 2008 del Foro de la Gobernanza de Internet en España (IGF Spain, en el ámbito internacional).

Desde entonces, a través del proceso de preparación y el desarrollo de sus Jornadas Anuales, el IGF Spain ha asumido las tareas de producir el debate español sobre la gobernanza de Internet en España y de elevar sus propuestas a la comunidad internacional.

El informe que presentamos supone un cambio cualitativo en las actividades de nuestro foro y sin duda el mejor ejemplo hasta el momento de "best practices & multistakeholder" en este ámbito.

Los temas tratados fueron identificados en el marco de nuestro Consejo Asesor compuesto por más de cincuenta personalidades relevantes de las más diversas entidades públicas y privadas competentes en la materia. Para la elaboración de cada uno los ocho capítulos que componen el informe, se ha constituido un grupo de expertos procedentes igualmente de todos los sectores.

En este informe el lector encontrará el análisis detallado de las principales preocupaciones y controversias que suscita Internet en España. Para ello se documenta e interpretan los acontecimientos de índole técnico, socioeconómico, regulatorio y de política pública sucedidos durante el año 2014 y lo que llevamos del 2015.

El debate sobre la gobernanza de Internet en los foros internacionales, la difícil transformación de ICANN en estructura *multistakeholder* global para la gestión de los recurso críticos de Internet, las amenazas a la seguridad del ecosistema digital, los riesgos sobre la privacidad de las personas, los retos y oportunidades de Internet para los niños y jóvenes, las cuestiones relativas a los derechos sobre los contenidos y la gestión de la propiedad intelectual, el eterno debate sobre la Internet abierta y la neutralidad de red, el empleo y el emprendimiento en la economía digital, son sucesivamente analizados en los diferentes capítulos del informe.

El informe no pretende dar respuesta a los enormes desafíos planteados por Internet, más bien al contrario plantea nuevas preguntas y desafíos. En mi opinión, su principal valor es que describe de forma holística la evolución del proceso de reflexión/acción en que nos encontramos y los necesarios equilibrios que todas las partes involucradas deben alcanzar si queremos que Internet no se fraccione y siga siendo uno de los principales instrumentos de la innovación técnica y social de nuestro siglo.

Para finalizar quisiera agradecer personalmente y en nombre del Foro de la Gobernanza de Internet las contribuciones que han hecho posible esta obra.

En primer lugar, a los patrocinadores del Foro: la Fundación Telefónica, la Fundación Vodafone, Orange, Google, la Entidad Empresarial Red.es, la ETSI de Telecomunicación de la UPM y al Rectorado de la Universidad Politécnica de Madrid.

Quiero también dar las gracias a todos aquellos que de manera desinteresada han contribuido a esta obra. Muy especialmente a la coordinadora general de la obra, a los coordinadores de los grupos de trabajo, a los autores/editores de cada capítulo y a los componentes de los grupos de trabajo.

Sus nombres se encuentran en el frontispicio de cada capítulo, único reconocimiento que podemos hacer en este momento al esfuerzo que han realizado. Muchas gracias a todos.

Madrid, 17 de mayo de 2015

Jorge Pérez Martínez
Coordinador del Foro de
Gobernanza de Internet en España

Resumen

La gobernanza de Internet es un asunto de gran interés para toda la sociedad. Desde sus orígenes ha contado con una organización muy particular, un modelo multipartito o *multistakeholder*, como se denomina en el ámbito anglosajón, que ha funcionado razonablemente. En este modelo horizontal, todas las partes (sociedad civil, comunidad técnica, academia, sector privado y gobiernos) colaboran en pro de un interés común: preservar y garantizar una Internet única, segura y abierta a toda la comunidad.

La supervisión de los recursos críticos es uno de los primeros elementos imprescindibles para garantizar el funcionamiento de Internet tal y como la conocemos, un espacio global, con identificadores y direcciones únicas en todo el espacio, estándares, etc. Los años 2014 y 2015 están siendo especialmente intensos en el ámbito de estos recursos críticos. El organismo privado internacional encargado de su gestión ICANN, bajo la supervisión desde sus orígenes del Departamento de Comercio de los EEUU, está inmerso en estos momentos en un profundo proceso de cambio.

Las limitaciones del modelo de gestión de los recursos críticos han ido evidenciándose a lo largo de los años en los que la desconfianza y suspicacias entre los stakeholders se han hecho cada vez más ostensibles. Las revelaciones en 2014 del ex agente de los servicios de seguridad estadounidenses NSA y de la CIA, E. Snowden sobre la seguridad en Internet fueron el último elemento que contribuyó en la puesta en marcha de este cambio tan significativo del modelo de gestión de los recursos críticos.

Con la transición de funciones de ICANN al organismo IANA el Gobierno de los EEUU está tratando de alcanzar unos objetivos básicos que consisten en dar apoyo a un mecanismo multistakeholder que garantice la apertura de Internet, la seguridad y satisfaga las necesidades de los usuarios de los servicios de la nueva IANA (IANA es en la actualidad un organismo autónomo adscrito a ICANN).

En estos momentos se encuentran en proceso de debate los cambios que deberán realizarse en el modelo de gestión hasta alcanzar el mecanismo multipartito definitivo que controlará los recursos críticos.

Desde distintos países se aboga por la necesidad de encontrar mecanismos que doten a los gobiernos de una presencia más significativa en la gobernanza de Internet, mucho más allá del actual Comité Asesor Gubernamental de ICANN en el que están representados los gobiernos. Otros países llevan años apoyando mecanismos multilaterales como la Unión Internacional de Telecomunicaciones (ITU) para gestionar estos recursos críticos.

Tras la celebración de la Conferencia Netmundial en Brasil en abril de 2014 se reforzaron los mecanismos de consenso en la comunidad para encontrar el camino hacia una transición de las funciones más críticas de ICANN, aunque el proceso no está libre de obstáculos y se está alargando en el tiempo. El plazo inicialmente establecido por la NTIA estadounidense para realizar la transición de funciones de ICANN a IANA expira a finales de septiembre de 2015. La NTIA ya ha anunciado, ante el ritmo del proceso, que si fuera necesario este plazo se prorrogará hasta que la comunidad encuentre el modelo más satisfactorio.

En el ecosistema digital **la seguridad** es un asunto clave. La gobernanza de Internet en este ámbito ha avanzado en los últimos años a nivel internacional. Existe una creciente preocupación por parte de toda la comunidad por la dinámica del sistema y los continuos retos en esta materia. Los ciberataques son cada día más intensos, de mayor magnitud y complejidad. El impacto de estos nuevos ciberataques supone en muchos casos un riesgo mayor y más peligroso que las agresiones tradicionales, ya que el daño que pueden ocasionar es enorme y las vulnerabilidades de las infraestructuras o recursos no son tan visibles.

A nivel internacional el origen de los ataques se encuentra en muchas ocasiones en los propios estados, por ejemplo, los casos de China y Rusia, o los de otros gobiernos occidentales, o EEUU, como las revelaciones de Snowden pusieron de manifiesto.

Otra de las tendencias observadas es la profesionalización de la ciberdelincuencia. En 2014 se han identificado organizaciones delictivas que han encontrado su espacio en la red para cometer sus crímenes. Internet no establece fronteras y en estas organizaciones criminales es habitual que los individuos que forman parte de ellas estén localizados en distintos lugares del mundo. Los grupos más extremistas en sus reivindicaciones sociales también han encontrado acomodo en la red, los *hacktivistas*, algunos vinculados a grupos como Anonymous, realizan sus acciones en el ciberespacio que a su vez sirve de plataforma de captación de nuevos miembros y propaganda.

En España el organismo Red.es y el Instituto Nacional de Ciberseguridad de España (INCIBE) han analizado en distinto estudios a lo largo de 2014 y 2015 las incidencias y tendencias en este ámbito en los hogares españoles. Entre los incidentes más habituales en este ámbito destacan los accesos no autorizados. Situaciones de fraude a través de Internet son también muy frecuentes. Sin embargo algunas medidas de seguridad como el uso de programas antivirus está muy generalizado en los hogares, y los ciudadanos españoles empiezan a mostrar un creciente interés por la seguridad en Internet. La confianza de los internautas en España es elevada a pesar de que casi un 13% de los usuarios encuestados manifiesten tener poca o ninguna confianza en la Red.

Determinados servicios en la red, como los de banca y comercio electrónicos son ejemplos destacados de buenas prácticas en materia de seguridad aplicadas por parte de los usuarios españoles en 2014. La incidencia más destacada por parte de los usuarios es el spam o correo electrónico no deseado, una situación que afecta a todo tipo de dispositivos de conexión a Internet (PC, smartphone, tablet), según reflejan los últimos estudios realizados.

En el ámbito de las Administraciones Públicas y la grandes empresas 2014 ha sido un año especialmente intenso en ataques contra las Tecnologías de la Información y las Comunicaciones (TIC) de gobiernos, administraciones públicas y empresas con alto valor estratégico.
Esta forma de ciberespionaje, junto con el ciberterrorismo y la ciberdelicuencia organizada constituyen nuevas amenazas para la sociedad española y la tendencia es claramente de fuerte crecimiento en los últimos años. 2014 ha sido especialmente intenso, según indican los estudios del CCN-CERT (adscrito al Centro Nacional de Inteligencia español).

También la industria y los operadores de infraestructuras críticas del país han sufrido ataques cibernéticos de creciente complejidad en el último año.

Las respuestas regulatorias a las vulnerabilidades en ciberseguridad son continuas, si bien es difícil adelantarse a los nuevos retos. En la Unión Europea (UE) en septiembre de 2014 se aprobó un nuevo Reglamento Nº 910/2014, sobre identificación electrónica y confianza digital. Otras acciones en proceso durante 2015 son la propuesta de una nueva Directiva para garantizar un nivel común de seguridad de las redes y de la información dentro de la UE o el nuevo Reglamento sobre la protección en el tratamiento de datos personales y su circulación.

En España hay varios proyectos legislativos en marcha desde 2014, como el proyecto de Ley Orgánica de Seguridad Nacional o el anteproyecto de modificación de la Ley de Enjuiciamiento Criminal, y el proyecto de Ley Orgánica de modificación del Código Penal.

Las tendencias tecnológicas han sido muy variadas durante 2014 y continúan siéndolo en 2015. Entre ellas destacan el uso de los smartphones como prueba de identidad, el acceso cada vez más extendido a la red de forma anónima, ocultando la identidad del origen y destino de las comunicaciones, y se ha extendido también al caso de los proveedores de servicio. Otros avances como el uso de criptografía, cifrado en la nube, enrutadores, *proxies* opacos y navegadores específicos ubicados en países con un entorno legislativo permisivo complican el trabajo de las fuerzas de seguridad al dificultar la trazabilidad. La Internet profunda es un espacio que ofrece muchas facilidades para el delito y la ocultación, algo que combinado con formas de pago propias del ecosistema como la moneda virtual bitcoin, dificulta aún más el control de los movimientos de capital.

En la estrategia de protección y prevención en materia de ciberseguridad la colaboración público-privada sigue siendo esencial. La participación de los usuarios finales es imprescindible para mantener la confianza de los ciudadanos que navegan por la red. La armonización del marco jurídico a nivel global en estos aspectos es compleja pero esencial, así como una educación adecuada de los usuarios, especialmente la formación a aquellos que pertenecen a los colectivos más vulnerables.

La **privacidad** es otro de los temas de gran relevancia entre los asuntos destacados de la gobernanza de Internet. El debate sobre esta cuestión ha sido más vivo que nunca durante 2014. A ello han contribuido las cuestiones ya señaladas ligadas al espionaje masivo en la red.
Los casos más alarmantes para la sociedad han sido los de colaboración de gobiernos democráticos y empresas privadas, especialmente en países occidentales.

En Europa el Tribunal de Justicia de la UE publicó dos sentencias en abril y mayo de 2014 que han supuesto un cambio significativo en la forma de abordar la cuestión del derecho a la protección de datos. La primera porque supone en la práctica la derogación de la Directiva 2006/24/CE sobre conservación de datos en las telecomunicaciones, y la segunda porque recoge el derecho al olvido, cuando el criterio de búsqueda en Internet sea el nombre y apellidos de una persona. Si bien el alcance de ambas resulta limitado. En la UE en estos momentos hay un nuevo Reglamento de protección de datos en proceso de elaboración y debate que incluirá aspectos novedosos en el tratamiento de estas cuestiones.

En España la legislación ha sido garantista en la protección de la vida privada de los ciudadanos. En la actualidad hay varias iniciativas legislativas en marcha que inciden en la protección de datos. Algunas instituciones como la Agencia Española de Protección de Datos han ejercido un papel relevante durante 2014 en distintas líneas de actuación como la formación y divulgación en esta materia.

Desde la sociedad civil son numerosas las organizaciones que desarrollan una intensa labor como la orientación hacia la protección de los menores, los usuarios, o los profesionales, por mencionar algunos de ellos. Una de las conclusiones principales de todos los Foros Internacionales sobre Gobernanza de Internet celebrados en 2014 es que la privacidad debe garantizarse para mejorar la confianza de los usuarios y garantizar la seguridad. Están surgiendo nuevas oportunidades como el Internet de las cosas (IoT) o el acceso de múltiples dispositivos conectados permanentemente a la red o los avances que se están produciendo en el tratamiento de la información con el Big Data que traerán consigo problemas de seguridad y privacidad de distinta índole, como ya ocurre con los derivados del consentimiento en Internet relacionado en muchas ocasiones con la aparente gratuidad de aplicaciones y servicios dirigidos a los usuarios.

Las oportunidades y los retos que plantea Internet en un colectivo especialmente sensible como es el de **los niños y los jóvenes** han movilizado a la comunidad desde la gobernanza de Internet prestando una especial atención a estas cuestiones en 2014 como ha venido ocurriendo en los últimos años.

La evolución del ecosistema digital hace que la protección de los menores requiera cambios legislativos. Entre las iniciativas que se han realizado en este ámbito en España están desde aquellas para conocer mejor la problemática, por ejemplo, en 2014 se constituyó una Comisión conjunta de las Comisiones de Interior, de Educación y Deporte, y de Industria, Energía y Turismo con el fin de analizar los riesgos derivados del uso de la Red por parte de los menores, riesgos tanto de Internet como en Internet (de contenidos, de contacto). Dicho trabajo se tradujo en una ponencia de estudio. En la actualidad se está elaborando un Proyecto de Ley para incorporar nuevas obligaciones, más adecuadas a la realidad de la red, adaptando la normativa europea en relación a los menores e Internet para dotar con mayores protecciones a los menores y jóvenes.

En el marco de la Agencia Digital para España el gobierno ha realizado a lo largo de 2014 distintas campañas informativas dirigidas a reforzar la confianza digital y la seguridad de los menores. A través de la Entidad Pública Red.es y en colaboración con las CC.AA. y el Ministerio de Educación, Cultura y Deporte se están realizando planes de formación para orientar a los padres, tutores y educadores en las habilidades TIC necesarias para acompañar a los menores y jóvenes en su aprendizaje digital. Otras iniciativas en marcha son el marco del Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos, liderado por el Ministerio del Interior con recursos formativos generados por Red.es, para su aplicación en el entorno educativo; o el Foro de colaboración público-privada de “Menores e Internet”, impulsado por Red.es, para la protección de los menores y jóvenes en Internet.

Desde el ámbito sanitario se han elaborado protocolos de actuación y colaboración, como el convenio entre Red.es y el Hospital de La Paz y la Sociedad Española de Medicina del Adolescente (SEMA) que ha permitido elaborar una Guía clínica sobre ciberacoso para profesionales de la salud. Los riesgos a los que están expuestos los menores en la red exigen modificar las competencias y responsabilidades de muchos profesionales. En el ámbito de la salud los pediatras están abocados a desarrollar cada día una mayor labor de prevención en salud para un uso adecuado, responsable y seguro de las TIC en coordinación con otros profesionales y el entorno familiar. En el caso de los adolescentes resulta imprescindible una detección precoz del ciberacoso, o la posibilidad de suicidios. Los casos de ciberacoso escolar según el Ministerio del Interior estaban próximos al medio millón en 2014.

El acceso a contenidos violentos, o la pornografía son fuente de trastornos en los adolescentes, por ejemplo. En muchas ocasiones los peligros se deben a una falta de formación en las TIC y a la facilidad de acceso en la web a una información poco adecuada para su edad.

Otras situaciones conflictivas son el creciente ciberacoso escolar, o *ciberbullying* entre menores, o de adultos contra menores con fines sexuales, el denominado *grooming*. La colaboración entre distintos Ministerios para reforzar la seguridad y la protección de los menores en la red sigue más vigente aún en 2015, e incluye planes específicos como el portal chaval.es desde el Ministerio de Interior (Guardia Civil, Policía) en coordinación con el Ministerio de Justicia, el Ministerio de Educación, Cultura y Deporte y el Ministerio de Sanidad, Servicios Sociales e Igualdad junto a las CCAA y Red.es.

No solo el Estado está realizando una labor intensa en este ámbito, también, el sector privado, la sociedad civil y los centros educativos desarrollan una importante labor en el día a día.

Cada año son más los menores que se conectan a Internet y cada vez lo hacen a edades más tempranas. En España se sitúa el inicio en el uso de las TIC entre el primer y el segundo año de vida del menor y está descendiendo.

El tiempo medio que los jóvenes pasan delante de una pantalla de ordenador, smartphone o tablet es superior a las 7 horas diarias. Las redes sociales se han convertido en herramientas de socialización muy extendidas entre los jóvenes españoles. Los factores externos con los que se encuentran los menores cuando acceden a la red son muy diversos y tienen consecuencias. Cómo se realiza el acceso, cuál es el entorno socioeconómico en el que se encuentra el menor, el país, el sistema educativo, etc. son factores que influyen en que el uso sea principalmente consumista y social, o bien tenga un carácter más formativo y creativo. Son enormes las posibilidades de comunicación, como compartir intereses y aprendizaje con otros menores, pero también con todo tipo de personas. Lo que hace necesario vigilar la privacidad no siempre bien gestionada de los jóvenes y menores ante los posibles acosos que pueden surgir en el entorno.

Internet es una herramienta imprescindible que las nuevas generaciones deben aprender a utilizar con inteligencia. Las competencias digitales no son solo instrumentales, ligadas al uso con una orientación laboral o el ocio, sino que deben permitir mejorar el desarrollo de la personalidad, ligadas al conocimiento y al uso creativo, crítico y seguro de las TIC. Es un aprendizaje continuo y adaptativo imprescindible para aprovechar las nuevas posibilidades asociadas al ecosistema digital y sus retos en la evolución hacia la nueva sociedad del conocimiento del s. XXI. Reforzar la identidad digital y la educación en valores en los centros educativos es una de las tareas pendientes.

La utilización de la red como herramienta educativa con experiencias piloto llevadas a cabo en centros educativos en España en 2014 por compañías como Facebook, por ejemplo, son un punto de partida en esa necesaria evolución.

Las cuestiones relativas a **los derechos sobre los contenidos y la gestión de la propiedad intelectual** en el ecosistema digital son un elemento de suma importancia en los debates sobre la gobernanza de Internet. Los contenidos en el ecosistema digital son elementos competitivos a nivel global. Europa y España en particular, deben adaptarse a un nuevo escenario más exigente cada día en la producción de estos contenidos. En este sentido, el impacto económico y estratégico del conocimiento y los desarrollos creativos debieran protegerse adecuadamente, así como avanzar con mayor rapidez hacia un mercado digital único, como está ocurriendo en otras economías desarrolladas, EEUU por ejemplo.

En 2014 se han producido numerosos cambios legislativos en todo el mundo. A nivel europeo en 2014 se aprobó la Directiva 2014/26/UE sobre la gestión colectiva de derechos con una clara orientación hacia un Mercado Único Digital en el espacio de la UE. Entre otras muchas iniciativas en la UE, el Parlamento Europeo aprobó a principios de año una Resolución sobre los cánones por copia privada para mejorar la gestión colectiva de derechos.

La sentencia Svensson del Tribunal de Justicia de la UE a principios de 2014 estableció nueva jurisprudencia al dictaminar que no constituía una acto de comunicación al público proporcionar enlaces a otras páginas de Internet que conducen a obras que pueden consultarse libremente en otra página de la red, aunque sí podría considerarse un acto de comunicación al público si concurren determinadas circunstancias que pueden vulnerar los derechos de propiedad intelectual.

En 2015 se están realizando numerosas iniciativas en la UE, entre ellas la presentación del informe Reda, en enero de 2015, relativo a la armonización de derechos de autor en el ámbito de la sociedad de la información. Otros proyectos pendientes que previsiblemente tendrán gran influencia son las iniciativas legislativas en marcha sobre el Mercado Único Digital en la UE, en un avance hacia una mayor homogeneidad regulatoria, o el Tratado de Libre Comercio entre la UE y los EEUU, en negociación en la actualidad.

En el caso de España, en 2014 se aprobó una nueva Ley de Propiedad Intelectual (Ley 21/2014 de 4 de noviembre) donde entre otros objetivos destacables se ha tratado de mejorar la defensa de los derechos de propiedad intelectual en Internet y de reforzar la protección de los autores.

Por ejemplo, se ha adaptado el límite legal de cita o reseña a los agregadores de contenidos de Internet, reconociendo como un derecho irrenunciable de las empresas editoras y autores de noticias ser compensados económicamente por su trabajo. Estos cambios han tenido consecuencias. Entre ellas una de las primeras fue la decisión de la empresa Google de dejar de incluir en su servicio de noticias Google News a los medios de comunicación españoles y el cierre del servicio Google News Spain. La nueva legislación provocó reacciones y gran polémica entre los cibernautas, creadores de contenidos y asociaciones como Adigital o Adepi, entre otros agentes, que hacen prever nuevos cambios legislativos a medio plazo.

En 2015 se ha mantenido la continuidad de acciones dirigidas por parte de la Administración a mejorar la regulación en el ámbito de la propiedad intelectual con medidas encaminadas a mejorar la autorregulación y la colaboración entre los agentes, muchas de ellas promovidas por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI). La reforma del Código Penal cuya entrada en vigor es julio de 2015, forma parte de nuevas acciones contra la vulneración de los derechos de propiedad intelectual en la red.

Otros cambios legislativos previstos son el desarrollo de nuevos reglamentos como, por ejemplo, para determinar la metodología de las tarifas que deberán aplicar las entidades de gestión. Así como otros trabajos con el fin de trasponer las últimas Directivas aprobadas en la UE a la legislación española.

El debate sobre **Internet abierta y neutralidad de red** ha sido especialmente intenso durante los foros internacionales sobre gobernanza celebrados en 2014. Como se ha señalado, el sentimiento de fragilidad y pérdida de seguridad ante muchas de las revelaciones que saltaron al primer plano de la actualidad en 2014 provocó una crisis de confianza entre los stakeholders con reacciones desde todos los ámbitos y encendidos debates. Las cuestiones relativas a la neutralidad de red y la Internet abierta son temas complejos en el ámbito del ecosistema digital que sobrepasan el análisis a nivel nacional y exigen una amplitud de miras a nivel global ya que su resolución no admite soluciones locales o restringidas a una parte del ecosistema.

En la comunidad no hay una definición unánime sobre qué es la Internet abierta o el alcance de la neutralidad de red. Las discrepancias entre los distintos stakeholders que conviven en el ecosistema digital en algunos casos tienen este origen.
Las posiciones en torno a la cuestión son muy distintas según dónde se centre el debate. Así, mientras los países en vías de desarrollo la defensa de la Internet abierta e integradora se enmarca en un espacio de acceso y crecimiento; en países donde hay censura y la libertad de expresión está limitada, la cuestión de una Internet abierta adquiere connotaciones ligadas al poder y el control de la información.

Cuando el debate se centra en el ámbito económico el conflicto entre modelos de negocio es la cuestión más relevante. Así, los desarrolladores de contenidos y aplicaciones defienden el acceso a las redes con la calidad de servicio adecuada frente a los operadores de telecomunicaciones que reclaman el fin de una asimetría regulatoria y un marco adecuado al nuevo escenario y los nuevos modelos de negocio.

Otro de los aspectos del debate sobre la neutralidad de la red es la gestión de los diferentes tipos de tráfico, en términos de calidad de servicio.

La problemática de la Internet abierta afecta a aspectos esenciales en la red como la competencia en los diferentes eslabones de la cadena de valor de Internet, cuestiones que pueden analizarse desde el punto de vista de los derechos del consumidor, o también el respeto a los derechos humanos en la Red. Uno de los eventos más destacados sobre la gobernanza de Internet en 2014 fue la Cumbre Mundial multipartita sobre Gobernanza de Internet NETmundial celebrada en Brasil en el mes de abril.

Este encuentro ha supuesto un cambio sustancial en el papel que venía ocupando en la esfera pública la gobernanza de la red. Como resultado de este evento se elaboró un documento, no vinculante, sobre los principios de gobernanza de Internet y una hoja de ruta sobre su evolución. No obstante, las cuestiones relativas a la neutralidad de red, a pesar de la gran relevancia que despertaron en la Cumbre, no pudieran avanzar lo necesario para alcanzar un mínimo consenso necesario en este ámbito.

Por todo ello, este debate quedó aplazado al noveno encuentro anual del Internet Governance Forum, IGF 2014, celebrado en septiembre en Estambul, donde una vez más se evidenciaron las discrepancias entre los stakeholders y lo lejos que se sitúan las partes para alcanzar un consenso razonable.

En distintos foros y encuentros internacionales el debate sobre la neutralidad de red ha sido una cuestión que ha generado gran interés durante el 2014. En Europa, en el foro de debate europeo sobre Gobernanza de Internet, EuroDIG, celebrado en Berlín en junio de 2014 también se abordó esta cuestión, en una de las mesas redondas la cuestión de Internet abierta y el debate sobre la neutralidad de red también ocupó un lugar destacado entre los participantes. En el ámbito de la UE, los debates sobre la neutralidad de la red e Internet abierta han sido intensos en el Parlamento europeo durante los primeros meses de 2014, donde los defensores a favor de la neutralidad de red han logrado reforzar algunas ideas en el proceso de debate y enmiendas.

Principios como la no discriminación, o dotar de mayores garantías la gestión del tráfico en la red, o la calidad de los servicios de acceso a Internet han sido debatidos intensamente. En 2015 la discusión continúa en el Consejo de la UE.

En Europa la perspectiva de los operadores europeos de telecomunicación sobre estas cuestiones pone el foco especialmente en posibles vías de solución, situando el debate en la necesidad de un nuevo marco que los operadores llevan tiempo reclamando a las autoridades, un *level playing field*, o un espacio equilibrado en el que poder competir con los servicios de las empresas *Over the Top* (OTT) bajo un marco regulatorio simétrico.

En EEUU se han producido cambios importantes en este tema durante 2014 y 2015. Las consecuencias de resoluciones judiciales como la de la Corte de Columbia en 2014 que aceptó parcialmente una apelación del operador estadounidense Verizon contra la Orden de Internet Abierta adoptada por la FCC en 2010, anulando las reglas de no bloqueo y de no discriminación establecidas en dicha Orden, han provocado cambios regulatorios.

El gobierno EEUU y su presidente Obama han manifestado públicamente su predisposición hacia una Internet abierta y a favor de la neutralidad de red. En febrero de 2015 el regulador de telecomunicaciones estadounidense, Federal Communications Commission (FCC), modificó la regulación reclasificando el servicio de acceso a Internet de banda ancha con la categoría de servicio de telecomunicación. En su definición, este servicio de banda ancha a Internet no incluye a las redes privadas virtuales ni a las redes de distribución de contenidos o los servicios de backbone. Entre las nuevas reglas establecidas destacan el no bloqueo, la no ralentización, no priorizar el tráfico por pago (no discriminación por retribución monetaria o de otro tipo), la no interferencia injustificada, así como mejores mecanismos de gestión y de transparencia.

El ecosistema digital ha experimentado un desarrollo excepcional gracias a las características de Internet, una red abierta, con estándares y protocolos compartidos, abiertos, con un marco regulatorio poco desarrollado a nivel global y su evolución hacia un espacio donde la ubicuidad, la interacción y conexión son permanentes. Que Internet siga siendo una red abierta es esencial para todos aquellos que confían en la continuidad del modelo original en su evolución futura.

El ecosistema digital ha transformado el **entorno económico** y seguirá haciéndolo en el futuro. En esta revolución digital, la gobernanza de Internet desarrolla un valioso papel que deberá hacerse más visible por su relevancia en los próximos años.

Internet es un entorno muy dinámico en el que las posibilidades de crear nuevos negocios son enormes. La innovación, el emprendimiento e Internet van unidas. La innovación de productos y servicios ligados al ecosistema, la innovación de procesos, las innovaciones de marketing y de organización, son innovaciones también tecnológicas que han aumentado la productividad en numerosos sectores productivos. No obstante, el problema del crecimiento, la competitividad y el empleo exigen un esfuerzo por parte de los gobiernos, empresas y de la propia sociedad hacia la digitalización. En este afán el papel de los emprendedores como catalizadores de la innovación es indispensable.

En el nuevo entorno se evidencia la necesidad de fomentar la iniciativa emprendedora, que exige una nueva forma de pensar y entender el mundo y el ecosistema digital.

La creatividad, la capacidad y la motivación características del emprendedor no deben considerarse únicamente elementos individuales o personales sino ser incentivados como sociedad, a nivel organizativo y, también, de entorno regulatorio.

Son numerosas las instituciones y organismos internacionales en los últimos años que destacan las bondades de la digitalización en los indicadores de crecimiento económico, como el incremento del producto interior bruto (PIB), o en la disminución de la tasa de paro, como señalan el World Economic Forum o el Banco Mundial, entre otros. La UE acepta que el denominado dividendo TIC, retorno de la inversión en TIC, genera mayor crecimiento y productividad que otros tipos de inversiones. Los datos justifican estas valoraciones.

Los países de la UE que más han invertido en TIC en los últimos años tienen incrementos de productividad muy por encima de la media. En el caso de España o Italia, por ejemplo, en los que la inversión ha sido mucho menor que en esos países de la UE, el crecimiento medio de la productividad es, también, de los más bajos.

Disponer de las infraestructuras de telecomunicaciones adecuadas para garantizar la conectividad y las velocidades de acceso necesarias en todo momento, requiere ingentes inversiones en infraestructuras, un marco regulatorio adecuado en coordinación con políticas públicas que facilite a las empresas un escenario más predecible y estable, sin asimetrías regulatorias; pero todo esto no es suficiente.

Es necesario que además del acceso a Internet, las nuevas tecnologías se incorporen completamente en los procesos productivos, entre otros efectos se encuentra la automatización de los procesos, se instituyan acuerdos de comercio electrónico a nivel global que establezcan una normativa unificada en temas arancelarios, impositivos, pagos y transacciones comerciales, o incluso en materia de garantías de calidad y protección a los consumidores.

Las competencias digitales son necesarias para el crecimiento de la sociedad en un entorno global, abierto e interconectado. Entre las prioridades identificadas destacan:

La alfabetización digital de la población en riesgo de exclusión.

El reciclaje profesional en los sectores más sensibles a la deslocalización y la globalización.

Adaptación de los programas de estudio en las distintas fases de la educación primaria, secundaria y universitaria.

Uno de los principales desafíos en Europa y, también, en España es el desempleo. El ecosistema digital supone, en este sentido, una gran oportunidad. Uno de los mayores retos en el ecosistema digital es que gran parte del empleo en el ecosistema se realiza en la red y la ubicación geográfica del trabajador es irrelevante, por lo que la competencia es global. Afortunadamente, las oportunidades también son proporcionalmente mucho mayores que en un escenario restringido al ámbito nacional o regional.

Es esencial que los proyectos educativos se hagan más dinámicos e incorporen cuanto antes una formación adaptativa, más adecuada al nuevo entorno socioeconómico que el ecosistema digital representa.

El espacio de Internet ha dado lugar a nuevos modelos económicos, es el caso de la economía colaborativa. La tecnología permite compartir, crear, interaccionar y establecer nuevos modelos de relación en los que la figura de los agentes participantes y sus roles pueden ser varios y dinámicos, con ciudadanos que cada vez más son también productores y consumidores en este ecosistema. Es posible identificar nuevos modelos de producción y organización en este entorno. En el ámbito de comercio electrónico destacan los negocios entre empresa y cliente al modo tradicional oferentes-demandantes, tipo B2C (*business to consumer*) o B2B (*business to business*), B2G (*business to government*), o C2C (*consumer to consumer*).

En este entorno económico han surgido nuevos mecanismos de colaboración financiera como el *crowdfunding* y, también, en esta línea de economía colaborativa mecanismos de cooperación entre consumidores, usuarios, la ciudadanía colaborativa, o la cultura del conocimiento en abierto, por destacar algunos ejemplos.

La evolución del ecosistema de Internet está permitiendo descubrir nuevos modelos de relación social y económica que ofrecen nuevas oportunidades para aumentar el crecimiento de las economías y extender con más facilidad las novedades y mejoras en calidad de vida a los habitantes de todo el mundo. El espacio global de la red es único para el crecimiento, la innovación y los nuevos emprendedores digitales que, afortunadamente, se atreven a embarcarse en una nueva aventura cada día.

Silvia Serrano
Coordinadora de la obra La Gobernanza de Internet en España 2015
Directora de la Oficina Técnica. IGF Spain Secretariat.

Capítulo 1

Evolución y contribución al Gobierno de Internet de los principales stakeholders

Coordinación: **Silvia Serrano Calle**

Editores/Autores: **Sandra López Michavila, Juan Antonio Quintana Franco, Silvia Serrano Calle**

Grupo de Trabajo:

Gonzalo Arranz Santamaría (Becario/ Cátedra Red.es)

Zoraida Frías Barroso (Investigadora/ETSI de Telecomunicación, Universidad Politécnica de Madrid)

Carlos González Valderrama (Investigador/ETSI de Telecomunicación, Universidad Politécnica de Madrid)

Sandra López Michavila (Becaria/ Cátedra Red.es)

Alexandre Marcos Conca (Becario/Cátedra Red.es)

Juan Antonio Quintana Franco (Becario/Cátedra Red.es)

Silvia Serrano Calle (Profesora/ETSI de Telecomunicación, Universidad Politécnica de Madrid)

1 | 1 Orígenes de la Gobernanza de Internet

Desde la creación de Internet como una red científica durante la década de 1960 hasta el ecosistema digital que hoy conocemos la evolución de Internet ha seguido un ritmo veloz. Muchos de los usuarios de la red mundial la perciben como un bien público que pareciera funcionar de manera independiente, por sí mismo. Sin embargo, sus recursos críticos son gestionados por diversas organizaciones en un modelo que, cada vez con más fuerza, es llamado a un cambio. Este cambio pide que su gestión no esté en manos de unos pocos gobiernos u organizaciones, sino que todas las partes interesadas de todo el mundo puedan participar en la gobernanza de Internet.

La gobernanza de Internet es un campo complejo debido a su naturaleza multidisciplinar que engloba una serie de aspectos muy diversos: socioeconómicos, tecnológicos, de desarrollo, legislativos y políticos.

El sector privado, los gobiernos, los usuarios, el ámbito académico, etc. tienen sus propios intereses en Internet. Estados Unidos tuvo el papel protagonista en la creación de Internet y, desde entonces, ha seguido desempeñando un papel fundamental y decisivo en la estructura de Internet, desde la topografía de los ISP hasta la generación de los contenidos que circulan por la red, pasando por la gestión de las direcciones IP y los DNS. Esta situación genera gran debate ya que las funciones centrales de la coordinación de Internet se consideran un activo estratégico de Estados Unidos. Desde hace tiempo se ha intentado moderar ese poder por parte de algunas autoridades públicas en el marco del sistema de Naciones Unidas creando nuevos organismos e instituciones como el Consejo Económico y Social (ECOSOC) y la Unión Internacional de Telecomunicaciones (UIT). La UIT se reúne desde 1994 cada 4 años, a través de la Oficina de Desarrollo de las Telecomunicaciones (BDT), en una conferencia mundial de desarrollo de telecomunicaciones (CMDT).

1 | 1 | 1 Primeros eventos 1994-2011

La Cumbre Mundial de la Sociedad de la Información (CMSI) fue el evento que principalmente promovió el debate sobre la gobernanza de Internet. La primera fase de la CMSI tuvo lugar en Ginebra en 2003 y la segunda en Túnez en el año 2005.

En la primera fase de la cumbre los gobiernos reconocieron el papel de Internet como elemento sobre el que se sustenta la Sociedad de la Información y mostraron su preocupación ante las distintas opiniones que surgían en la gestión de sus recursos, así como el papel de la regulación y las políticas públicas relativas a Internet. En esta primera fase, las visiones de lo que debería ser la gobernanza de la infraestructura técnica de la red quedaron divididas en dos posiciones: por un lado los partidarios de ICANN, favorables a mantener la situación que prevalece desde el nacimiento de Internet, y por otro lado, aquellos que eran partidarios de una transferencia progresiva de funciones desde ICANN hacia la UIT.

En la segunda cumbre se aceptó que todos los gobiernos debían tener un papel relevante en la gobernanza de Internet para garantizar la estabilidad, seguridad y continuidad de la Red. Al principio, Estados Unidos se negó a ceder el control de una tecnología que ellos habían creado. Sin embargo, dado que Internet había tenido un impacto tan grande, Estados Unidos señaló que las entidades comerciales, las instituciones académicas y la sociedad civil debían tener un asiento en las mismas condiciones en la mesa de discusión de la gobernanza de Internet. Esto supuso un paso importante en la idea del Foro de Gobernanza de Internet (Internet Governance Forum, IGF).

Uno de los resultados más exitosos de la CMSI fue el establecimiento del IGF, un espacio abierto y descentralizado para el debate sobre políticas que favorecen la sostenibilidad y solidez de Internet que reúne a los gobiernos, sector privado, comunidad técnica, academia y sociedad civil. El IGF surge a raíz de la batalla por el control de los recursos críticos de Internet que enfrenta a la Unión Internacional de Telecomunicaciones (UIT) y a ICANN.

La agenda para el primer IGF celebrado en Atenas (2006) se elaboró alrededor de cuatro áreas temáticas que engloban de alguna manera la “visión amplia” de la gobernanza de Internet: el acceso, la seguridad, la apertura y la diversidad. En el segundo IGF en Río de Janeiro (2007), se añadió una quinta área temática a la agenda que no había sido incluida en la primera reunión del IGF, los recursos críticos de Internet.

Desde entonces, estas cinco áreas temáticas han ayudado a estructurar la arquitectura del programa del IGF e incluso a dar forma a la definición de la gobernanza de Internet. Aunque las clasificaciones pueden variar en su enfoque, la gobernanza de Internet trata un conjunto de problemas que por su complejidad y alcance se mantienen a lo largo del tiempo, pero cuya relevancia va cambiando cada año.

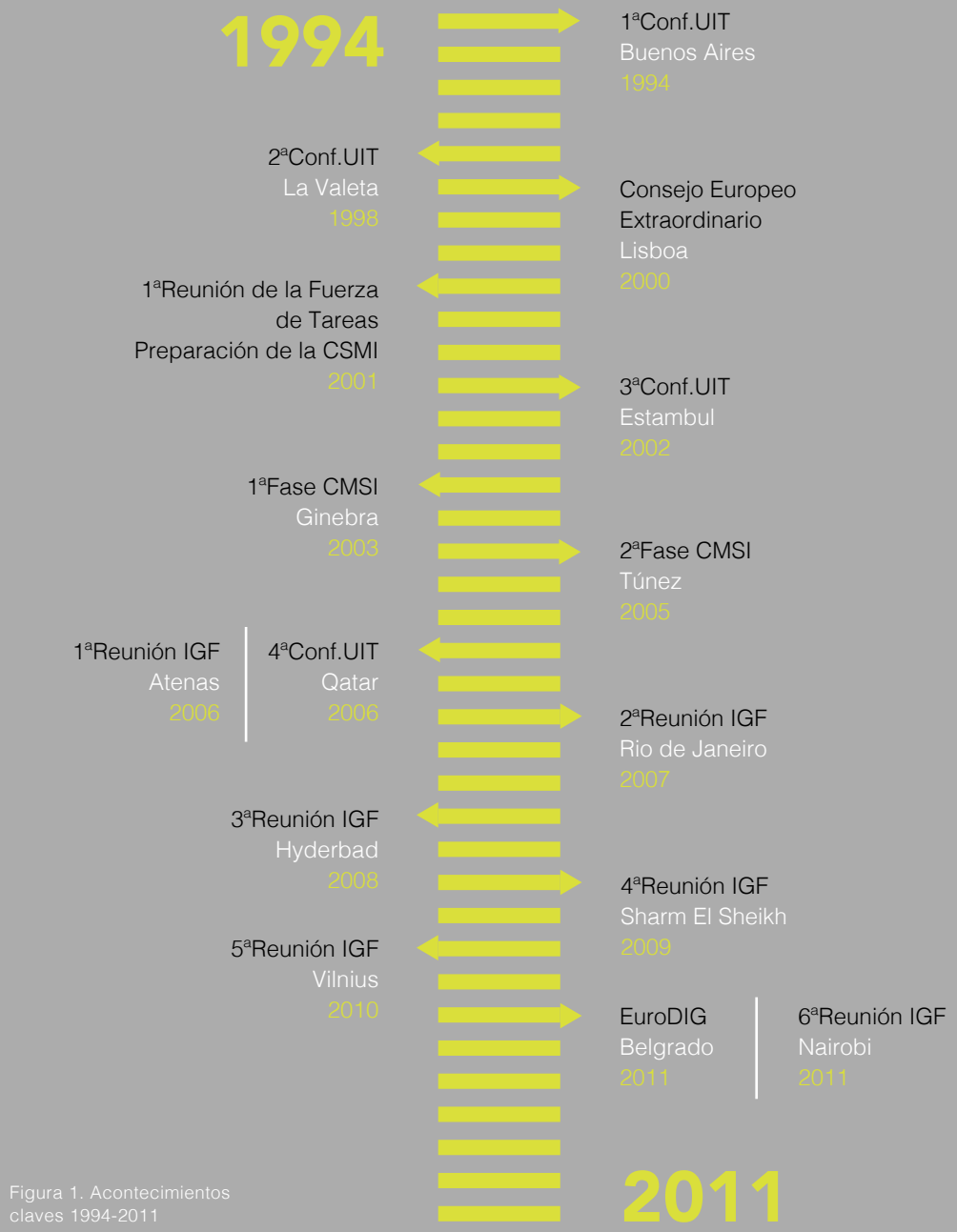


Figura 1. Acontecimientos claves 1994-2011

El Foro de Gobernanza de Internet recibe financiación pública (gobiernos finlandés, suizo, holandés, japonés, noruego, por ejemplo, y también organizaciones tales como la UIT) y privada (ICANN, Siemens, AT&T, VeriSign, Cisco, Google, entre otros).

La gran mayoría de los nuevos actores estaban más en consonancia con las políticas de Internet de Estados Unidos que los de sus rivales. ONGs, académicos y entidades comerciales (muchos de los cuales eran empresas de tecnología con sede en EE.UU.) apoyaron ampliamente las políticas estadounidenses sobre el acceso, la libertad de expresión y la censura.

El gobierno de EE.UU. se ha movido lentamente para debilitar sus vínculos con ICANN. Sus rivales estatales, por el contrario, han tratado con fuerza de cambiar las reglas del juego, y más concretamente en la reunión de 2012 de la UIT (WCIT-2012), donde modificaron el Reglamento de las Telecomunicaciones Internacionales (RTI), aunque fue rechazado por Estados Unidos y sus aliados.

Recopilando los eventos más importantes que se han celebrado hasta el año 2011 incluido puede verse la figura 1.

1 | 1 | 2 Acontecimientos entre 2012 y 2013

El año 2012 tuvo un evento clave en la gobernanza de internet, la Conferencia Mundial de Telecomunicaciones Internacionales (WCIT-2012) celebrada en Dubai. En esta reunión organizada por la UIT se actualizó el Reglamento de las Telecomunicaciones Internacionales (RTI) para que éste abarcase al mundo de las telecomunicaciones actuales, Internet incluido. Sin embargo, esta cumbre escenificó una ruptura importante. Tras la cumbre surgieron dos grupos de países con posiciones muy distintas sobre la gobernanza de internet: aquellos que firmaron el nuevo reglamento y aquellos que no lo firmaron y se quedaron con el antiguo de 1988. En otras palabras, aquellos que mantienen la “Internet justa y segura” y los que quieren la “Internet abierta y libre”.

El nuevo RTI debería entrar en vigor en 2015 y la firma del Tratado por parte de solo 89 de los 144 posibles países firmantes plantea un escenario de fragmentación del marco regulador de las telecomunicaciones ya que coexistirían dos tratados internacionales.

Estados Unidos, Canadá, Japón y los países de Europa, entre otros, no firmaron el nuevo RTI mientras que países como Brasil, Rusia, India, China y Sudáfrica (BRICS) apoyaron el nuevo RTI. Este hecho ha constituido un hito relevante en el debate sobre el papel que debe corresponder a los gobiernos en el control y gestión de Internet. Vid. Figura 2, con los países firmantes del nuevo RTI en color verde; y los países no firmantes en gris.

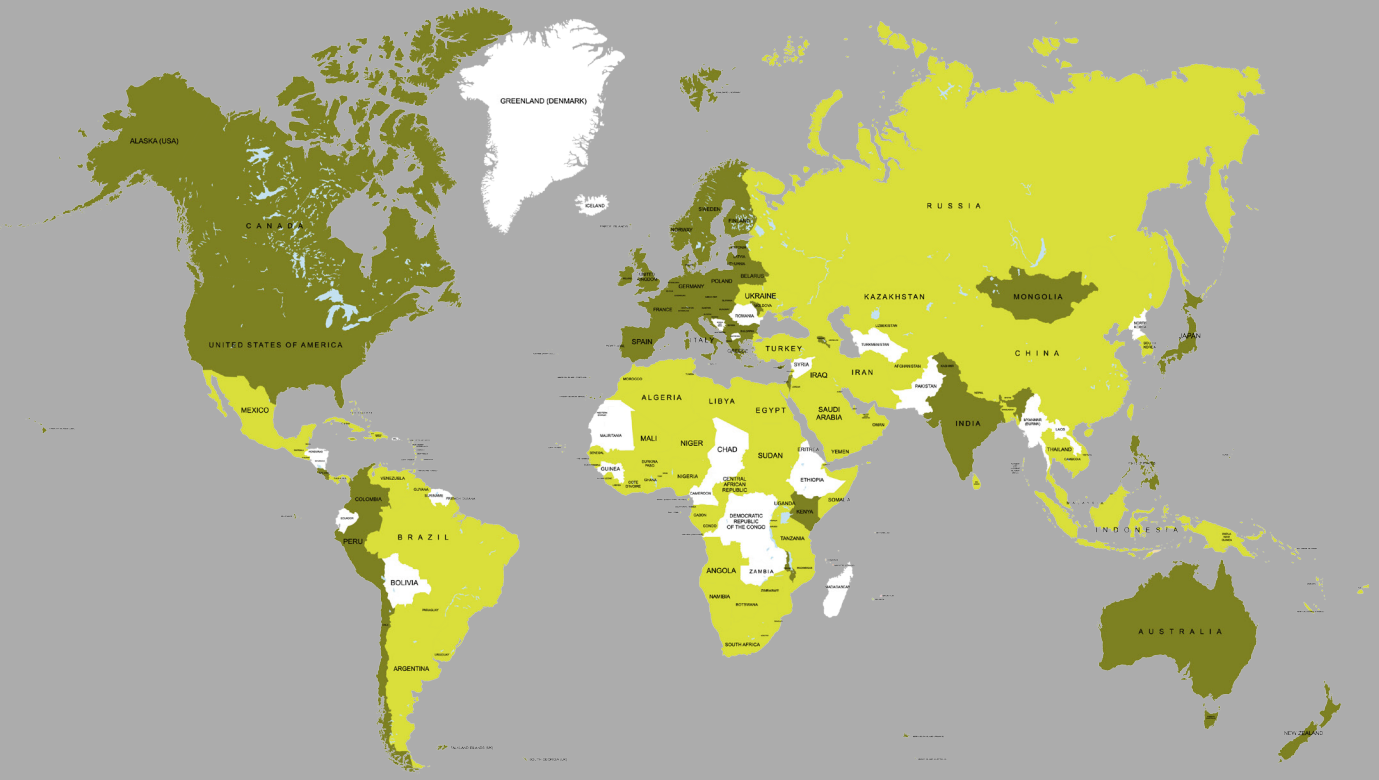


Figura 2. Mapa países firmantes (verde) y no firmantes (verde oscuro) del nuevo RTI

En el mes de Mayo de 2013 tuvo lugar la reunión del Foro Mundial de las Políticas de Telecomunicaciones (WTPF-13) también organizado a instancias de la UIT para intercambiar visiones y poner en común soluciones en torno a las claves políticas en el ámbito de las Tecnologías de la Información y las Comunicaciones entre empresas, gobiernos y la sociedad civil.

Meses más tarde ocurrió sin duda uno de los principales acontecimientos de la gobernanza de los últimos años, el conocido como caso Snowden. Las revelaciones sobre la existencia de programas secretos para la vigilancia electrónica masiva e internacional dados a conocer por el ex-analista de la Agencia de Seguridad Nacional (National Security Agency, NSA), Edward Snowden, han agitado el mundo de Internet y han tenido gran repercusión a nivel global. Una de las reacciones más importantes en este sentido fue la protagonizada por los principales órganos responsables de recursos críticos de la Internet global (ICANN, IAB, IETF, ISOC, W3C y los responsables de numeración IP regionales) en octubre de 2013 mediante la Declaración de Montevideo que insta a reforzar la cooperación multistakeholder en la gobernanza de Internet para proteger a la Red, y en consecuencia a todos los usuarios, de escenarios de fragmentación. Estas revelaciones han puesto en peligro la confianza en el mundo de Internet.

Declaración de Montevideo y su impacto

En octubre de 2013 se reunieron en Montevideo los líderes de organizaciones responsables de la coordinación de la infraestructura técnica de Internet a nivel global para debatir sobre el futuro de Internet. En el que se alcanzaron cuatro puntos importantes de consenso[1]:

- Reiteraron la importancia de una operación coherente de Internet a nivel global y alertaron sobre una posible fragmentación de Internet a nivel nacional. Expresaron su profunda preocupación por el debilitamiento de la confianza de los usuarios de Internet a nivel global debido a las recientes revelaciones acerca del monitoreo y la vigilancia masiva.

- Identificaron la necesidad de realizar un esfuerzo continuado para abordar los desafíos que presenta la Gobernanza de Internet y acordaron catalizar los esfuerzos de la comunidad hacia la evolución de una cooperación global multipartita en Internet.

- Llamaron a acelerar la globalización de ICANN y de las funciones de IANA, hacia un entorno en el cual todos los actores, incluyendo todos los gobiernos, participen en condiciones de igualdad.

- Reforzaron la transición a IPv6, para que continuara siendo una prioridad a nivel global. En particular, los proveedores de contenido de Internet deben entregar contenido a través de servicios tanto en IPv4 como en IPv6.

Las revelaciones relacionadas con la NSA tuvieron un efecto especialmente intenso en el plano político internacional. El gobierno de Brasil aceleró por la vía constitucional de urgencia la aprobación del Marco Civil de Internet en el país – un conjunto de principios reguladores básicos en torno a la neutralidad de red y los derechos de los usuarios en el uso de Internet- , que se encontraba en tramitación. En la misma línea, tanto Brasil como Alemania instaron al resto de naciones a la elaboración de un marco común básico sobre Internet que recogiera los principios fundamentales.

El enfado del gobierno alemán provocó que Barack Obama comunicase su intención de terminar con el polémico programa de vigilancia masiva de llamadas telefónicas de la NSA. La Administración norteamericana prometió trabajar en una propuesta legislativa para reestructurar la forma de acceso, almacenamiento y consulta de esa información, garantizando un mayor control judicial de todo el proceso. No obstante, la fragmentación de Internet parecía una amenaza real.

Esta información secreta desvelada fue un duro golpe que supuso un gran paso para debilitar la supervisión, la autoridad y presunto control sobre Internet de Estados Unidos. Las revelaciones de Snowden avanzaron las discusiones sobre la gobernanza de Internet, la privacidad y la vigilancia en el IGF de Bali 2013 y otros foros internacionales como EuroDIG.

[1]Véase artículo: https://www.icann.org/resources/press-material/release-2013-10-07es

1 | 1 | 3 Principales eventos de la gobernanza de internet en 2014

El año 2014 fue muy relevante para la gobernanza de Internet. Durante ese año sucedieron una serie de acontecimientos sin precedentes que es posible que marquen un punto de inflexión en la gobernanza de Internet. Los más destacados han sido la celebración de la "Cumbre Mundial Multistakeholder sobre el Futuro de la Gobernanza de Internet" NETmundial, y el anuncio de la Administración Nacional de Telecomunicaciones e Información de Estados Unidos (NTIA) de su intención de transferir la custodia de las funciones de IANA a la comunidad global multistakeholder.

Otros eventos importantes en 2014 han sido las tres reuniones anuales de ICANN, la novena reunión anual del IGF y la Conferencia de Plenipotenciarios de la Unión Internacional de Telecomunicaciones (UIT), que se celebra cada 4 años y en la que se elige el equipo nuevo de alta dirección de la UIT.

Algunos de los cambios más esperados, como son el proceso de transición de la custodia de las funciones de IANA y la mejora de rendición de cuentas de ICANN, no verán sus frutos de manera inmediata.

NETmundial

Con los sucesos ocurridos en 2013 y principios de 2014 sobre revelaciones que cuestionaban la seguridad y el modelo de gestión de la red anteriormente mencionados, en 2014 surgió el movimiento NETmundial, que hasta ahora ha sido la cumbre multistakeholder más importante que se ha celebrado por el alcance y consenso alcanzados. NETmundial ha sido un catalizador necesario para reanudar y reconducir el debate en torno a la Gobernanza de Internet. En esta cumbre se elaboró la "Declaración de São Paulo" que recoge una serie de principios generales para la gobernanza de Internet y una hoja de ruta para la evolución de la gobernanza del ecosistema de Internet.

NETMundial se celebró en São Paulo, Brasil, durante los días 23 y el 24 de abril de 2014 con el objetivo de redefinir el futuro de la gobernanza de Internet. Asistieron a este evento participantes de más de 80 países de todo el mundo con representación de todas las partes interesadas (modelo multistakeholder): gobierno, sociedad civil, academia, comunidad técnica y sector privado.

Los orígenes que dieron pie a esta Cumbre de Brasil se remontan a la 68ª Asamblea General de Naciones Unidas celebrada en el mes de septiembre de 2013, donde la Presidenta del Gobierno de Brasil, Dilma Roussef, urgió a que Naciones Unidas comenzara a regular adecuadamente el papel de los Estados miembros en torno a la gobernanza de Internet tras las revelaciones de E. Snowden.

El objetivo era tomar decisiones sobre los temas más candentes, pero con dos focos fundamentales: En primer lugar, fijar los principios de la gobernanza de Internet, y por otro lado, establecer una hoja de ruta para la evolución del ecosistema. ICANN reaccionó al poco tiempo creando una coalición internacional, denominada 1net[2], para fortalecer el carácter multistakeholder de las contribuciones y aportaciones realizadas en el camino y durante la propia celebración de NETmundial.
La comunidad técnica manifestó entonces su deseo de que este debate, todavía en su fase más inicial, tuviera lugar dentro de ICANN, evitando que NETmundial se impusiera trantando de que la discusión se centrase más en cuestiones de política pública, como la privacidad, la accesibilidad, la inclusión de los países en vías de desarrollo, etc.

A partir de las aportaciones recibidas en las consultas previas, el Comité Multisectorial Ejecutivo (EMC) de NETmundial elaboró una propuesta de documento de trabajo y lo sometió a consulta con el Comité Multisectorial de Alto Nivel de NETmundial (HLMC) el 3 de abril de 2014. Después de incorporar las aportaciones del HLMC, bajo la dirección del Presidente de NETmundial y Copresidentes, el Comité Ejecutivo dio a conocer en Internet el borrador final que se emplearía durante las sesiones de trabajo. Este borrador se había dado a conocer previamente a través de Wikileaks, avivando el debate en Internet durante los días previos a su difusión oficial.

El día 22 de abril el senado brasileño aprobó la ley Marco Civil[3] a modo de carta de derechos ciudadanos que establece principios, garantías, derechos y deberes para usuarios y proveedores de Internet. A raíz de este hecho, Tim Berners Lee, uno de los padres de internet, sugirió que en la Cumbre de São Paulo podría crearse una Carta Magna de Internet inspirada en dicho Marco Civil. Sin embargo, finalmente los dos temas principales del Marco Civil de Brasil, la neutralidad de red y la privacidad, tuvieron un papel más secundario a lo largo de la cumbre y una nula presencia en el documento final que se redactó.

[2]1net es una plataforma abierta e inclusiva de múltiples partes interesadas para avanzar en los debates mundiales sobre la gobernanza de Internet. 1net surgió de la “Declaración de Montevideo”, que aboga por los esfuerzos de toda la comunidad hacia la evolución de la cooperación multisectorial mundial de Internet.

[3]Marco Civil da Internet, Lei nº 12.965”, 23 de abril de 2014

Cumbre y declaración de São Paulo

El encuentro NETmundial concluyó con la presentación de la denominada "Declaración Multisectorial de São Paulo", versión final del documento resultante tras el debate. Esta declaración es un conjunto no vinculante de principios generalmente aceptados y una hoja de ruta que se anima a todos los interesados a seguir. Durante la sesión de clausura, en la que se presentó el documento final, Cuba, India y Rusia manifestaron públicamente su intención de no adherirse al documento por no estar de acuerdo en varios puntos del mismo que, según manifestaron violaban la soberanía de las naciones.

La Declaración de São Paulo quedó dividida en los dos grandes apartados sobre los que versaron la Cumbre: "Los Principios del gobierno de Internet" y "La Hoja de Ruta para la evolución futura de la gobernanza de Internet".

El apartado de Principios quedó estructurado en nueve puntos:

1. Derechos humanos y valores compartidos
2. Protección de intermediarios
3. Diversidad Cultural y lingüística
4. Espacio único y no fragmentado
5. Seguridad, estabilidad y resiliencia de Internet
6. Arquitectura abierta y distribuida
7. Entorno propicio para la innovación sostenible y creatividad
8. Principios del proceso de gobernanza de Internet
9. Estándares abiertos

En esta primera parte de la Declaración se identifica un conjunto de principios comunes y de valores importantes que contribuyan a la creación de un modelo inclusivo, multistakeholder, efectivo y legítimo y reconozca que Internet es un recurso global que debe ser gestionado al servicio del interés público.

Los derechos que tienen las personas fuera de la Red también deben ser protegidos en Internet, de acuerdo con las normas internacionales de derechos humanos, incluyendo los Pactos Internacionales de Derechos Civiles y Políticos y de Derechos Económicos, Sociales y Culturales, y la Convención sobre los Derechos de Personas con discapacidad.

Se asume que los principios para la Gobernanza de Internet deben reflejar valores inalienables como la libertad de expresión, la libertad de asociación, la privacidad, accesibilidad, libertad de información y de acceso a la misma y de utilizar internet para el desarrollo económico.

Además, en los principios del documento se garantiza la protección de la limitación de responsabilidad de los intermediarios de manera que promueva el crecimiento económico, la libre circulación de información y la colaboración de todas las partes para combatir las actividades ilegales. Internet debe seguir siendo único, global e interconectado, basado en un conjunto común de identificadores que permita la libre transmisión de datos de acuerdo a la legislación vigente. La seguridad, estabilidad y resiliencia de Internet se identifican como uno de los objetivos fundamentales de todas las partes involucradas en la gobernanza de Internet.

En la Declaración se defiende que Internet debe mantener su actual arquitectura de sistema abierto y su naturaleza de extremo a extremo creando un ecosistema propicio para la sostenibilidad, la innovación y la creatividad. El documento refuerza el modelo de gobernanza multistakeholder, participativo, abierto, transparente, inclusivo, equitativo, accesible, distribuido y colaborativo.

Hasta entonces, muchas de las decisiones sobre la gobernanza de Internet se tomaban sin la participación significativa de todos los interesados. En la hoja de ruta se insistía especialmente en que la toma de decisiones se hicieran bajo el modelo multistakeholder, mejorando la formulación de políticas con el fin de asegurar la plena participación de todos los organismos involucrados, reconociendo los diferentes papeles de las distintas partes.

La transparencia y la rendición de cuentas han adquirido mayor relevancia, en todas las organizaciones, instando a informar de forma periódica sobre los avances logrados en estas cuestiones. El documento aborda la necesidad de profundización del debate a escalas nacionales, haciendo hincapié en la necesidad de replicar a escala local mecanismos de reunión que sirvan como vínculo con las instancias de debate regional y mundial.

Dentro de las mejoras institucionales se generó un importante consenso respecto al fortalecimiento del IGF, garantizando su financiación y que este comenzara a emitir recomendaciones y resultados tras crear los mecanismos necesarios para garantizar el debate y el diálogo permanente.

En el Documento aparece el tema de la transición de la administración de las funciones de IANA, anunciado por la NTIA un mes antes de la Cumbre. NETmundial dio la bienvenida a este anuncio. En la Declaración se exponía que esta transición tenía que realizarse a través de un proceso abierto con la participación de todos los interesados, más allá de la comunidad de ICANN, asegurando la seguridad y estabilidad de Internet, potenciando el principio de igualdad de participación entre todos los grupos de interés, y recalcando el esfuerzo para lograr una transición completa según el calendario inicial que fijaba su fecha de cumplimiento en septiembre de 2015.

En el Documento también se menciona el proceso de globalización de ICANN, que se desea que convierta a esta organización en una realmente global al servicio del interés público con mecanismos de rendición de cuentas y transparencia realizables y verificables. Tras el proceso de debate de las múltiples partes interesadas para obtener puntos de vista de la comunidad acerca de los principios y mecanismos para la transición de la custodia de las funciones de la IANA ejercida por la NTIA, y de la convocatoria sobre la versión preliminar impulsada por la comunidad, se creó el Grupo de Coordinación de la Transición de la Custodia de las Funciones de la IANA (ICG) integrado por 30 personas seleccionadas por las 13 comunidades representadas, encargadas de recomendar un plan de transición de las funciones de custodia de IANA a la comunidad de Internet, en consonancia con los principios clave indicados en el anuncio formulado por la NTIA el 14 de Marzo de 2015.

En los puntos a discutir más allá de NETmundial aparecen los de determinar los diferentes roles y responsabilidades de los multistakeholders en la gobernanza de Internet, los problemas de jurisdicción, los sistemas de evaluación e indicadores de la aplicación de los principios de la gobernanza de Internet y, por último, la neutralidad de la red.

Conclusiones de NETmundial y su documento de salida

Comparando el documento final de NETmundial con el borrador previo a la cumbre, se aprecia que, a pesar de las numerosas aportaciones, apenas se introdujeron modificaciones. A parte de matizar algunos términos, en el apartado de principios para la gobernanza de Internet sólo se ha añadido un nuevo principio: “Protección de los intermediarios”, que parece heredado del Marco Civil brasileño. Por otro lado, el tema de la neutralidad de red, que no aparecía en el borrador y que quizás haya sido el aspecto más destacado y discutido en el evento, no tiene peso en el documento final y, de hecho, solo aparece como un tema a discutir más allá de NETmundial debido a que no se alcanzó un consenso en esta conferencia. Estados Unidos y la Unión Europea, entre otros, se negaron a añadir la Neutralidad de red en el texto.

Los representantes de la sociedad civil mostraron su descontento respecto a que la neutralidad de la red quedara excluida y no se hiciera mención al escándalo del espionaje global ni se criticara con mayor dureza la vigilancia masiva de la National Security Agency (NSA) ni de las empresas cómplices del espionaje, ya que fue una de las razones por que surgió este evento mundial y una de las preocupaciones que más ha aparecido en las aportaciones recibidas para los documentos iniciales.

NETmundial fue un éxito por el impacto y la gran participación que logró, implicando a todos los grupos de interés y un gran número de países, entre ellos países en desarrollo que no habían estado anteriormente representados en eventos de este tipo. La participación multistakeholder, su impacto y el hecho de haber elaborado un documento de salida, dieron legitimidad a NETmundial, pese a que la Declaración no fuera vinculante.

Berlín EuroDIG 2014

En junio de 2014 se celebró la reunión anual de European Dialog on Internet Governance (EuroDIG) en la capital de Alemania. El evento siguió a NETmundial y al anuncio del gobierno estadounidense de iniciar el proceso de transferencia de las funciones de IANA a la comunidad internacional. EuroDIG se situaba en esos momentos como un foro de referencia para la continuación de los debates anteriores respecto a la gobernanza de Internet con el componente adicional de ser un foro realizado en Europa y, por tanto, la posición de Europa ante el panorama internacional ocupa un lugar destacado. El lema que adoptó esta edición fue el de "La sociedad digital en juego: Europa y el futuro de Internet".

Las jornadas se enfocaron sobre diversos temas de debate, como la sociedad digital, la ruptura de la confianza pública en Internet, la seguridad y la economía de Internet. Las principales cuestiones abordadas se presentas a continuación.

La sociedad digital en juego: Europa y el futuro de Internet

El lema del encuentro invitaba a la reflexión sobre la situación de Europa en el contexto internacional y su capacidad para jugar un papel relevante en la gobernanza de Internet, especialmente dada la situación de creciente decadencia de la industria TIC europea.

Cuestiones como la necesidad de preservar los derechos humanos en Internet estuvieron presentes en el debate, buscando fórmulas más efectivas, indicando como uno de los próximos pasos abordar el problema de los conflictos de jurisdicciones en Internet. El papel de los Estados y el rol de los distintos stakeholders para preservar los derechos humanos, en la red y fuera de ella. Los Estados y la legislación son los garantes en última instancia.

La idea de consenso aproximado, o "rough consensus" en el ámbito social, donde cada vez son más las partes implicadas en el ámbito del policy-making apostando por crear normas y acuerdos, que aunque inicialmente no tengan el consenso deseado puedan dar lugar a nuevas vías de resolución de los problemas pendientes. Como se ha conseguido en otros ámbitos más técnicos de la red como los estándares técnicos.

La legislación en Europa protege una amplia variedad de derechos. Un reto para el continente cuando se enfrenta a la protección de todos ellos en el ciberespacio, donde convergen las jurisdicciones de tantos países. Como ejemplo, los derechos a la protección de los datos o a la vida privada, no se reconocen como fundamentales en otras regiones del mundo. Hacer cumplir la legalidad en ocasiones es origen de puntos de conflicto.

Las estructuras de gobernanza y nuevos marcos de cooperación y colaboración en la red fueron otro de los aspectos contemplados en el debate.

Ciberseguridad y derechos humanos

La cuestión de la ciberseguridad y la protección de los derechos humanos se abordó desde diferentes ópticas como son los mecanismos necesarios para luchar contra la ciberberdelincuencia en espacio en el que confluyen diferentes marcos jurídicos; por otro lado debatió sobre el equilibrio necesario entre la ciberseguridad y otros derechos fundamentales, como la privacidad, en clara alusión a las revelaciones sobre los programas de vigilancia masiva.

La seguridad en Internet es a menudo utilizada por los Estados para justificar injerencias arbitrarias en los derechos fundamentales de los ciudadanos. Mediante la aplicación de definiciones vagas a términos como “seguridad nacional” y “terrorismo” muchos gobiernos adoptan medidas desproporcionadas como la vigilancia masiva de las actividades online de sus ciudadanos. Por lo tanto, se apuntó a que el desarme digital era una necesidad urgente.

El conflicto de jurisdicciones fue una cuestión recurrente en todos los debates que tuvieron lugar en EuroDIG2014.

Sin embargo, el último plenario celebrado abordaba directamente este problema desde la óptica de la ciberdelincuencia, llevando por título “Un ciberespacio seguro y no fragmentado. El estado de derecho en un entorno transfronterizo”. En él se abordó la problemática de los marcos institucionales para ciberseguridad, la universalidad de Internet y la necesidad eliminar la fragmentación existente, así como del papel de los intermediarios en el ecosistema de la ciberseguridad. En la discusión se mencionó que una de las causas de la fragmentación del ciberespacio era la confusión sobre los términos y sobre lo que realmente engloba la ciberseguridad, por ejemplo, hay que saber distinguir bien entre la ciberdelincuencia, la ciberguerra o la seguridad nacional de un país. Una de las conclusiones más destacadas es la necesaria colaboración entre los sectores público y privado, que deberá ir más allá de las cuestiones sobre el papel de los ISPs en la lucha contra la ciberdelincuencia y considerar todos los intermediarios posibles, incluyendo las plataformas, los proveedores de servicio global, los proveedores de comercio electrónico y otras entidades.

Accesibilidad

Los debates en torno a la accesibilidad estuvieron focalizados hacia encontrar retos y posibles soluciones en cuanto al acceso, la inclusión y el empoderamiento. Casi un 20% de la población europea nunca ha usado Internet y se abordaron cuestiones como la accesibilidad, incluyendo a discapacitados, pero también a mayores y niños. La digitalización ha traído consigo muchas ventajas para las personas discapacitadas, que es necesario aprovechar y percibir también como una oportunidad, para lo que se necesitan estándares y cooperación público-privada.

Un problema que se identificó para el desarrollo fue las diferentes situaciones de partida entre los distintos países europeos. Cada uno tiene sus leyes específicas sobre estas cuestiones, lo que supone un conflicto para las compañías si quieren proveer servicios en distintos países así como para los usuarios que se trasladan o desplazan por Europa. Hubo consenso en la importancia de la armonización de las normativas referentes a estos temas en Europa.

Desarrollo económico y TIC en Europa

La sesión plenaria sobre el desarrollo económico se enfocó hacia tres temas principales: el papel de las pequeñas y medianas empresas (PYMES) en la economía digital, los nuevos modelos de negocio online, y cómo reducir las barreras regulatorias a la innovación para competir en mercados globales.

El debate comenzó reconociendo el papel fundamental que ha constituido la naturaleza abierta de Internet para la innovación y la generación de nuevos servicios y nuevos modelos de negocio, buscando la forma de equilibrar una Internet libre y abierta con un ecosistema sostenible en su conjunto.

Se remarcó la importancia de las PYMES que desarrollan productos y servicios disruptivos, muy importantes en la innovación en el ecosistema de Internet y la economía digital. Sin embargo, en Europa el marco regulatorio existente supone una fuerte barrera que dificulta la posibilidad de alcanzar la escala necesaria para que estas empresas puedan competir a nivel global, porque no hay un verdadero mercado interno, con 28 ordenamientos jurídicos que dan lugar a barreras en el ámbito del derecho contractual o de fiscalidad, en el derecho laboral, en el cumplimiento de los mismos o en el ámbito de la normalización. Se apuntó a la necesidad de acelerar la integración europea de los entornos normativos y hacerlos ágiles para apoyar y no obstaculizar la evolución de la tecnología y los negocios. Además, se señalaron otros factores sobre los que resulta necesario actuar, como los sistemas educativos, o la aversión al riesgo y al fracaso, más apalancado en los ciudadanos europeos que en los de otras regiones del mundo.

Otra de las cuestiones en el debate fue la desventaja de las empresas europeas frente a las de otros países, como las estadounidenses, por lo restrictivo de la legislación europea en la mayoría de los ámbitos, por ejemplo, la protección de datos y la necesidad de equilibrar las condiciones para que pueda darse una competencia real.

Neutralidad de red

El debate se centró en las redes y el acceso físico a internet. Cuestiones como la gestión de tráfico, relacionado con la calidad de servicio, de forma adecuada, transparente y no discriminatoria. Se apuntó a la necesidad de aplicar el principio de neutralidad de red para garantizar los derechos fundamentales de los usuarios en Internet.

Se debatió sobre cómo la propuesta de Reglamento de Mercado Único de Telecomunicaciones de la Comisión reconoce los servicios especializados, siempre que no causen un perjuicio para la calidad de la “Internet abierta”.

Copyright

Durante el EuroDIG se celebró un importante debate sobre los marcos reguladores en relación con los derechos de autor. Se reconoció que la Comisión se ha esforzado para reformar el copyright. Pese a ello, las dudas sobre los resultados en la Unión Europea, y lograr que se reflejen en la legislación las posiciones y los puntos de vista de los diferentes grupos de interés de las sociedades europeas es un tema complejo. Las leyes actuales sobre copyright difieren online y offline. Considerando el estado actual, los mismos derechos de los usuarios que se aplican offline deberían garantizarse online. El consenso sobre la necesidad de una reforma legislativa en este sentido se manifestó, así como establecer unos estándares mínimos que aseguren que se mantienen algunos de los ideales más holísticos de interés público del derecho de autor que han tenido lugar desde el principio.

Esto no será posible sin la colaboración y el diálogo entre las múltiples partes interesadas que consigan la elaboración de un nuevo reglamento para la regulación del copyright.

9º Internet Governance Forum, Estambul 2014

En septiembre de 2014 se celebró el 9º Foro de la Gobernanza Internacional IGF en Turquía. El lema del foro de este año fue "Conectando continentes para mejorar la gobernanza multistakeholder de internet".

Tras la celebración del encuentro NetMundial en Brasil en el mes de abril ese mismo año, el IGF se vio obligado a tomar el testigo de los asuntos más importantes allí debatidos, tratando de concretar algunas de las propuestas ya debatidas en foros anteriores. Pese a ello, los resultados obtenidos no consiguieron estar a la altura de las expectativas creadas, aunque sí puede reconocerse un significativo avance de cara al futuro. La influencia de NetMundial sobre el IGF 2014 fue muy notable en sesiones plenarias como la organizada sobre neutralidad de red, una de las sugerencias lanzadas desde NetMundial y que el foro aceptó. Otra de las novedades de este IGF fue la recuperación de los foros orientados a trabajar en el ámbito de las mejores prácticas Best Practices Forum, cuyas recomendaciones han sido publicadas tras someterse a distintos procesos abiertos de consulta pública.

Entre los temas principales que se abordaron en los 225 workshops[4] destacaron los centrados en:

- Políticas para facilitar el acceso a Internet
- Creación de contenidos
- Divulgación y utilización
- Internet como motor de crecimiento y desarrollo
- El rol de IGF en el futuro ecosistema de Internet
- Mejora de la confianza digital
- Internet y los derechos humanos
- Recursos críticos en Internet
- Recursos críticos en Internet

El enfoque de IGF ha seguido siendo fiel a su espíritu inicial, un foro de encuentro integrador, sensible a distintas visiones, de participación abierta y con un modelo multistakeholder, siendo esta una de las principales características del IGF[5].

El mandato de Naciones Unidas para la continuidad del IGF más allá de 2014 estaba aún pendiente de ratificación y fue otro de las cuestiones a debate. A pesar de los intentos por lograr una postura de consenso durante el foro, no fue posible avanzar más allá del acuerdo general sobre la necesidad de la renovación y continuidad del IGF. Tampoco fue posible alcanzar en este encuentro un consenso sobre el papel que debería desarrollar el IGF en el futuro, como ir más allá de ser un foro de encuentro y debate.

Entre los temas más destacados abordados en el IGF se encuentran:

[4]http://www.intgovforum.org/cms/wks2014/index.php/proposal/list_public_accepted

[5]Las transcripciones de todas las sesiones principales y los diferentes workshops celebrados durante el noveno IGF están disponibles en la web, así como distintos contenidos de vídeo de muchas de las sesiones: http://www.intgovforum.org http://www.youtube.com/user/igf - http://twitter.com/intgovforum http://www.facebook.com/IntGovForum

Revisión del mecanismo multistakeholder y evolución del rol de IGF en la gobernanza de internet

El IGF se enfrenta al reto de adaptarse a los cambios en el ecosistema digital. En las sesiones celebradas en Estambul numerosos stakeholders (con participantes de la UNESCO, el CSTD, la UIT, organizaciones como ISOC, ICANN y otras organizaciones representantes de la sociedad civil) reclamaron un papel del IGF más orientado a la acción, con resultados concretos que permitieran prepararse para los retos futuros y dar continuidad al trabajo realizado. Un proceso de gobernanza de internet que permite a todos los agentes participar en las mismas condiciones, junto a transparencia, sostenibilidad y apertura son muy apreciados.

La idea de un ecosistema de internet a nivel global es un modelo válido pero también se reconoció el trabajo a nivel nacional o regional. El enfoque de la gobernanza de internet más integrador, especialmente en países en vías de desarrollo, de forma que aquellos países o regiones que no estén conectados pasen a estarlo, entendiendo esa conexión en un sentido amplio, que se extiende más allá del acceso, incorporando, además, al ámbito del diálogo el desarrollo de nuevas medidas políticas y las regulaciones necesarias. Facilitar la participación, en especial la de los países en vías de desarrollo, la divulgación y la innovación. Una de las conclusiones es que el IGF debería funcionar transfiriendo el conocimiento recopilado y avanzando desde el diálogo a la acción.

En el foro se discutió sobre la creación de nuevos mecanismos más inclusivos, manteniendo la participación de los stakeholders en igualdad de condiciones, pero valorandose la posibilidad de gestionar de otra forma esta participación en términos de tiempo, extensión, etc. Como la participación antes y después del foro anual, los mecanismos que utiliza el MAG, Multistakeholder Advisory Group, encargados de la organización y planificación de los IGFs, involucrado en los workshops o sesiones que tienen lugar durante el foro, etc. El IGF es un foro abierto donde todo está sujeto al debate y esto es extensivo al propio foro.

Neutralidad de red

El debate de neutralidad de red despertó muchas expectativas y también opiniones enfrentadas entre los distintos stakeholders participantes en el IGF.
En el último foro de NETMundial celebrado en Brasil este tema fue muy controvertido y el debate quedó pendiente de continuar desarrollándose en este IGF.
En esta ocasión el debate se centró únicamente en algunos de los aspectos que supone la neutralidad de red. Se trató de alcanzar puntos comunes en la misma definición de qué es la neutralidad de red y su análisis desde distintas perspectivas, principalmente el enfoque se ha centrado en tres aspectos: el técnico, el social y el económico, aunque todos ellos estén interrelacionados.

Algunas propuestas como el zero rating defendidas por algunos ponentes por su éxito en distintos mercados y posible solución para otros, encontraron críticas de otros asistentes que no compartían esa misma valoración. Este es uno de los temas en los que se evidencia que no hay consenso y no hay una decisión válida para todos de forma global. Salvo aspectos como la necesidad de mayor transparencia o de reforzar el contenido legal, donde hay unanimidad, el debate está muy abierto y será necesario seguir trabajando en este tema en el próximo IGF en septiembre de 2015.

ICANN y la transición de IANA

La autoridad para asignación de dominios, direcciones IP, numeración y otros recursos relativos a protocolos en Internet, Internet Assigned Numbers Authority (IANA) está inmersa en un proceso de transición en todos los aspectos relacionados con la administración de la misma. IANA es en la actualidad un organismo adscrito a ICANN, Internet Corporation for Assigned Names and Numbers, una organización internacional sin ánimo de lucro con sede en California. En esta evolución de IANA hacia un nuevo modelo de gestión, los distintos miembros presentes en el ecosistema de Internet tienen diferentes ideas para mejorar el modelo actual. Con este fin en el noveno IGF se celebraron varias sesiones que recogieron la diversidad de opiniones y permitieron entender mejor las funciones de IANA.

Una de las primeras conclusiones de esas sesiones en el IGF fue el convencimiento de lo difícil que sería cumplir con el calendario establecido para el proceso, tal y como se había diseñado, ya que no contemplaba la participación multistakeholder.

La gobernanza y el modelo de rendición de cuentas de ICANN es otro tema importante ligado al anterior que preocupa a la comunidad, interesada en que el proceso y los resultados de la transición sean lo más transparentes y eficientes posible. Este tema también fue debatido en Estambul durante el IGF, y en este caso no solo por los expertos y los técnicos más involucrados directamente, como es habitual, sino además por toda la comunidad enriqueciendo el debate. La participación multistakeholder está muy alineada con mejorar la rendición de cuentas de todos los organismos involucrados en la gobernanza de internet, especialmente en cuestiones técnicas como estas. Una de las conclusiones de estas sesiones fue la necesidad de adoptar mecanismos de participación que garantizasen la presencia multistakeholder para aumentar el alcance del proceso, dar mayor confianza en el mismo y dotarle, en definitiva, de mayor legitimidad.

Mejora del acceso, crecimiento y desarrollo de Internet

El principal problema de los países en vías de desarrollo sigue siendo el acceso y crecimiento de Internet. Uno de los próximos retos es lograr los próximos cuatro mil millones de personas conectadas a nivel global, lo que sin duda será uno de los temas a abordar en la agenda del próximo IGF en 2015. La disponibilidad de datos estadísticos fiables es uno de los inconvenientes para evaluar en un contexto supranacional el número de hogares y personas conectadas a la red, establecer estándares que permitan aplicar una metodología e incrementar la transparencia han seguido siendo temas de debate en este foro.

La creación de contenidos es uno de los factores determinantes para el crecimiento y el desarrollo de Internet, impulsado a su vez por el lado de la demanda, que a su vez reclama mejor acceso a las nuevas aplicaciones. En el foro se trataron de identificar estrategias que permitieran acelerar ese desarrollo, pero las infraestructuras siguen siendo un elemento esencial, en particular el acceso a la banda ancha y la disponibilidad de la tecnología. Reducir la brecha digital sigue siendo una prioridad, y a ello contribuye el acceso abierto, especialmente en materia de recursos destinados a la educación. Otra de las conclusiones importante en este contexto es que los profesores y educadores estén formados adecuadamente en competencias digitales.

En el IGF se ha abordado el tema de reconocer el acceso a la banda ancha universal como un derecho universal fundamental para conseguir una sociedad digital abierta, que facilite el acceso a los discapacitados y atienda aspectos como el multilingüismo. Entre otros aspectos contemplados en estas sesiones destacó la necesidad de formar e incentivar la participación de los más jóvenes en el crecimiento de la red, la neutralidad de red es otro de los temas que más preocupa en este ámbito y el respeto a los derechos humanos, que destacan como elementos cruciales en la evolución a futuro de la red.

Derechos humanos

Los asuntos relacionados directa o indirectamente con los derechos humanos ocuparon un papel destacado en el debate. Distintos aspectos se han abordado en todos los encuentros anteriormente celebrados en las reuniones anuales del IGF por lo que el debate en este ámbito tiene una notable madurez. En esta ocasión se centró en particular la implementación de ciertos derechos o principios básicos a nivel nacional o en determinadas regiones geográficas.

Muchos de los participantes sugirieron que el IGF mantuviera un contacto periódico con otros organismos de Naciones Unidas y con instituciones regionales que trabajan en materia de la defensa de los derechos humanos relacionados con Internet y la seguridad en la red. El documento final elaborado en el foro NETmundial en la defensa de los derechos humanos estaba influenciado por los debates que en anteriores foros del IGF se habían desarrollado y a su vez ha servido de base para trabajar en este foro en el avance del reconocimiento de esos derechos a nivel regional y nacional.

Una de las recomendaciones lanzadas desde los participantes en estas sesiones fue la creación de un nuevo best practice forum para el próximo IGF 2015, que recoja las recomendaciones y mejores prácticas para proteger la privacidad en el mundo digital.

Best Practices Forums

La puesta en marcha de distintos Forums sobre mejores prácticas en temas relevantes para la gobernanza de internet fue una de las iniciativas más novedosas del 9º IGF. Estos forums representan un cambio importante en la línea de trabajo habitual del IGF, pasando de los debates a la acción, produciendo resultados tangibles de los que quede constancia documental y acciones concretas.

Compartir el conocimiento y las experiencias de los distintos stakeholders es una fórmula contrastada para mejorar la gobernanza de internet. Se trata de una iniciativa que pretende pasar del debate de las ideas a un enfoque más pragmático en el que se definan métodos y prácticas comúnmente aceptadas que se han demostrado útiles para conseguir los mejores resultados. Aunque el título traducido al español es las mejores prácticas, en realidad el acuerdo generalizado es que se buscan las mejoras prácticas o las lecciones que pueden extraerse en ese ámbito hasta la fecha, para precisar el objeto de esos forums. Esta es una iniciativa abierta a todos los stakeholders, en la que participan además consultores profesionales y expertos. La adopción de cualquier recomendación por parte del IGF sigue un enfoque dinámico y flexible porque las recomendaciones válidas hoy pueden dejar de serlo mañana y deberán seguir evolucionando al ritmo que marca la propia evolución de internet, que es muy rápido. Dentro de estos nuevos foros dirigidos a recoger las mejores prácticas se establieron inicialmente cinco ámbitos principales:

- Desarrollo de mecanismos significativos multistakeholder
- Regulación y minimización de las comunicaciones no deseadas (Spam)
- Establecimiento y soporte CERTs para la seguridad de Internet
- Creación y provisión de un entorno para el desarrollo de contenidos locales
- Seguridad y protección de los menores en la red

IGF regionales y nacionales

Las iniciativas de creación de IGFs nacionales y regionales surgieron nada más crearse el primer IGF internacional. En primer lugar empezaron los foros de gobernanza de internet a nivel nacional, entre los pioneros se encuentra el foro IGF España, y más tarde los regionales. Estos foros regionales y nacionales que funcionan con autonomía son un elemento importante en la participación y preparación del propio foro IGF internacional y permiten realizar un trabajo diversificado y más distribuido con un enfoque adaptado al entorno.

En estos momentos hay once entidades que se definen a sí mismas como iniciativas IGFs regionales y otras 20 IGFs nacionales.
Se celebran además foros adicionales, por otra parte las iniciativas y reuniones a nivel nacional y regional son muchas y diversas a lo largo del año y del mundo.

Uno de los asuntos abordados en el IGF 2014 con sesiones específicas fue identificar los aspectos que podrían tratar mejor los foros regionales y nacionales y qué similitudes pueden encontrar en aquellos foros las distintas materias que se tratan en el IGF. La colaboración y participación de los IGFs regionales y nacionales en el IGF internacional es constante, especialmente para llevar el debate a todo el mundo, con un enfoque más específico y adaptado a la idiosincrasia de cada lugar. En general, los foros regionales y nacionales funcionan con autonomía y son muy variados, respondiendo a la necesidad de lograr cambios en internet, adaptados a lo que demanda el contexto económico y social de cada país.

Capítulo 2

Recursos críticos. Avances destacados en la Gobernanza de Internet

Coordinación: **Ana Olmos**

Editores/Autores: **Ana Olmos**

Grupo de Trabajo:

Jesús Cano Carrillo (Secretario/IEEE e-Government Computer Society)

Lluís Dalmau (Fundació guifi.net)

César García (Capítulo Español de ISOC (ISOC-ES))

Gaël Hernández (Packet Clearing House)

Josep Ibañez (Universitat Pompeu Fabra)

Carlos E. Jiménez Gómez (Presidente/IEEE e-Government)

Paloma Llaneza (Abogada, Socia Directora/Razona Legal Tech.)

Ana Olmos (Capítulo Español de ISOC (ISOC-ES))

Gorka Orueta (Universidad del País Vasco)

Lorena Rivera (Investigadora colaboradora/Syntagma)

Javier Seriñá Martínez (Public Policy and Internet, Telefónica)

Para la elaboración de este documento se ha seguido también de cerca el trabajo realizado por la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en el GAC de ICANN. Estamos agradecidos, en concreto, a Gema María Campillos y Rafael Pérez Galindo, de cuyo conocimiento y trabajo hemos aprendido y a quienes reconocemos el compromiso con el Foro de la Gobernanza de Internet y una importante contribución a los procesos que afectan a la gestión de los recursos críticos.

2 | 1 Supervisión de los recursos críticos

La red global, en su consideración como sistema de información global, depende del buen funcionamiento y eficacia de una larga cadena de sistemas, tecnologías, aplicaciones e infraestructuras. Entre ellos, es necesario el funcionamiento de unos pocos recursos, incluyendo la coordinación de la asignación de los parámetros técnicos de los protocolos de Internet, la administración de ciertas responsabilidades asociadas con la zona raíz de la gestión del DNS y la asignación de los recursos de numeración de Internet. Un conjunto limitado de identificadores únicos es el nexo que mantiene unida a una Internet global y única.

La gestión de estos recursos fue delegada por el Gobierno de los Estados Unidos a una organización privada, ICANN, a finales de los años 90. La supervisión vestigial de dicho Gobierno ha causado gran controversia en los debates de gobernanza de Internet. La presión internacional que desde hace años intenta forzar una mayor internacionalización en esta gestión ha adquirido mayor intensidad tras las revelaciones de Snowden.

Finalmente, en 2014, y coincidiendo con una etapa en la que ICANN ha intensificado sus procesos de apertura, Estados Unidos anunció la intención de renunciar a dicha supervisión, siempre y cuando se encontrara un mecanismo multistakeholder adecuado que sirviera de reemplazo.

Dos grandes hitos que se debaten en estos instantes, con gran valor simbólico y múltiples escenarios posibles, son la transición de IANA y la rendición de cuentas de ICANN.

Desde 2005 la comunidad internacional ha ido evolucionando su postura hacia una mayor exigencia a ver cambios en el control de los recursos críticos. A raíz de arduos debates en la Cumbre Mundial de la Sociedad de la Información se formó el Foro de la Gobernanza de Internet, que proporcionaba un lugar para que la comunidad multistakeholder global pudiera debatir la regulación y políticas que afectan a los recursos críticos de Internet, así como otras muchas cuestiones que se agrupan bajo el concepto de “gobernanza de Internet”.

En 2010 y 2011 hubo muchas controversias alrededor del programa de nuevos dominios genéricos de alto nivel (gTLD, por sus siglas en inglés) y la controversia sobre el dominio .xxx llevó a algunos gobiernos a argumentar a favor de una mayor influencia gubernamental en los procesos de desarrollo de políticas de ICANN. La mayoría de los gobiernos de los países occidentales, aun cuando algunas voces defienden la necesidad de un rol más significativo del Comité Asesor Gubernamental (GAC, por sus siglas en inglés), apoyan el modelo multistakeholder actual de ICANN para el gobierno del sistema de nombres de dominio (DNS, por sus siglas en inglés). Otros países, tales como Brasil, Suráfrica e India, apoyaban la creación de una entidad circunscrita a Naciones Unidas, cuya misión incluyera integrar y supervisar organizaciones encargadas del funcionamiento técnico y operativo de Internet (como ICANN). Un tercer grupo de países, incluyendo Rusia y China, proponían un “código de conducta internacional para la seguridad de la información”, código en el que se intuye el establecimiento de una gestión internacional, multilateral, transparente y democrática de Internet.

Alrededor de la Conferencia Mundial de Telecomunicaciones Internacionales se generó mucho debate y tensión. Aprovechando la necesidad de actualizar el Reglamento de Telecomunicaciones Internacionales (ITR, por sus siglas en inglés), se presentó una propuesta apoyada por Rusia, China, Arabia Saudí y Sudán que pedían explícitamente ampliar la jurisdicción de dicho Reglamento sobre el tráfico de Internet, su infraestructura y su gobernanza. El debate se avivó y se generaron muchas expectativas para los siguientes encuentros internacionales tratando diferentes cuestiones relacionadas.

En octubre de 2013, un conjunto de organizaciones involucradas en la coordinación de la infraestructura técnica global de Internet, incluyendo ICANN, emitieron un comunicado pidiendo fortalecer los mecanismos actuales para la cooperación multistakeholder en Internet, incluyendo expresamente la petición de acelerar la globalización de las funciones de ICANN e IANA. Esta idea volvió a reforzarse en NetMundial en Brasil en 2014.

2 | 2 Traspaso de las funciones IANA

El rol de ICANN incluye la coordinación de los recursos críticos de Internet, el DNS y el direccionamiento IP ("Internet Protocol") y el registro de parámetros de protocolo. Además de la dimensión política en la gestión de los dominios de alto nivel genéricos, ICANN también es responsable de gestionar y actualizar la zona raíz del DNS, esto es, las funciones IANA.

La gestión de IANA está divida entre ICANN, que coordina las políticas y los aspectos administrativos, y Verisign, que gestiona la base de datos de forma separada y en virtud de un contrato aparte con el Gobierno de Estados Unidos.

ICANN siempre ha tenido una relación regulada con el Gobierno de Estados Unidos, aunque este último siempre ha sido claro en su propósito de retirarse de su posición como autoridad de supervisión una vez que el modelo ICANN estuviera "establecido y estable". A pesar de esta declaración de intenciones, la relación entre la organización y el Gobierno se ha mantenido a lo largo de los años y a través de diferentes fórmulas. La Afirmación de Compromisos, efectiva desde 2009, es la tercera iteración de la relación entre ICANN y Estados Unidos, en concreto, el Departamento de Comercio. Uno de sus elementos centrales es el requisito de que ICANN se someta a revisiones regulares sobre sus operaciones y su gestión. El contrato actual que regula las funciones IANA fue adjudicado en 2012 y expira en 2015 (renovable un periodo de cuatro años), siendo las partes ICANN y el Departamento de Comercio de Estados Unidos y el objeto la gestión operativa de la base de datos IANA.

A través de este contrato, el Gobierno de Estados Unidos tiene la autoridad última sobre las funciones IANA y, en consecuencia, sobre el sistema de navegación en Internet. El simbolismo de que un solo gobierno controle uno de los pocos puntos críticos de Internet ha encubierto el hecho de que IANA funciona bien. El Gobierno de Estados Unidos ha mostrado prudencia en su función supervisora y ejercido una labor principalmente administrativa. Sin embargo, la presión internacional y la reacción airada de la comunidad internacional ante los excesos del Gobierno de Estados Unidos en cuestiones de vigilancia internacional han creado un clima difícil de sostener.

En marzo de 2014, poco antes del encuentro NETmundial en Brasil, la Administración Nacional de Telecomunicaciones e Información (NTIA, por sus siglas en inglés) del Gobierno de Estados Unidos anunció su intención de iniciar la transición de las funciones clave en el sistema de nombres de dominio a la comunidad global multistakeholder, esto es, que incluya a múltiples partes interesadas (reuniendo a gobiernos, sector privado, sociedad civil y comunidad científico-técnica), en virtud del contrato que expira el 30 de septiembre de 2015. En su anuncio, se solicita a ICANN que desarrolle una propuesta de transición que satisfaga cuatro principios:

- Que apoye y realce el modelo multistakeholder.
- Que mantenga la seguridad, estabilidad y resiliencia del sistema de nombres de dominio en Internet.
- Que satisfaga las necesidades y expectativas de los clientes y socios globales de los servicios IANA.
- Que mantenga la apertura de Internet.

El Gobierno de Estados Unidos no ha definido un modelo de sucesión. Este ejercicio, que recae ahora sobre la comunidad multistakeholder internacional, sirve de examen para poner a prueba el modelo multistakeholder y la capacidad de esta comunidad para organizarse y alcanzar un consenso.

En este sentido, el encuentro NETmundial de abril de 2014 fue un ejemplo de procesos multistakeholder capaces de entregar resultados sobre una base de consenso y en un tiempo oportuno, elevando los niveles de confianza sobre una posible resolución satisfactoria.

Algunas voces argumentan desde hace tiempo que el rol del Gobierno de Estados Unidos debía transferirse a un modelo multilateral, en el que actuasen todos los gobiernos sobre un recurso global; en resumen, sustituir un gobierno por todos los gobiernos. Esta postura tiene cierta lógica, teniendo en cuenta la legitimidad inherente de los gobiernos soberanos para supervisar recursos globales y proteger el interés público.

Esto, a su vez, genera tensiones internas en Estados Unidos por el temor a que la salida de la NTIA provoque una captura de ICANN o de las funciones IANA por la ONU/UIT o gobiernos no afines. En esta línea, se esgrimen argumentos que apuntan a un posible riesgo de politización de los recursos críticos de Internet o una vía para limitar la libertad de los usuarios en Internet o poner en peligro los intereses de la industria norteamericana. De hecho, el Gobierno de Estados Unidos ha anunciado que no aceptará una propuesta de transición que reemplace a la NTIA con una solución liderada por gobiernos o intergubernamental.

Por otro lado, difícilmente se puede ignorar el rol de otros actores, como la comunidad científico-técnica y la sociedad civil, en la construcción de Internet tal y como lo conocemos; su participación y contribuciones han sido elementos claramente distintivos de su evolución y constituyen una de las claves del éxito del crecimiento de Internet y la innovación en la red. Las formas de trabajo que caracterizaron la construcción técnica de Internet son mucho más ágiles y eficientes, además de ligados a la realidad operacional, de lo que nos tienen acostumbrados los procesos de negociación intergubernamentales.

Desde el nacimiento del Foro de la Gobernanza de Internet se ha hablado largo y tendido sobre esta comunidad multistakeholder y cómo las múltiples partes interesadas se complementan y construyen nuevos procesos y modelos de trabajo más afines con un recurso que es global y tiene impacto a todos los niveles: político, económico y social.

Por otro lado, las debilidades del proceso multistakeholder, como pueden serlo las cuestiones de legitimidad, los costes de participación, el liderazgo del sector privado (que dispone de más recursos) y de la sociedad de los países desarrollados, ponen de manifiesto que los procesos abiertos no garantizan una participación equitativa y justa para todos los afectados por las decisiones en el ámbito de los recursos críticos de Internet.

El 8 de abril de 2014, ICANN lanzó el proceso multistakeholder para acordar una propuesta que elevar a la NTIA. Se creó un IANA Stewarship Transition Coordination Group (ICG) formado por miembros de todos los grupos de interés representados en ICANN, para remitir una propuesta a ICANN, quien, a su vez y sin poder vetarla o modificarla, la elevará a la NTIA para su aprobación. El 15 de junio de 2015 sería la fecha límite para elevar la propuesta de consenso a la NTIA.

Las tres comunidades operacionales (clientes de IANA) han recibido el encargo de elaborar propuestas en su ámbito. Según lo previsto, tanto las comunidades de protocolos (IETF) como la de números (Regional Internet Registries, RIR) han presentado una propuesta al ICG. Para ambas, no ha sido un ejercicio complicado puesto que las estructuras contractuales y de control ya eran externas a ICANN.

Más difícil ha sido de articular la propuesta que debe realizar la comunidad de nombres, que agrupa a grupos muy diferentes: industria de dominios, registros, registradores, gobiernos. Éstos, además, se ocupan de recursos de diferente naturaleza, pues el tratamiento otorgado a los nombres genéricos (gTLD) y a nombres de país (ccTLD) debe ser diferente, dependiendo éstos últimos, en última instancia, de la legislación nacional. Tras varios intentos, la comunidad de nombres elevará su propuesta definitiva al ICG, previsiblemente en junio de 2015.

Una de las cuestiones que más se ha debatido es si debería crearse una nueva organización o entidad para supervisar el contrato de las funciones IANA (modelo externo) o si el propio ICANN (sujeto a medidas de rendición de cuentas mejoradas) debería asumir la autoridad sobre IANA (modelo interno).

En el modelo externo, la nueva entidad sustituiría el rol de la NTIA. Esta nueva entidad, que podría ser, por ejemplo, una organización sin ánimo de lucro o un consorcio, integrado y liderado por la comunidad multistakeholder, contrataría las funciones IANA a ICANN, quien bajo dicho contrato continuaría ejecutando esta labor operativa. La entidad externa renovaría el contrato periódicamente y tendría la opción de asignar las funciones IANA a otro operador si el desempeño de ICANN no se considerara satisfactorio.

En el modelo interno, la NTIA transferiría su autoridad sobre las funciones IANA a la propia ICANN. En este caso, ICANN tendría la autoridad sobre estas funciones y al mismo tiempo continuaría siendo el operador. Para ello, tendría que haber mecanismos de mejora de rendición de cuentos que permitieran a la comunidad multistakeholder exigir a ICANN la transferencia de la autoridad a otra entidad, si fuera necesario.

En caso de no cumplirse el plazo previsto, la NTIA ha anunciado que podría prorrogar el contrato actual para dar más tiempo a la comunidad de presentar su propuesta.

2 | 3 Rendición de cuentas de ICANN

La misión central de ICANN es coordinar, en un nivel general, los sistemas mundiales de Internet de identificadores únicos y, especialmente, asegurar el funcionamiento estable y seguro de esos identificadores únicos. Básicamente, ésta es una función de coordinación técnica pero de importancia fundamental para la estabilidad y el funcionamiento interno de Internet.

ICANN funciona con un modelo de múltiples partes interesadas que se reúnen para tratar cuestiones normativas incluidas entre las áreas de responsabilidad de ICANN. Dicho modelo sigue un patrón de elaboración de normas de abajo hacia arriba y se basa en el consenso de sus partes interesadas. Para que este modelo funcione eficazmente, ICANN necesita alentar la participación, infundir confianza, facilitar el acceso a la información y contar con sólidos mecanismos de análisis y disputa.

Según se estipula en los estatutos de ICANN: “ICANN y sus órganos constitutivos deben operar de la manera más abierta y transparente que sea posible, de acuerdo con los procedimientos trazados para asegurar la imparcialidad”. Para la mejora de rendición de cuentas de ICANN es necesario un análisis de cuáles serán los nuevos o mejores mecanismos necesarios ante la ausencia de la relación contractual histórica de ICANN con el Gobierno de Estados Unidos.

La Afirmación de Compromisos exige que cada tres años se realice una revisión de la transparencia y rendición de cuentas (“accountability”) de ICANN. Gracias a lo aprendido en este proceso, así como la implicación de la comunidad multistakeholder en el debate, se ha llegado a entender relativamente bien cuáles son las cuestiones críticas, lo que no significa que se hayan identificado las soluciones adecuadas.

Algunas de las debilidades identificadas tienen que ver con la Junta Directiva ("Board") de ICANN, el rol de los gobiernos y la influencia de la industria de nombres de dominio. El fuerte compromiso de ICANN con la transparencia, en principio un elemento clave para ganarse la confianza de la comunidad internacional, resulta a veces en una sobredosis de información que resulta difícil de digerir para los que tienen interés por seguir los procesos y contribuir a las políticas.

La desvinculación de ICANN del gobierno de los EE.UU. y su globalización podría pasar por:

- Su constitución conforme a otro status jurídico propio del Derecho Internacional.
- La resolución del contrato actual (Afirmación de Compromisos) y su novación en un verdadero acuerdo internacional.
- Reforzar los mecanismos de legitimidad, transparencia y rendición de cuentas.
- Promover la participación de más partes interesadas, incluyendo a sectores y regiones mundiales que están infrarrepresentadas en ICANN.
- La aceptación institucional, internacional, consensuada y generalizada de compromisos éticos para el ciberespacio a través de mecanismos de derecho internacional.

ICANN ha constituido un grupo de trabajo multisectorial ("Cross-Community Working Group on Enhancing ICANN Accountability" o abreviado, "CCWG") cuyo objetivo es mejorar los mecanismos de rendición de cuentas de ICANN. Este grupo estudiará, en primer término, los instrumentos de control más ligados al ejercicio de las funciones IANA, pues éstos deben estar en pie cuando se efectúe el traspaso. Posteriormente, analizará otros aspectos de la responsabilidad de ICANN no relacionados con las funciones IANA y que puedan esperar. Sus propuestas se elevarán a la Junta Directiva, que puede rechazarlas por una mayoría de 2/3 si cree que refuerzan adecuadamente la responsabilidad de la organización.

La pertenencia al CCWG está abierta a individuos designados por las diferentes organizaciones que representan a las diferentes organizaciones de la comunidad ICANN. Las decisiones se toman por consenso. Además, el CCWG está abierto a cualquier persona interesada en participar.
Los participantes podrán asistir y contribuir en todas las reuniones, pero su voto no contará para el consenso ni participarán en la toma de decisiones.

Además, un grupo de hasta siete asesores, seleccionados por un Grupo de Expertos Público, podrán aportar consejo independiente e investigación, así como identificar mejores prácticas. Otros miembros del CCWG incluyen a un miembro del personal de ICANN, un miembro de un equipo haya ejecutado alguna de las revisiones de rendición de cuentas y transparencia, un enlace con el ICG y un enlace con la Junta Directiva de ICANN. Todos estos individuos participan pero no forman parte del proceso de toma de decisiones.

Inicialmente concebidos como dos procesos independientes, lo cierto es que la mejora de rendición de cuentas de ICANN es fundamental para el éxito de la transición de la custodia de las funciones IANA.

El riesgo de combinar ambos procesos es que acaben requiriendo una reorganización de tal magnitud que no se llegue a alcanzar el nivel necesario para su realización en años. Al mismo tiempo, para muchos es una oportunidad para poner sobre la mesa ciertas cuestiones relacionadas con la rendición de cuentas que, ligándolas a la transición delas funciones IANA, pueden resultar más fácil de negociar que fuera de este contexto.

2 | 4 Observaciones

Finalmente, el debate de la transición de IANA se reducirá a la propuesta definitiva de transición que la comunidad multistakeholder entregue a la NTIA. Ahora mismo se plantea la duda de si realmente será posible efectuar la transición de IANA el 30 de septiembre de 2015 (la NTIA ha anunciado flexibilidad para continuar la situación actual en caso de necesidad).

El futuro de cómo ICANN y el DNS serán gestionados y supervisados es muy relevante para la cuestión más general sobre cómo Internet debería ser gobernado. Aunque es verdad que la jurisdicción de ICANN está limitada a la gestión técnica de internet (identificadores únicos tales como nombres de dominio y direcciones), también es verdad que las decisiones políticas de ICANN (tales como la expansión de nombres de dominio genéricos o gTLD) puede tener un impacto en otras áreas como la propiedad intelectual, la ciberseguridad, la privacidad y la libertad en Internet.

A medida que Internet crece y se hace más presente en todos los aspectos de la sociedad moderna, la cuestión sobre cómo debería ser gobernado se hace más acuciante, con gobiernos reconociendo un valor cada vez más alto en las decisiones que toma ICANN, especialmente en aquellos casos en los que la política de DNS intersecta con leyes nacionales y otros intereses.

Este proceso puede tener un profundo impacto y constituir un precedente para futuros debates de políticas públicas y gobernanza de Internet y qué roles deberían tener cada una de las partes interesadas, incluyendo gobiernos, sector privado, sociedad civil y comunidad científico-técnica.

Fuentes consultadas

ICANN (2015). www.icann.org

Internet Governance Project (2015). www.internetgovernance.org.

Kruger, L. G. (2014). Internet domain Names: Background and Policy Issues. Congressional Research Service.

Kruger, L. G. (2015). The Future of Internet Governance: Should the U.S. Relinquish Its Authority Over ICANN? Congressional Research Service.

Taylor, E. (2015). ICANN: Bridging the Trust Gap. Global Commission on Internet Governance.

Capítulo 3

Regulación y ciberseguridad
Contribuciones al modelo de Gobernanza

Coordinación: **Manuel Carpio Cámara**

Editores/Autores: **Manuel Carpio Cámara, Ángel León, Jesus Cano Carrillo, Carlos E. Jiménez**

Grupo de Trabajo:

Gema Campillos González (Subdirectora General de Servicios de la Sociedad de la Información, Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información)

Jesús Cano Carrillo (Secretario/IEEE e-Government Computer Society)

Manuel Carpio Cámara (Director de Seguridad de la Información y Prevención del Fraude/ Telefónica)

María de Miguel De Santos (Consejera Técnica, Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información)

Francisco Falcone (Profesor/Universidad Pública de Navarra)

Carlos Galán (Profesor de Derecho de las TIC/Universidad Carlos III de Madrid)

Javier Pérez (Consejo General de Colegios Profesionales de Ingeniería Informática – CCII)

Carlos E. Jiménez Gómez (Presidente/IEEE e-Government)

Ángel León (Vocal Asesor, Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información)

Paloma Llaneza (Abogada, Socia Directora/Razona Legal Tech.)

Francisco Pérez (Secretario General/Incibe)
Miguel Rego (Director General. CEO/Incibe)

Javier Seriña Ramirez (Jefe de Política de Comunicaciones Públicas/Telefónica)

Alberto Urueña (Responsable de Estudios del Observatorio de la Sociedad de la Información de RED.es/Red.es)

3 | 1 Situación de partida

3 | 1 | 1 Situación de la ciberseguridad en España

En el análisis de la situación de la ciberseguridad en España debe considerarse por una parte el punto de vista de los usuarios finales y del gran público, y por otra parte el de las grandes empresas y administraciones públicas, caracterizándose 2014 desde ambas perspectivas por un elevado número de incidentes y una preocupación creciente por la ciberseguridad para empresas y ciudadanos.

En el primero de estos ámbitos es significativo el estudio realizado por Red.es (www.red.es) y el Instituto Nacional de Ciberseguridad de España (INCIBE, www.incibe.es) relativo a la adopción de medidas de seguridad y las situaciones que pueden constituir riesgos de seguridad, así como el grado de confianza que los hogares españoles depositan en el uso de las nuevas tecnologías de la información.

El objetivo del estudio es el análisis del estado de ciberseguridad de los hogares españoles[1] a través de indicadores basados en la percepción de los usuarios sobre la misma, así como el nivel de confianza de estos respecto a la seguridad y su evolución, haciendo un contraste comparativo con el nivel real de seguridad que mantienen los equipos informáticos. Se pretende impulsar el conocimiento y seguimiento de los principales indicadores y políticas públicas relacionadas con la seguridad de la información y la e-confianza. Así, el informe tiene como finalidad, entre otras, informar del comportamiento y utilización segura y privada de las nuevas tecnologías mediante los consejos y enlaces de la Oficina de Seguridad del Internauta (OSI, www.osi.es) de INCIBE, además de servir como apoyo para la resolución de los eventuales incidentes que pudieran producirse, por parte de los usuarios y adopción de medidas por parte de la Administración.

El estudio se realiza a través de dos vías: el análisis de las declaraciones aportadas por los internautas encuestados y el contraste de dicha información con el análisis de seguridad real de los equipos informáticos mediante el escaneo de dichos terminales mediante la herramienta iScan, desarrollada por INCIBE.

[1]Se han publicado tres oleadas en los años 2014 y 2015 disponibles en: http://www.ontsi.red.es/ontsi/es/estudios-informes/ciberseguridad-y-confianza-en-los-hogares-espa%C3%B1oles-febrero-2015

En lo que se refiere a empresas y administraciones públicas, el año 2014 se ha caracterizado por la especial virulencia en los ataques contra la seguridad de sus sistemas de las Tecnologías de la Información y las Comunicaciones (TIC). Los incidentes de gran envergadura se han venido sucediendo, mes a mes, en un intento continuo, por parte de los atacantes, de apropiarse de información valiosa o sensible desde los puntos de vista político, estratégico, de seguridad o económico. Es lo que hemos venido denominando como acciones de ciberespionaje.

También la ciberdelincuencia, con nuevos modelos de negocio como el Crimen como Servicio; el hacktivismo, con intenciones más modestas, pero que también pueden poner en peligro la prestación de servicios y el normal funcionamiento de las organizaciones; o el ciberterrorismo y la ciberguerra, como potenciales amenazas, han hecho acto de presencia en un año en el que España también ha sido víctima de ciberataques de todo tipo.

Adentrarse en este panorama, sus orígenes, desarrollo y consecuencias e, incluso, vislumbrar las tendencias para los próximos meses en materia de ciberseguridad son los objetivos del Informe[2] de Ciberamenazas 2014 y Tendencias 2015 (CCN-CERT IA-9/15) elaborado por el CCN-CERT, del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI).

En su elaboración se ha utilizado la experiencia de este CERT Gubernamental además de otras fuentes documentales, nacionales e internacionales, públicas y privadas.

Por otro lado, según los datos del CERT-SI[3], CERT de Seguridad e Industria operado por INCIBE y el CNPIC, los incidentes en el ámbito de los operadores estratégicos e infraestructuras críticas tienen una componente más de calidad que de cantidad, entendiéndose por ésta que los ataques realizados a estos sectores no tienen tanta importancia por su número como por su objetivo y sofisticación.

Hábitos de comportamiento en la navegación y usos de Internet

El comportamiento y los hábitos de seguridad adoptados por los usuarios españoles cuando acceden a Internet son indicativos del nivel de precaución ante los peligros que se pueden encontrar en el mundo digital.

En este apartado se analizan algunos de esos comportamientos y hábitos referentes a los usuarios; y con respecto a los menores de edad se persigue informar del comportamiento y utilización segura y privada de las nuevas tecnologías mediante los consejos y enlaces de la Oficina de Seguridad del Internauta (OSI) de INCIBE.

[2]https://www.ccn-cert.cni.es/index.php?option=com_docmanpriv&task=doc_download&gid=303&Itemid=168&lang=es

[3]https://www.incibe.es/CERT/Infraestructuras_Criticas/

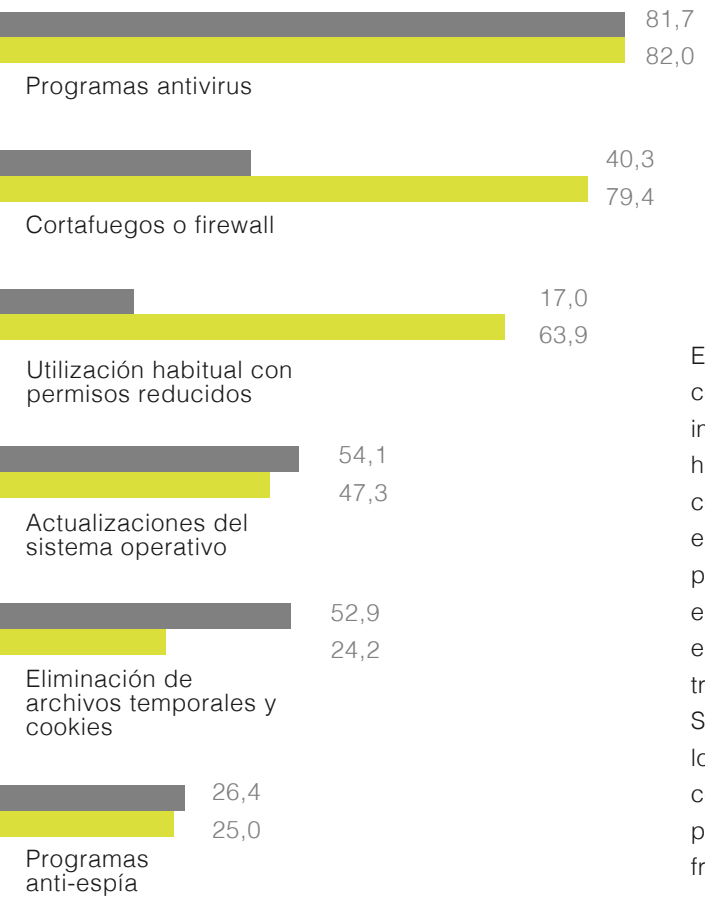


FIGURA 1: Uso declarado vs. real de medidas de seguridad (%) Fuente: Panel hogares, INCIBE, ONTSI

[4]Se denomina malware a todos aquellos programas y códigos maliciosos o malintencionados cuyo objetivo es infiltrarse en un equipo informático sin el consentimiento del propietario. Comúnmente se conocen como virus, en realidad se trata de un término más amplio que engloba otras tipologías.

El 40,6% de los internautas afirman que, de manera consciente y de forma puntual, adoptan conductas que implican un riesgo de seguridad mientras navegan o hacen uso de los servicios de Internet. No obstante, en el contexto de los servicios de la banca en línea y el comercio electrónico, la mayoría de usuarios se muestran más prudentes y aplican buenos hábitos en su uso. Así ocurre, en general, para más del 73% de los internautas, aunque el uso de tarjetas prepago o monedero para hacer pagos a través de la Red es utilizado por solo 2 de cada 5 usuarios. Sin embargo se trata de una buena medida que evita que los datos reales de las tarjetas bancarias puedan verse comprometidos y, al tener un saldo limitado, minimiza el posible impacto económico en caso de ser víctima de un fraude a la hora de realizar un pago a través de la Red.

Medidas de seguridad

Las principales medidas de seguridad implantadas, según su uso real detectado por iScan, son el software antivirus (82%) y el cortafuegos (79,4%). No obstante, este último dato se debe principalmente a la inclusión de dichas soluciones firewall en los sistemas operativos, por lo que su existencia pasa desapercibida para un gran número de usuarios (el uso declarado se encuentra 39 puntos porcentuales por debajo del uso real).

Incidentes de seguridad

La incidencia percibida principalmente por el usuario es el spam, o correo electrónico no deseado, tanto en el equipo informático del hogar (85,3%) como en dispositivos móviles y smartphones (76,6%).

Las incidencias relacionadas con el malware[4] (31,7%) en el ordenador personal ocupan un segundo lugar, y son meramente presenciales en smartphones, con un porcentaje del 7,1%. Sucede al contrario que con el spam, es decir, el objetivo del malware es principalmente pasar desapercibido, evitando ser detectado tanto por el software antivirus como por el usuario.

Aproximadamente el 21% de los usuarios entrevistados declaran haber detectado malware alojado en sus ordenadores. Esto supone un mínimo con respecto a declaraciones de anteriores oleadas. Sin embargo el análisis real que la herramienta iScan lleva a cabo en los ordenadores detecta una cantidad de infecciones bastante superior: casi un 59%.

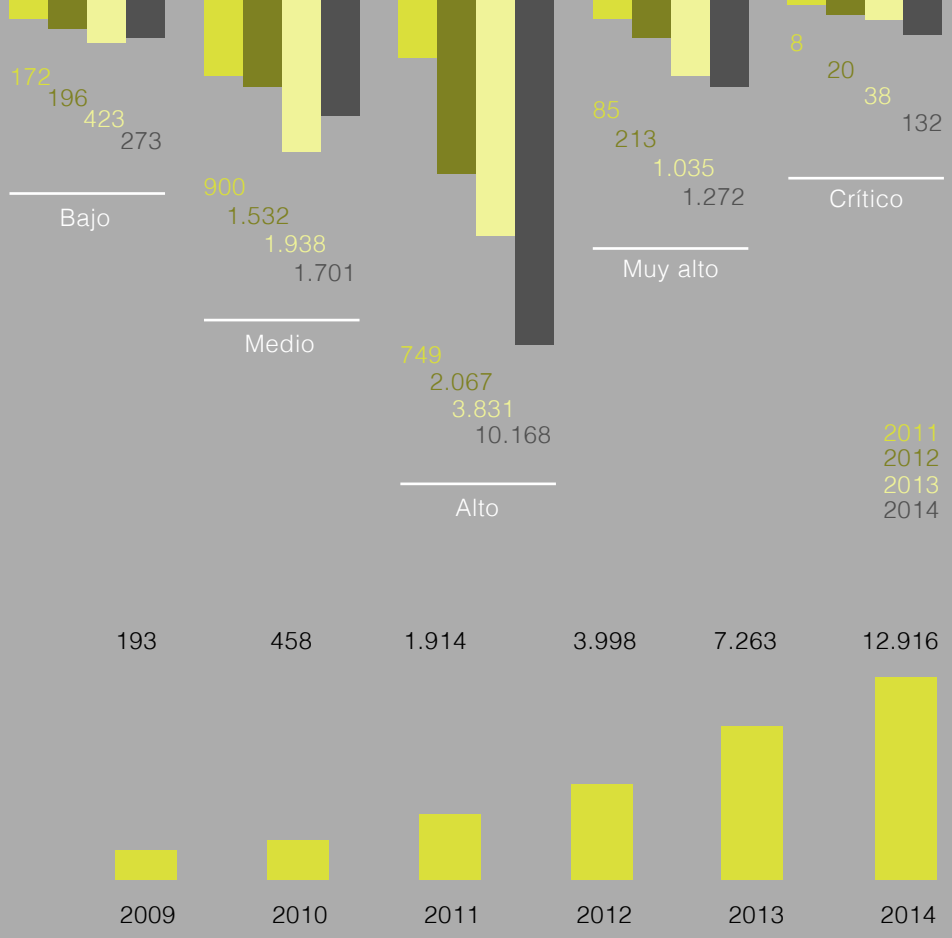


FIGURA 4. Incidentes gestionados por el CCN-CERT (en número y criticidad).
Fuente: Informe CCN-CERT IA-09/15. CIBERAMENAZAS 2014 TENDENCIAS 2015

Subclasificación general	Clasificación	Nº incidentes
Troyano	Código Dañino	9.371
Explotación de vulnerabilidades	Intrusión	833
Inyección SQL	Intrusión	460
Inyección de Ficheros Remota	Intrusión	460
Gusano	Código Dañino	459
Spyware	Código Dañino	258

Tabla 1: Principales subcategorías de incidentes gestionados en 2014 por el CCN-CERT

Al analizar la tipología del malware detectado con la herramienta iScan en los ordenadores de los usuarios, se observa que los principales tipos de software malicioso son los que intentan reportar un beneficio económico a sus creadores. Así destacan los troyanos (37,9%) y el adware publicitario (35,1%). Esto revela cuales son los motivos principales para evitar ser detectados, ya que si el malware logra pasar desapercibido tiene muchas posibilidades de reportar beneficios al desarrollador.

Atendiendo los datos recabados por el CCN-CERT, 2014 ha sido un año especialmente significativo en materia de ciberamenazas en el que se han atendido un número creciente de incidentes, con especial importancia del ciberespionaje y APTs[5], código dañino y ransomware[6].

También el CERT-SI confirma estas tendencias, habiendo gestionado más de 80 incidentes cibernéticos en los diferentes sectores de las infraestructuras estratégicas, cuya tipología se centra en primer lugar en el malware avanzado (49,2%), robo de información (14,3%) seguidos de otro tipo de amenazas, como el fraude, la denegación de servicio o los accesos no autorizados.

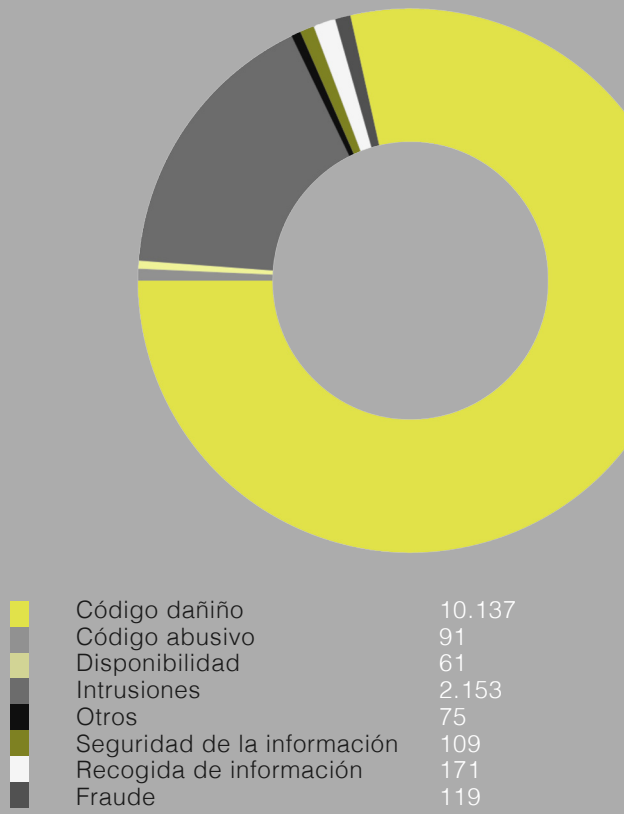


FIGURA 5. Principales subcategorías de incidentes gestionados en 2014

[5]APT – Advanced Persisten Threat

[6]Tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y tiene como objetivo bloquear el uso del ordenador o parte de la información que contiene y pide un rescate a cambio de quitar esta restricción

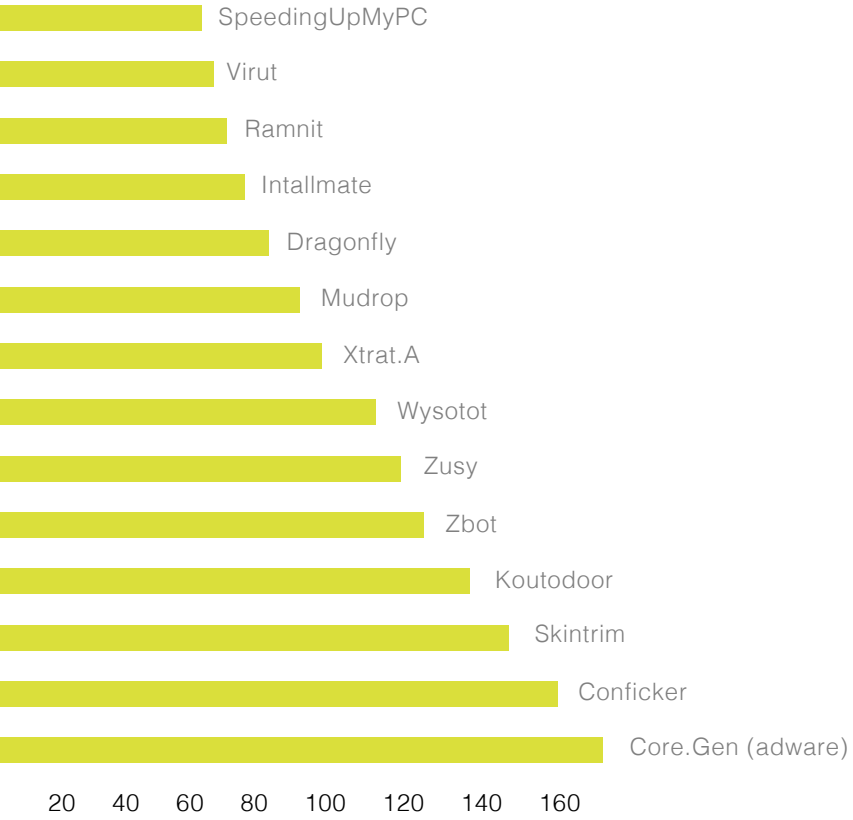


FIGURA 6. Código dañino más detectado por el CCN-CERT

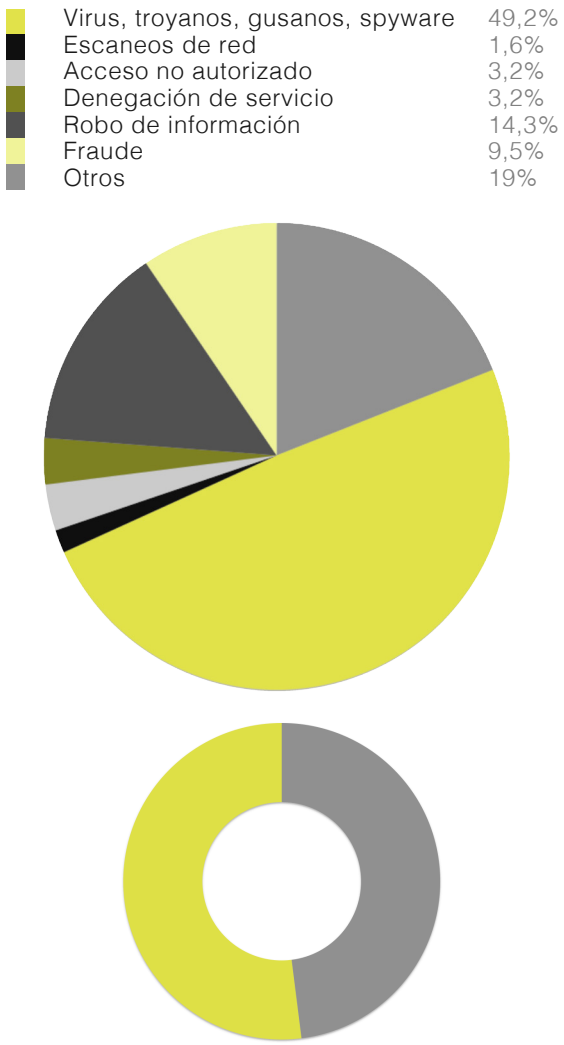


FIGURA 7: Tipologías de ataques sobre infraestructuras estratégicas. CERT-SI (INCIBE y CNPIC)

Consecuencias de los incidentes de seguridad y reacción de los usuarios

A partir de las incidencias de seguridad acontecidas, se concretan cuáles son las consecuencias derivadas de ellas, así como las reacciones de los usuarios y las medidas de seguridad y hábitos prudentes adoptados y/o modificados con el propósito de evitar que vuelvan a producirse.

Casi la mitad (48%) de los internautas entrevistados responden afirmativamente ante la pregunta de haberse vistos involucrados en algún tipo de situación de fraude a través de Internet. Sin embargo sólo el 21,1% manifiesta haber sufrido alguna situación de fraude telefónico[7].

Al analizar las formas con que las incidencias de intento de fraude se realizan se puede concluir que la invitación a visitar alguna página web sospechosa (57,3%) es la más común. En la mitad de las ocasiones (50,1%) el intento de fraude llega al usuario bajo la forma de un ofrecimiento de servicios no solicitados y, aprovechando la situación actual, el 44,7% se presenta como una oferta de trabajo falsa o sospechosa.

[7]Este dato incluye las llamadas y SMS fraudulentos, suscripciones indeseadas a servicios o aplicaciones móviles e incitaciones a visitar páginas Web sospechosas

La forma menos percibida, con menos del 11% de las declaraciones entre aquellos usuarios que han sufrido un intento de fraude, son las páginas web falsas (phishing[8]) de entidades bancarias, comercios online o administraciones.

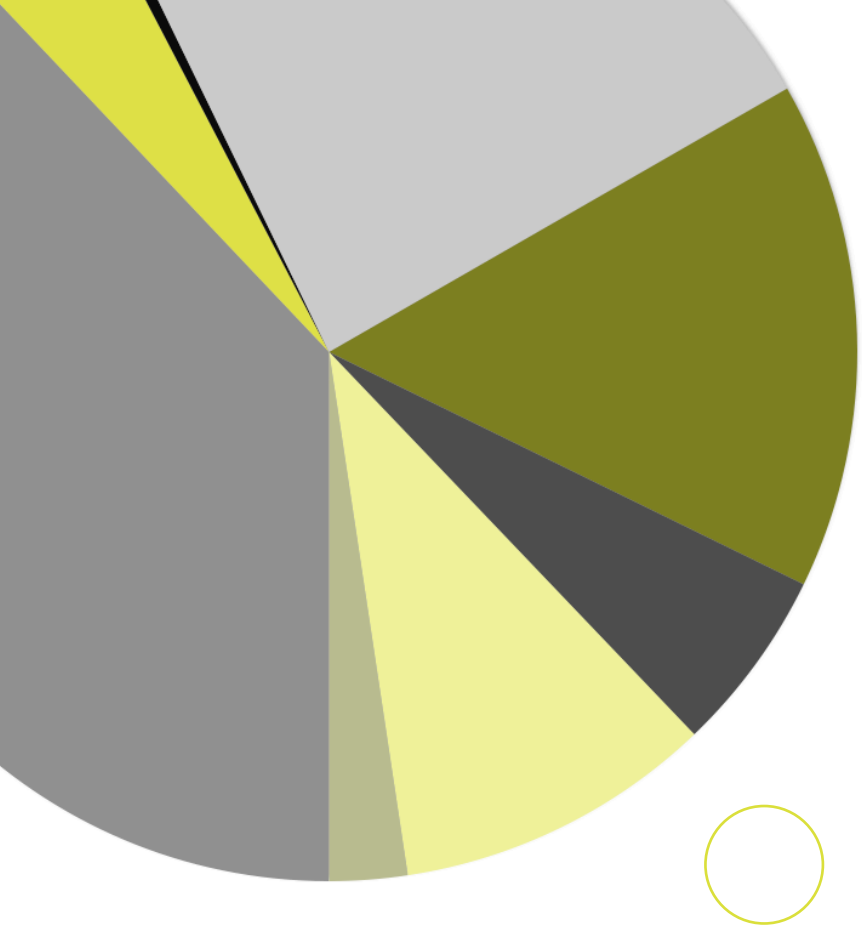
También resulta interesante analizar en cada caso cuál es la forma adoptada por el remitente de la comunicación sospechosa de ser fraudulenta. Así se obtiene que la principal forma es la de entidad bancaria cuando se trata de solicitar claves de usuario (54,3%) y de páginas web falsas (phishing) de entidades bancarias, comercio electrónico, etc. (63,1%). Añadido a lo anterior, los atacantes suelen suplantar a entidades de comercio electrónico para ofertar servicios no solicitados (37,2%), y productos desde páginas falsas (39,8%).

Por último INCIBE también publica en su Informe Anual de Actividad del 2014 que resolvió más de 17.800 incidentes de ciberseguridad de los cuales encabezan la lista de los más prolíficos los accesos no autorizados (con casi un 38%), las distintas modalidades de fraude electrónico (23,90%) y finalmente las infecciones por malware (9,76%). Este organismo ha atendido casi 8.000 llamadas a través de su servicio de atención al internauta en ciberseguridad de la OSI (901 111 121) y detectó más de 161.900 direcciones IP con indicios de actividad maliciosa. Finalmente INCIBE realizó más de 20.500 notificaciones a ISPs, empresas y operadores de infraestructuras estratégicas o críticas durante el 2014[9].

[8]Phishing: ataques en los que se trata de engañar a los usuarios mediante correos electrónicos o páginas web falsas.

[9]https://www.incibe.es/extfrontinteco/img/File/actividad_2014.pdf

FIGURA 8. Consecuencias y reacciones de los usuarios.
Fuente: Panel hogares, INCIBE, ONTSI



Acceso no autorizado	37,94%
Denegación de servicio	4,41%
Robo de información	0,45%
Fraude	23,9%
Otros	15,55%
Spam	5,62%
Virus, troyanos, gusanos, spyware	9,76%
Escaneos de red	2,38%

FIGURA 9. Incidentes gestionados por INCIBE

Confianza en el ámbito digital en los hogares españoles

De forma general, los servicios físicos inspiran en el usuario más confianza que los servicios digitales homólogos. En este sentido, la mayor brecha entre el servicio físico y el online se observa en las operaciones bancarias (casi un 18%). Sin embargo, a la hora de realizar pagos, el internauta español deposita casi tanta confianza en el pago online utilizando intermediarios como PayPal (43%), como en el uso de una tarjeta de crédito/débito en un establecimiento público (43,4%).

El internauta español percibe dos riesgos determinados al hacer uso de Internet.
El principal, declarado por el 43% de los encuestados, es ver comprometida su privacidad, a través del robo y uso de información de carácter personal (nombre, dirección, fotografías, etc.) sin consentimiento ni conocimiento del propio usuario.

El segundo de los riesgos es el perjuicio económico derivado de un intento de fraude a través de Internet, declarado por el 37,8%.

Ser consciente de la repercusión que las acciones propias tienen sobre la seguridad en Internet, puede influir en un aumento de hábitos prudentes, uso de medidas de seguridad, disminución de conductas de riesgo y, por tanto, una disminución de incidencias de seguridad.
El 36,8% de los internautas españoles son conscientes de que la responsabilidad de la seguridad en Internet recae sobre ellos mismos. Otro tercio de la población (32,9%) opina que, por el contrario, esta responsabilidad corresponde a las Administraciones Públicas.

Un 45,3% de internautas manifiesta tener mucha o bastante confianza en Internet. La Red inspira poca confianza para el 11,3% de la población española mientras que el 1,4% afirma no tener ninguna confianza en ella.

3 | 1 | 2 Eventos significativos relacionados con la ciberseguridad

Como así han señalado distintas fuentes[10], 2014 ha sido un año singularmente significativo en materia de eventos relacionados con la ciberseguridad, muy especialmente por la profusión, magnitud y complejidad de los ciberataques que han sufrido muchos países, España entre ellos.

Atendiendo a su peligrosidad e impacto, podemos clasificar tales acciones en los siguientes grupos:

Internacionalización de los ciberataques

Las acciones de ciberespionaje originadas en otros países, durante 2014 han constituido una fuente de amenazas muy peligrosas. Muchas de estas amenazas se han dirigido especialmente contra las entidades gubernamentales, los organismos del sector público y empresas poseedoras de un importante patrimonio tecnológico. La sofisticación de los ataques, desarrollados en buena medida utilizando técnicas y tácticas complejas, tales como APTs, ha asegurado el éxito de muchas de tales acciones, al tiempo que ha dificultado enormemente su atribución o autoría concretas.

Dos han sido los orígenes más significativos de los ataques: Rusia y China. Respecto de Rusia, en 2014 se han detectado 501 incidentes de este tipo, 113 de ellos de naturaleza crítica, siendo los más destacados los denominados Agent.btz, Snake, Uroburos, Turla, Octubre Rojo y Energetic Bear. Cada uno de ellos ha mostrado especial interés por atacar determinado tipo de víctimas, siendo las más frecuentes: entidades gubernamentales y administraciones públicas, organizaciones diplomáticas y embajadas, universidades y centros de investigación, empresas comerciales, empresas de los sectores de energía (carburantes y gas) y aeroespacial e instituciones militares.

Respecto de China, y atendiendo a las fuentes citadas, en 2014 se han detectado 151 incidentes, 3 de ellos de nivel crítico. Estos ataques, cuyo origen se ha atribuido en ocasiones a organizaciones del gobierno chino, se han dirigido especialmente contra los sectores aeroespacial, energía, defensa, gubernamental, farmacéutico, químico, de tecnologías de la información, financiero y transporte, y se han caracterizado por el uso de herramientas comerciales, centrando su atención en la propiedad intelectual o industrial de las organizaciones atacadas, siendo los más destacados los denominados: Ice Fog, Hiden Lynx, Snowman, Net Traveler y, la más conocida, APT1.

[10]Entre ellas, el Informe de Ciberamenazas 2014 y Tendencias https://www.ccn-cert.cni.es/index.php?option=com_docmanpriv&task=doc_download&gid=303&Itemid=168&lang=es

La empresa Mandiant[11] atribuyó directamente a la Unidad 61398, del Ejército Popular de China, la campaña APT1, cuyas víctimas han sido las empresas TIC, sector aeroespacial, administraciones públicas, sector satélites y telecomunicaciones, centros de investigación, energía, transportes, construcción y fabricación, y organizaciones internacionales, afectando los ataques a los Estados Unidos, Reino Unido, Israel, Canadá, Suiza, Noruega, Bélgica, Luxemburgo, Francia, Sudáfrica, India y Emiratos Árabes Unidos, entre otros.

No podemos concluir esta lista, necesariamente sumaria, sin mencionar otros ciberataques, alguno de ellos con origen en países hispano-hablantes (tales como las acciones denominadas Careto - The Mask o Machete), o aquellos otros de los que han podido servirse gobiernos occidentales, como los que se pusieron de manifiesto a raíz de las revelaciones de Edward Snowden. En este grupo, podemos situar las acciones denominadas Babar, Hacking Team, Regin o Equation Group, entre otras.

Finalmente queda señalar que 2014 también ha evidenciado ciberataques perpetrados por autores de lengua árabe. Quizás, el más significativo de todos ellos fue el denominado Desert Falcons.

Ciberdelincuencia profesionalizada en el ciberespacio

En 2014, con mayor intensidad que nunca, hemos observado cómo las organizaciones delincuenciales han encontrado en el ciberespacio una superficie idónea para sus acciones delictivas, algunas de las cuales han mostrado características de complejidad y sofisticación comparables a los ataques de ciberespionaje.

Así, además de acciones concretas, hemos sido testigos del surgimiento de ciberservicios de naturaleza delincuencial, que ponen a disposición de terceros herramientas -complejas y sofisticadas, en algunos casos- para la comisión de ciberdelitos. En este sentido, y de modo singular, nos encontramos con el llamado ransomware y, muy especialmente, la aparición de su variante más virulenta: el cryptoware[12], lo que ha evidenciado un nuevo modelo de negocio para los delincuentes, el llamado Crime-as-a-Service.

[11] http://intelreport.mandiant.com/

[12] También denominado ransomware de cifrado (encrypting ransomware o filecoders), impide el acceso a los datos del usuario cifrando los archivos del ordenador. Una vez infectado se realiza una petición de dinero por la clave para recuperar los datos.

La motivación de los atacantes ha sido la misma en todos los casos: el beneficio económico. En este sentido, merece la pena destacar el ciberataque conocido como Carbanak, que constituye la primera APT de naturaleza específicamente delincuencial. Los autores de esta amenaza fueron capaces de sustraer mil millones de dólares de cien instituciones financieras de todo el mundo, actuando directamente contra los bancos y no, como era lo habitual, a sus usuarios. Su autoría no ha sido definitivamente atribuida, sabiéndose que la responsabilidad de las acciones podría estar en un equipo multinacional compuesto por individuos de Rusia, Ucrania, China y otros países de Europa.

Otras motivaciones

Aunque no podemos olvidar las acciones llevadas a cabo por cibervándalos o hacktivistas con connotaciones de ciberterroristas o ciberdelincuentes, script kiddies[13] y actores internos, quizás los agentes de la amenaza que pueden completar el esquema descrito en estos párrafos lo constituyen los grupos denominados hacktivistas[14].

Entre ellos, como a los anteriores, la mayor amenaza la constituye el tronco común de Anonymous, del que se han desgajado grupos de acción regional, habiendo dirigido sus acciones tanto contra entidades gubernamentales y de las administraciones públicas de diferentes países, como organizaciones internacionales y empresas privadas. En la mayor parte de los casos sus acciones han perseguido la reivindicación de una postura política o social.

Aunque no se tiene constancia de acciones significativas, no podemos olvidar, por último, que el ciberterrorismo sigue siendo una amenaza importante. Mientras que, en la actualidad, los grupos terroristas parecen seguir apostando por acciones en el mundo físico, no es menos cierto que el ciberespacio suele ser ya su primer medio de propaganda e, incluso, de reclutamiento, por lo que será necesario redoblar los esfuerzos de inteligencia sobre tales grupos y acciones.

[13]Persona falta de habilidades técnicas que usa programas desarrollados por otros para atacar redes y sistemas y llevar a cabo cambios intencionados en páginas web.

[14]Individuos u organizaciones que promueven agendas o ideas políticas a través del uso subversivo de ordenadores y redes.

Las vulnerabilidades del software

Concluimos este apartado haciendo referencia a los problemas de seguridad derivados de la presencia de vulnerabilidades en software de uso común, lo que, durante 2014, ha sido causa de importantes problemas cuyos efectos todavía no han sido evaluados definitivamente.

Algunos de los casos más significativos han sido la vulnerabilidad “goto fail” de SSL (que llegó a afectar a dispositivos móviles de Apple que ejecutaban iOS 6 y 7 y a equipos de sobremesa que se basan en OS X 10.9), Heartbleed (descubierto en abril de 2014, y que afectó a la implmentación TLS de Open SSL) o Shellshock (que afectó a millones de equipos que funcionan con Linux y Mac OS), entre otros.

De las más de 7.000 vulnerabilidades catalogadas por INCIBE durante 2014 (basadas principalmente en la base de datos de referencia mundial del NIST del Departamento Homeland de EEUU) el 23,4% tenían criticidad alta y más del 66% criticidad media.

Ante esto, nos preguntamos: ¿Cuántas vulnerabilidades permanecen todavía sin descubrir en software que usamos cada día?

En este contexto resulta interesante la iniciativa del IEEE Computer Society, la principal asociación internacional de profesionales de tecnologías de la información, compuesta por miles de ingenieros de todo el mundo, para el diseño seguro y la identificación de defectos de diseño comunes en la esperanza de que los arquitectos de software pueden aprender de los errores de otros.

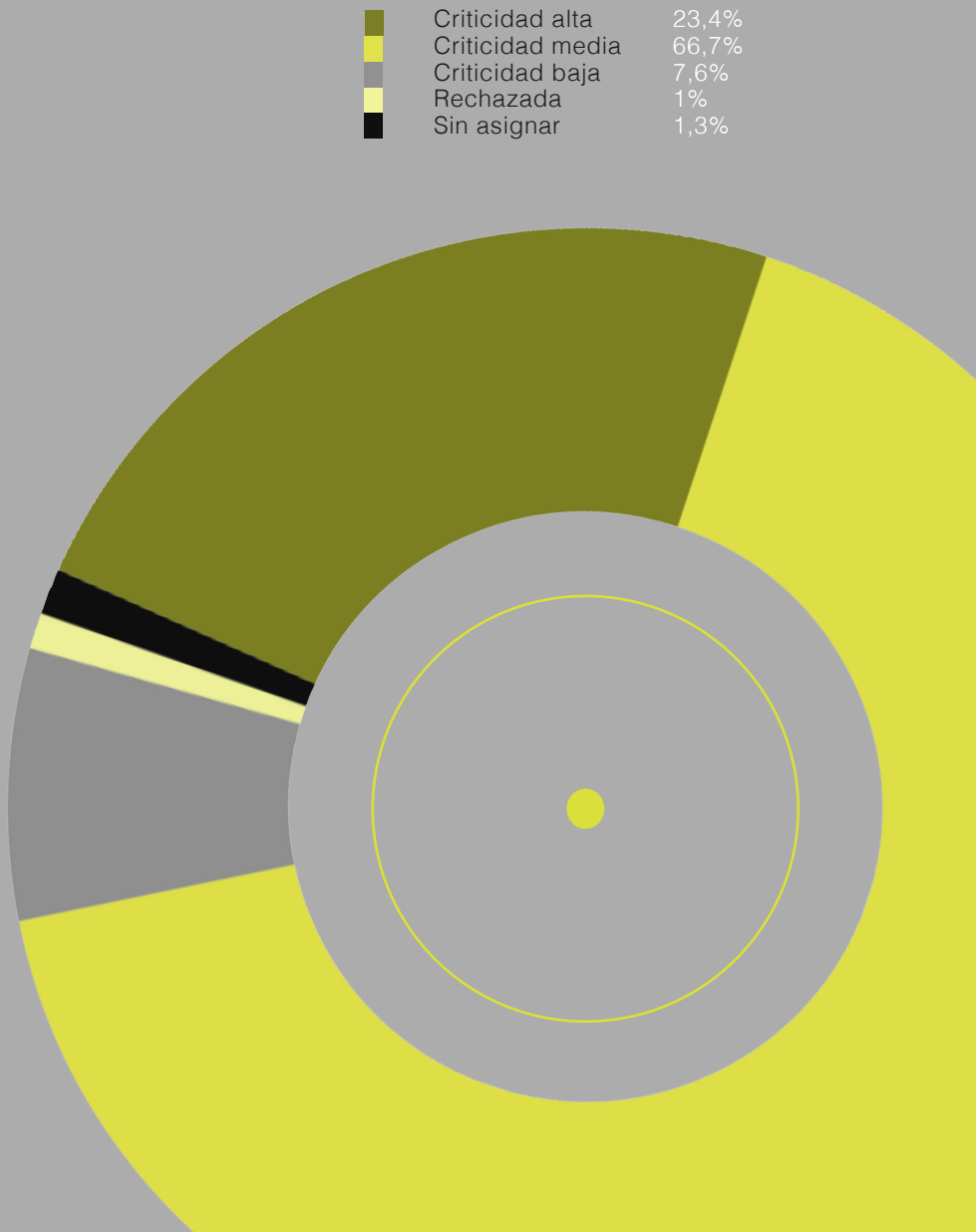


FIGURA 10. Tipologías de vulnerabilidades catalogadas por el CERTSI_ en 2014 (INCIBE y CNPIC)

3 | 2 Tendencias identificadas

3 | 2 | 1 Tecnología

Resulta difícil destacar alguna tendencia tecnológica concreta de entre todas las que alrededor de la seguridad de la información se han desarrollado durante el año 2014. A continuación proponemos cuatro, por su importancia estratégica, y pronosticamos que seguirán fortaleciéndose al menos durante los próximos años.

Uso de smartphones como prueba de identidad

Desde los albores de la informática, la combinación de un nombre de usuario y una contraseña ha sido la forma primaria de autenticación de usuarios de los servicios telemáticos. Es un mecanismo fácil y barato de implementar, por lo que ha sido el favorito del área de TI (Tecnología de la Información) en las empresas. Pero además, representa una mínima barrera de entrada para la usabilidad de los nuevos servicios, por lo que también es el favorito de las áreas de marketing.

Sin embargo, las debilidades en la selección y uso de credenciales usuario/contraseña, facilitan su actividad a los hackers, que así no necesitan romper complicados protocolos de bajo nivel para entrar al sistema.

La contraseña representa algo que solo el usuario sabe, pero una vez que este factor ha sido comprometido, todo el andamiaje de seguridad resulta inútil. La calidad de las credenciales puede mejorarse mediante la combinación de dos factores de entre la terna de “algo que se sabe, algo que se tiene o algo que se es”. El problema es que resulta caro proporcionar a los usuarios testigos (tokens o tarjetas inteligentes) o registrar características fisiológicas (biometría).

Tradicionalmente sólo las instituciones financieras han tenido un claro caso de negocio para implantar este esquema ya que la magnitud de las pérdidas por fraude puede crecer hasta números que preocuparían incluso a las áreas de TI y de marketing. Algunos de los mecanismos de autenticación por doble factor (2FA) involucran al terminal móvil, bien sea como generador de contraseña dinámica o como parte de un protocolo de desafío/respuesta. La penetración en el mercado de estos dispositivos y el uso de servicios fiables como el de mensajes cortos (SMS), lo convierten en el segundo factor de autenticación ideal, incluso frente a la tarjeta inteligente, para la mayoría de aplicaciones.

Redes anonimizadas (Tor, Freenet, I2P, etc.)

Son redes que ocultan la identidad del origen y del destino de la comunicación, así como la ruta que han seguido los paquetes de datos. En algunos casos también se oculta la identidad del proveedor del servicio de comunicación que emisor y receptor están usando (servicios de localización oculta). Esta característica se consigue, entre otros, por el uso de técnicas denominadas "encaminamiento de cebolla" para la gestión del tráfico en la Red. Con este sistema podemos tener infraestructuras para comunicaciones privadas sobre una red pública, orientada a conexión o a conmutación de paquetes. Las comunicaciones pueden ser bidireccionales, casi en tiempo real.
La criptografía de clave pública y claves simétricas de sesión protegen no sólo el contenido de la comunicación, sino también los metadatos de la misma. Por otro lado, el uso de estas redes, junto con el uso de enrutadores, proxies y navegadores específicos, aportados de forma voluntaria y situados en países con legislaciones permisivas en esta materia, dificultan en gran medida la trazabilidad de las comunicaciones, otorgando a sus usuarios un elevado grado de protección de sus comunicaciones y privacidad.
Sin embargo el uso de estas técnicas también se ha convertido en un quebradero de cabeza para las policías de todo el mundo, en particular el uso de esta tecnología en la constitución de lo que se ha dado en llamar la "red oscura" o "internet profundo". En esta capa superpuesta se están ofreciendo y contratando productos y servicios fuera de la ley. Además de los ilícitos tradicionales contra la propiedad y contra las personas, estafas, tráfico de armas, se negocian aquí ataques de denegación de servicio, extracción no autorizada de datos de compañías o personas concretas, etc.

Proxies opacos

Durante el año 2014 asistimos a una aceleración de los trabajos sobre el nuevo estándar http2, que se venían desarrollando discretamente en el seno del IETF (Internet Engeneering Task Force), que en febrero de 2015 fue aprobado por el Internet Engineering Steering Group y propuesto para publicar como RFC. Bajo la intención declarada de acelerar la introducción de los beneficios de esta nueva tecnología, mejorando la calidad y protegiendo la confidencialidad de las comunicaciones de los usuarios, cada uno de los grandes fabricantes y prestadores de servicios de internet norteamericanos han iniciado un proceso de concentración de los accesos desde los terminales de los usuarios hasta sistemas centrales (proxy), cifrando además la comunicación (opaco) entre el usuario y dichos equipos.

Las consecuencias estratégicas de este proceso de estandarización son variadas y profundas, no sólo en el terreno de la seguridad. Si los gobiernos, proveedores de acceso y otros ISPs (Internet Service Providers) no reaccionan, la persecución de los delitos será más difícil y costosa, la retención de datos para el auxilio a la justicia se volverá inoperante, y el mercado de servicios de seguridad cambiará radicalmente.
Cabe esperar también un aumento de casos de fraude y de expansión de software malicioso, ya que este tipo de ataques sólo se harán visibles en el propio terminal del usuario.

Cifrado para la nube

La migración de servicios a la nube plantea dos retos de seguridad: la pérdida de control y la pérdida de confidencialidad de los datos. En el primero de los casos, la preocupación surge por la necesidad del cumplimiento regulatorio en relación con los datos de carácter personal además del cumplimiento de los acuerdos de niveles de servicio. En el segundo de los casos, y sobre todo para las modalidades SaaS (Software as a Service) y PaaS (Platform as a Service), el tratamiento de los datos "en claro" en la nube es una fuente de preocupación, con el consiguiente riesgo de robo o filtración. Aún no existen soluciones de probada eficacia que apliquen técnicas de cifrado homomórfico[15] para salvar esta circunstancia.

Sin embargo, es posible aplicar técnicas de cifrado tradicional a la modalidad IaaS (Infrastructure as a Service) y a ciertos casos de uso de SaaS. Nos referimos fundamentalmente a los servicios de almacenamiento en la nube. Durante el año 2014 ha habido una gran oferta de servicios de cifrado masivo (proxy bulk encryption) para empresas o de soluciones para uso personal de almacenamiento. Sin embargo, muy pocas soluciones comerciales han sabido resolver los problemas del control de claves por un tercero independiente, y sobre todo, el problema de gestión de identidades entre diversos usuarios que han de compartir una misma información cuando se almacena cifrada en la nube.

[15]Un cifrado es homomórfico si se pueden realizar transformaciones con el texto cifrado sin necesidad de descifrarlo ni de conocer la clave, de manera que al descifrarlo, el texto en claro haya sufrido las mismas transformaciones.

3 | 2 | 2 Controversias

Privacidad vs. Seguridad. ¿Es el cifrado generalizado la solución a ambos problemas?

Las tensiones políticas y sociales y, por tanto, regulatorias siempre han basculado entre una norma positiva más restrictiva de las libertades individuales o más protectora de la vida privada y el derecho a la intimidad personal y familiar, dependiendo del miedo de la población o el ansia de control de sus dirigentes.

Es de recordar que los derechos humanos son una creación muy reciente y que las primeras declaraciones de derechos fundamentales tal como las conocemos no son anteriores a mediados del siglo XX. Su juventud no justificaría, obviamente, que fueran sacrificados en el altar de la seguridad, pero sin duda explican que se cuestionen de manera permanente, ya que su conquista se hizo frente al deseo de control de los gobiernos y no animados por ellos. Entre estos derechos fundamentales, los más cuestionados en este ámbito serían el derecho a la intimidad personal y familiar y la expectativa de privacidad de las acciones que no se hacen públicamente, y relacionado con ellos el de la protección de datos. Este derecho protege frente a las injerencias que el tratamiento de los datos de carácter personal tiene en la integridad personal y el desarrollo libre de la personalidad, y que no va necesariamente unido a acciones íntimas y que incluye, por tanto, desde las grabaciones de cámaras de seguridad en espacios públicos hasta las manifestaciones realizadas en las redes sociales.

Todos estos derechos pueden verse cuestionados por la intervención de gobiernos y empresas en las comunicaciones, poniéndose en cuestión la utilidad de la normativa tradicional sobre el secreto a las comunicaciones para lograr el necesario equilibrio en la protección de estos derechos, ante la irrupción de técnicas de “big data” que permiten perfilar y trazar con precisión el comportamiento e inclinaciones de los individuos sin necesidad de violar el contenido de las comunicaciones. Es por tanto necesario establecer sistemas muy robustos que permitan asegurar la privacidad y limitar la discrecionalidad de los gobiernos y empresas para intervenir las comunicaciones electrónicas o para aplicar las citadas técnicas de “big data” en perjuicio de los derechos fundamentales de los ciudadanos.

En este sentido, uno de los mecanismos utilizados por los ciudadanos para proteger su seguridad es el uso de los contratos de servicios. Los ciudadanos hacen concesiones legalmente informadas pero, en la práctica, sin ser conscientes del alcance de las mismas cuando firman mediante el “click” de aceptación las condiciones generales de contratación de diversos servicios de internet a los que no podrían acceder si no las aceptaran. Incluye prácticamente cualquier servicio en nube, incluidos los más extendidos, la mayoría de ellos sujetos a jurisdicciones ajenas a la europea y mucho menos protectoras.

Seguridad individual vs. seguridad pública

En ocasiones, los gobiernos se encuentran ante situaciones en las que se antepone la seguridad colectiva a la del individuo. Esa delgada línea a cruzar que supone la pérdida de derechos del individuo debe estar claramente definida. En el plano de la seguridad colectiva se sitúa la vigilancia legal e ilegal de los estados, con diversos intentos, más o menos consumados de intervención extrajudicial de las comunicaciones. En este contexto, creemos que las palabras del CEO de Apple en el Cybersecurity Summit organizado por la Casa Blanca el pasado febrero de 2015[16] son muy definitorias del conflicto y establecen una vía de solución. Para Cook, sacrificar el derecho a la privacidad puede tener consecuencias funestas y anima a usar la criptografía y la tecnología para protegerlo.

Siendo el uso de estas técnicas una práctica legítima para preservar la intimidad de los individuos, es indudable que su generalización implicará mayor dificultad de los Estados para desempeñar las labores de vigilancia y prevención de delitos que, como responsables de la seguridad pública, la ciudadanía espera que desempeñen.

Jurisdicción Local vs Servicios Globales

En el sentido indicado más arriba, no hay capacidad de toma de decisiones informada por parte del cliente si la información no es clara, precisa y se hace un esfuerzo por explicar los riesgos y consecuencias legales de uso de un servicio y producto. Dicho esfuerzo ha de venir de un deseo de transparencia con el cliente y de un cambio de mentalidad de los departamentos legal, técnico y de marketing del prestador. Mientras la complejidad sea alta y la explicación perezosa, se impone la relevancia de la legislación protectora del consumidor, surgiendo la cuestión de si debe aplicarse una jurisdicción local o una perspectiva de prestación de servicios globales.

Es indudablemente un reto desde un punto de vista práctico, y con frecuencia la regulación se enfoca más en la infraestructura física sobre la que se tiene jurisdicción que sobre los servicios finales que usa el ciudadano. La fijación de la jurisdicción es algo que ya aparece regulado en diversos tratados internacionales, siendo siempre de elección del consumidor final el fuero en el que quiera demandar. Sin embargo, hay barreras reales en esta norma internacional como la desproporción entre cuantía del procedimiento y coste del mismo, ley aplicable y ejecución en el extranjero de la sentencia que se dicte.

En cuanto a la tutela de derechos fundamentales, si bien el ciudadano español puede solicitarla teóricamente en su territorio, a veces resulta complicado conseguir que un estado extranjero atienda dichas peticiones o que una compañía que no se encuentra bajo el paraguas de la jurisdicción española respete sus derechos.

[16]http://www.theguardian.com/technology/2015/feb/13/apple-ceo-tim-cook-challenges-obama-privacy

3 | 2 | 3 Intereses de la sociedad en materia de ciberseguridad

En cuanto a las tendencias e intereses que preocupan a la sociedad en materia de ciberseguridad se subraya la limitación que supone en primer lugar los aspectos económicos, financieros y laborales de los ciudadanos y las empresas condicionados por la crisis económica. Frente a los ataques cibernéticos continuos y masivos, la industria afronta grandes gastos en seguridad relacionada con la tecnología informática, lo que hace alterar el esquema tradicional de negocios, más si cabe si se trata de infraestructuras esenciales como energía, sanidad o defensa, por mencionar algunas.

El apetito del riesgo en la sociedad digital

Una gestión apropiada de la gestión de riesgos y del balance del apetito de riesgo es importante en el modelo organizativo de una empresa. A estas alturas las instituciones públicas y las empresas privadas necesitan reforzarse hacia una nueva cultura de la ciberseguridad.

Esto supone un panorama de asunción progresiva, hasta alcanzar una posición equilibrada, de la función de gestión del riesgo como un elemento orgánico clave para la subsistencia de la organización. Sin embargo, en este sistema de equilibrios también se abre la agilidad y la oportunidad a empresas jóvenes que pueden afrontar las amenazas electrónicas actuales.

El apetito del riesgo que se plantean las empresas para alcanzar sus objetivos, como límite de la ecuación económica de asumir riesgos para conseguir retornos beneficiosos, necesita modularse adecuadamente. Uno de los puntos clave es situarlo dentro de un marco estratégico que incluya las políticas de seguridad de la información, los procesos, los controles y los activos de información implicados. Esto es así por las nuevas relaciones que surgen del avance de las tecnologías, que está provocando un cambio radical en las formas de negocio y entre las relaciones con los clientes.

Otro de los aspectos más significativos que podemos mencionar es el cambio en los comportamientos de las personas en relación con la globalización, enfatizado por la experiencia de la crisis mundial, y que tiene proyecciones tanto en su faceta como consumidores y como ciudadanos. Este cambio de tendencia ha puesto de relieve la necesidad de las empresas a acercarse a los clientes y poner el foco en las personas, frente a una visión antagónica centrada en los productos. En cuanto al sector público viene a poner de relieve grandes desafíos, la demanda de atención de los ciudadanos pone en jaque los mecanismos tradicionales burocráticos para abrir paso a los sistemas centrados en el ciudadano y en la participación.

Los avances en la sociedad de la información y el conocimiento influyen en gran medida en estos cambios en el comportamiento de las personas, que como consecuencia requieren nuevos servicios electrónicos, nuevos modelos de negocio y una mayor transparencia traducida en más información de mayor calidad. Esto supone posicionarse en las plataformas digitales, en los servicios online, en la telefonía móvil, en las redes sociales y en la gestión de la información masiva, como es la explotación del "big data" como fuente de información de clientes.

Todo ello suma en este ecosistema donde se mueve el apetito del riesgo, en tanto que influyen los riesgos clásicos del propio sector de negocio como los nuevos emergentes relacionados con la ciberseguridad. En definitiva, es pues un panorama de tendencias donde la confianza digital se postula como uno de los principales habilitadores para la sociedad digital y un desafío irrenunciable.

Las empresas prestadoras de servicios esenciales y los ciudadanos

La prestación de determinados servicios considerados esenciales en la vida de las personas se plantea como una evolución del libre mercado que involucra a empresas privadas en la gestión de los denominados servicios públicos, universales o de interés general.

A pesar del sistema garantista, la realidad cotidiana es percibida por los ciudadanos como que las empresas tienen su prioridad en el ejercicio legítimo de su beneficio empresarial, pero no tanto en los derechos de los usuarios. Si bien se reconoce la especial transcendencia de estos servicios y su interés público, esta situación pone de relieve un desequilibrio en la satisfacción de los usuarios con respecto a la prestación del servicio.

Sobre las tecnologías que dan soporte a los servicios esenciales, las empresas deben utilizar todos los medios necesarios para solucionar y prevenir las incidencias de seguridad. No tomar iniciativas de gestión de la seguridad, de evaluación del riesgo y salvaguardas, supone una negligencia en la línea de la "culpa in vigilando". De esta manera, la empresa actúa como cuidador reprochable en la responsabilidad de tener vigilado su ámbito de actuación y del control que debe ejercer sobre el servicio esencial.

La colaboración público-privada

El alto grado de interdependencia y la complejidad de todos los aspectos de la ciberseguridad hacen que su mejora pase por una armonía generosa entre el sector industrial y las Administraciones Públicas, pero donde también deben participar otros agentes sociales cualificados como las asociaciones profesionales y organismos de estandarización. Esto incluye el intercambio de información sobre vulnerabilidades, amenazas e incidentes de seguridad que permitan mejorar y compartir las lecciones aprendidas y buenas prácticas relacionadas con la ciberseguridad.

Por ello es importante analizar que todo esquema o iniciativa que se emprenda lleve a cabo una profunda reflexión para ubicar la ciberseguridad en el plano de la colaboración público-privada, como elemento esencial para asegurar la competitividad y el bienestar social.

En este sentido, la Estrategia de Ciberseguridad Nacional (ECSN[17]) expone los principios básicos para el sector público en España, entre los que se incluye una fluida colaboración público-privada. Así mismo, la normativa sobre Protección de Infraestructuras Críticas[18] abre una línea de diálogo entre organizaciones necesaria, pues afecta a recursos, servicios, tecnologías de la información y redes críticas, que ante un ataque podrían tener un gran impacto en la seguridad física o económica de los ciudadanos, o bien en el buen funcionamiento de la Administración.

La métrica viene determinada en función del potencial de víctimas, del impacto económico o público y los sectores estratégicos como son las tecnologías de la información y las comunicaciones, las centrales y redes de energía, el sistema bancario-financiero, el sector sanitario, las relacionadas con el espacio, la alimentación de la población, red de abastecimiento de agua, los transportes y seguridad vial, la industria química y nuclear, así como la administración pública de servicios básicos.
La colaboración del sector privado es fundamental en la consecución de los objetivos de seguridad nacional.

También el Plan de Confianza en el Ámbito Digital (PCD[19]), que hace suyo el mandato de la Estrategia de Ciberseguridad Nacional, contribuye a responder a los cometidos de dicha estrategia mediante la implicación de todas las partes interesadas. Entre otras medidas implantadas por el PCD, se ha creado el Foro Nacional para la Confianza Digital, constituido por distintos agentes del sector privado, industria, profesionales, I+D y consumidores.

[17]http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

[18]http://www.cnpic.es/Legislacion_Aplicable/Generico/index.html

[19]http://www.agendadigital.gob.es/planes-actuaciones/Paginas/plan-confianza-ambito-digital.aspx

Derecho cívico de información sobre ciberseguridad

Es importante garantizar que los ciudadanos y las empresas tengan acceso a la información sobre vulnerabilidades e incidentes de seguridad.
El concepto abunda en la ciberseguridad para mantener la confianza de los usuarios. La importancia de este derecho se realza desde el mismo momento en que pasa a ser relevante para la protección de otros derechos individuales, como la intimidad, la protección de datos personales o la defensa frente a la ciberdelincuencia. Al conjunto de actores que actúan en este escenario de seguridad de la información, debe sumarse el individuo como sujeto activo y pasivo.

Por poner algunos casos en este sentido, el ámbito en el que se enmarca la preocupación ciudadana relativa a preservar tanto sus datos privados como sus hábitos o tendencias, se ven modificados en el contexto actual. Como ejemplo, se puede mencionar el empleo de contadores eléctricos inteligentes (Smart meters dentro de Smart Grids), que a pesar de comportar un claro beneficio para el usuario en términos de ahorro energético, presenta serias dudas en relación con la preservación de la seguridad de los datos, no sólo en cuanto al contenido de los datos personales, sino en cuanto a que se puedan analizar patrones de comportamiento aunque la integridad de los datos quede preservada. Preocupaciones similares se presentan en el empleo de sistemas tales como redes de sensores o sistemas NFC/RFID (por ejemplo, para identificación perimetral o de acceso o sistemas de pago), sistemas que son fundamentales a la hora de implementar entornos contextuales, propios de las ciudades inteligentes.

Se presenta como una exigencia coordinar esfuerzos en armonizar el marco jurídico y las líneas de acción para que la información sobre ciberseguridad esté accesible por los ciudadanos como un derecho en sí, que posibilite una nueva visión más cercana, asequible y de utilidad para las personas.

Formación, educación y concienciación social

La formación y la conciencia social en ciberseguridad en el ciberespacio es un aspecto esencial para afrontar y prevenir los riesgos emergentes y el factor humano como objetivo de la amenaza frente a ataques de ingeniería social.

Contribuiría a ello la inclusión en todas las etapas educativas del sistema educativo la urbanidad cibernética y la cultura de ciberseguridad, desde la educación infantil, primaria, secundaria, formación profesional hasta la universitaria, adaptando los contenidos y procedimientos curriculares. Hoy día los más pequeños crecen manejando dispositivos electrónicos, acentuando la brecha digital de los más mayores. Los docentes necesitan una intensa formación en seguridad de la información para poder transmitir con solvencia a los alumnos los valores de la protección de la información en las redes sociales y otros servicios de Internet.

Complementariamente en las ingenierías y ciencias superiores relacionadas debe fortalecerse las líneas educativas relacionadas con la calidad para asegurar los diseños e implementaciones de los sistemas hardware y software, ya no sólo en áreas o asignaturas concretas, sino de forma trasversal. Para ello es necesario un mecanismo que permita evaluar en qué medida se aplica esta transversalidad. También en estudios universitarios relacionados con las ciencias sociales y jurídicas, así como el resto de ramas del conocimiento, debe de añadirse la ciberseguridad como una materia más, que sirva de puente y acerque la ingeniería que usan cada día los estudiantes al currículum educativo.

La formación continua en el ámbito laboral debe incorporar planes de educación en esta materia y la colaboración pública debe profundizar en las necesidades reales de las amenazas en el uso cotidiano de las tecnologías de la información y las comunicaciones de los usuarios.

Los estudios de posgrados, la investigación y el desarrollo, en la dinámica Universidad-Empresa, requiere de más líneas de trabajo en seguridad de la información, acorde con el crecimiento tecnológico, los avances y los riesgos emergentes.

La conciencia social no es un edificio que se construye en un día, pero es tarde si no se pone la primera piedra para establecer en el futuro más cercano unos cimientos sólidos en seguridad, lo que previsiblemente debe ofrecer una imprescindible adaptación del sistema educativo.

Seminarios en materia de seguridad

Una forma ágil de estar al día e ir moldeando la conciencia social, a distintos niveles técnicos y no técnicos, consiste en el fomento y desarrollo de seminarios, jornadas de debate, talleres prácticos y conferencias. Este elemento parece clave para la especialización, la discusión y el contraste de ideas. La repercusión social y económica viene de la mano de la compartición de experiencias, buenas prácticas y soluciones, lo que redunda en una mayor confianza en el mundo digital.

3 | 2 | 4 Respuesta a través de medidas regulatorias y otras actuaciones de los poderes públicos.

Establecimiento de responsabilidades en empresas prestadoras de servicios esenciales

En el ámbito civil, en general, las limitaciones a la responsabilidad no vienen por la vía regulatoria, ya que las acciones de culpa contractual y extracontractual son plenamente aplicables, sino a las limitaciones de responsabilidad contractual, que en este ámbito son amplísimas (no garantía de funcionamiento, entrega de software “as is”, cláusulas penales que minimizan el quantum, etc.).

A ello se acompaña una pobre sistemática de cálculo de las pérdidas o del daño causado, siendo extremadamente complicado calcular el daño patrimonial indirecto. En el caso de daño moral, no hay normas ni jurisprudencia consolidada.

Estas limitaciones son especialmente relevantes cuando se trata de la prestación de servicios esenciales, en cuya prestación los poderes públicos deben asumir una mayor responsabilidad moral, pero cuya delimitación no es siempre clara, ¿se trata de los antiguos servicios públicos, o de los prestadores y entidades con la consideración de infraestructuras críticas?

La vía de la responsabilidad civil por tanto parece poco práctica a no ser que se cambiase el derecho de daños mundial, algo que no va a suceder.

Por su parte, la modificación del Código Penal en 2010 que introdujo la responsabilidad penal de las personas jurídicas, no ha acabado siendo el catalizador que se esperaba, sobre todo por el limitado impacto que los delitos tecnológicos y su modo de comisión tienen en este ámbito.

Derecho de información

Aparte de distintas iniciativas privadas, existen distintas acciones impulsadas por las AAPP, como es el caso del Observatorio de Seguridad del Internauta (OSI) y el portal web del CCN-CERT.

En la Oficina de Seguridad del Internauta (OSI) de INCIBE se proporciona la información y el soporte necesarios para evitar y resolver los problemas de seguridad que pueden existir al navegar por Internet. En este portal se facilita información general sobre la seguridad en Internet y herramientas para ayudar a navegar de forma más segura. Además, existe un canal de avisos para estar al tanto de las últimas alertas de seguridad.

También en el portal del CCN-CERT se puede encontrar información muy valiosa relacionada con la ciberseguridad. Entre otros, se publica información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, y también las series de documentos CCN-STIC que ofrecen normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica y para garantizar la seguridad de los sistemas de Tecnologías de la Información en la Administración.

Colaboración público-privada

El Plan de Confianza en el ámbito Digital hace suyos los compromisos de la Agenda Digital para España[20], de la Estrategia Europea de Ciberseguridad (EUCS) y de la Estrategia de Ciberseguridad Nacional (ECSN) en los ámbitos de la confianza digital y en el alcance objetivo del mercado digital interior, la ciudadanía, las empresas, la industria y los profesionales, proponiendo un conjunto de medidas que contribuyan a darles cumplimiento y alcanzar los objetivos conjuntos en colaboración con todos los agentes implicados. Entre otras, algunas de las medidas del PCD se exponen a continuación:

- Implantación del Foro Nacional para la Confianza Digital, que está constituido por distintos agentes del sector privado, industria, profesionales, I+D y consumidores.
- Implantación de una plataforma tecnológica que permita generar inteligencia, a partir de fuentes de información de terceros y de eventos de seguridad conocidos a través de herramientas incorporadas en la propia plataforma.
- Puesta en marcha de un centro técnico y de atención al usuario (Punto neutro de gestión de incidentes) para dar soporte al código de conducta de gestión de incidentes de seguridad previsto en la disposición adicional novena de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Elaboración de un esquema de gestión de incidentes de seguridad que tiene por objetivo establecer mecanismos de colaboración entre INCIBE y los prestadores de servicios de la Sociedad de la Información, los registros de nombre de dominio y los agentes registradores que estén establecidos en España con el fin mejorar las capacidades de alerta temprana y prevención y de mitigar los incidentes de seguridad

La perspectiva de colaboración público-privada también resulta esencial en el desarrollo de la normativa que, en esta materia, tiene su origen fundamentalmente en la Unión Europea, como el recientemente adoptado Reglamento de Identidad Electrónica y Servicios de Confianza (reglamento eIDAS) y el actual proyecto de Directiva de Seguridad de la redes y de la Información (Directiva NIS). En la fase de negociación de estas normas es preciso establecer los mecanismos de coordinación entre las autoridades competentes y propiciar el diálogo con el sector privado para alcanzar los objetivos de la posición española, y en la fase de implementación se promueve la adopción de la normativa técnica de desarrollo buscando el necesario equilibrio entre las partes interesadas así como el desarrollo de medidas de acompañamiento.

[20]Los mandatos de la Agenda Digital para Europa (ADEU) están ya incluidos en la propia Agenda Digital para España de conformidad con el procedimiento de su propio proceso de elaboración.

3 | 2 | 5 Contribución del modelo de gobernanza

Papel de los desarrolladores de productos y sistemas

Con la interconexión de redes cada vez más generalizada, muchos de los requisitos técnicos que tradicionalmente se asociaban para sistemas críticos son cada vez más necesarios en la construcción de todo tipo de aplicaciones e infraestructuras, tanto privadas como públicas.

En este contexto adquiere relevancia la especificación de requisitos de calidad y su evaluación, que sigue siendo una tarea pendiente en nuestros esquemas de contratación, tanto pública como privada. En esta línea se sitúan estándares como SQuaRE ISO/IEC 25000 (Software Product Quality Requirements and Evaluation) que pretenden organizar y enriquecer este planteamiento respecto del propio producto software y no sólo respecto del proceso de construcción, así como la iniciativa del IEEE Computer Society, para el diseño seguro y la identificación de defectos de diseño comunes.

En este mismo marco, también cabe encuadrar el reciente mandato M/530[21] que la Comisión Europea ha dado a los Organismos Europeos de Normalización para la elaboración de normas técnicas europeas y documentos de apoyo correspondientes para garantizar la “privacidad por diseño”, que tendrá gran relevancia en la utilización de este tipo de productos al ser estas normas técnicas la base para la adopción de medidas reglamentarias de carácter técnico.

[21] http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548

Papel de las administraciones públicas

Aparte de por su papel como impulsores en el desarrollo de estándares y su eventual exigencia por vía normativa, las administraciones públicas tienen un papel especialmente relevante al ser probablemente el mayor usuario de productos y servicios TIC y por ello, poder condicionar el uso de estos productos en el resto de la sociedad.

Desde el punto de vista de la ciberseguridad, esto implica una importancia cada vez mayor en que estándares de la ingeniería del software en productos de las Administraciones Públicas garanticen el mayor nivel de corrección y calidad de producto a nivel técnico. Además de otras consideraciones, esto tendría implicaciones a nivel preventivo en cuanto a la seguridad.

Cabe destacar, además, el papel creciente que se vislumbra para la administración electrónica, en el marco de implantación y diseño del paradigma de Internet de las Cosas (IoT) y su expresión más cercana de cara a los ciudadanos, como entornos contextuales y Ciudades Inteligentes. En este contexto, en el cual se potencia un intercambio masivo de datos, así como la automatización de los mismos, se abren nuevas oportunidades de interacción entre los ciudadanos, así como con diversos estratos de las administraciones. Todo ello es factible si se analiza de manera detallada el reto de interoperabilidad y procesamiento masivos de datos.

En este esfuerzo, la participación de organizaciones profesionales de ámbito global que abarquen una amplia gama de áreas de tecnología aporta una perspectiva realista, enraizada en la industria, pero en la que es necesaria la introducción de múltiples partes interesadas, como las ciencias multidisciplinares, el derecho o la criminología para una visión diáfana de la ciberseguridad y la gobernanza en Internet. Ante los ciberataques sufridos en infraestructuras civiles y militares, especialmente los dirigidos al Pentágono, este mismo año Estados Unidos ha anunciado, a través de su presidente, que la lucha contra la piratería será una de sus prioridades legislativas, donde estas reuniones multi-parte y la compartición de información toma gran relevancia, lo que da una idea de la magnitud del esfuerzo y los retos a los que se enfrentan los gobiernos.

Servicios privados de ciberseguridad

La regulación del mercado de prestación de servicios privados de ciberseguridad viene marcada por la Ley 5/2014, de 4 de abril, de Seguridad Privada[22], cuyo artículo 6 prevé la imposición de requisitos técnicos específicos a las empresas, sean o no de seguridad privada, que presten servicios de seguridad informática (entendida como el conjunto de medidas encaminadas a proteger los sistemas de información a fin de garantizar la confidencialidad, disponibilidad e integridad de la misma) para garantizar la calidad de dichos servicios, por su incidencia directa en la seguridad de las entidades públicas y privadas.

[22]https://www.boe.es/boe/dias/2014/04/05/pdfs/BOE-A-2014-3649.pdf

La dilación en el tiempo de este desarrollo reglamentario supone un vacío normativo que deja en una indefinición los servicios privados de ciberseguridad, que para nada facilita la resolución de problemas de seguridad ni la coordinación esperada.

Adicionalmente hay que tener en cuenta que los servicios privados relacionados con los centros de operación de ciberseguridad (SOC), que gestionan y monitorizan la seguridad de redes y activos de sus clientes, se solapan en gran medida con entidades de respuesta ante incidentes CERT. La configuración actual de los CERT públicos, con diferentes dependencias orgánicas y aparente dispersión competencial, requiere ser analizada al objeto de proporcionar una estructura organizativa común que facilite la comunicación y la información de ciberalertas.

Es por tanto necesario desarrollar procedimientos adecuados que articulen de modo eficiente esta comunicación, poniendo especial hincapié en las sensibilidades que los sectores implicados tienen con respecto a sus actividades profesionales.

Protocolos de intercambio de información

Estandarizar protocolos de intercambio de información sobre incidentes es un reto tanto para las empresas privadas entre sí como con el sector público. La propia legislación reciente de seguridad privada deja como infracción muy grave la falta de comunicación de las incidencias relativas al sistema de cuya protección sean responsables, y también el proyecto de Directiva NIS establece la obligación de los operadores de comunicar los incidentes de ciberseguridad relevantes a las Autoridades competentes. Para todo ello se debe delimitar ya no sólo los métodos y mecanismos, sino la identificación de las tipologías preceptivas de comunicación.

Agilizar estos protocolos de información debe ser fruto de una reflexión que va más allá de la mera función burocrática, debe ser el cauce efectivo para mejorar la seguridad y la protección del ciberespacio de la ciudadanía y las empresas. Sin embargo, otros aspectos deben ser tenidos en cuenta, especialmente la privacidad de las personas y de las organizaciones y las prescripciones impuestas por ciertas disposiciones, como la normativa de protección de datos personales vigente, con respecto a la difusión de información que se pueda perfilar con datos sensibles.

Armonización penal y judicial

Sobre tipos delictivos y persecución judicial de los delitos, surgen diversos problemas derivados de la ubicación y la jurisdicción en un contexto de globalización donde Internet supone una extraordinaria independencia de las fronteras políticas. Añadido a los tipos penales tradicionales, han entrado en juego elementos específicos que pueden dificultar de forma relevante la persecución y sanción de conductas ilícitas. Así, la problemática heredada en cuanto a la regulación y la competencia de los Estados sobre conductas ilícitas a través de Internet, presenta también consecuencias negativas y lagunas jurídicas difíciles de abordar.

Es necesaria la existencia de una base armonizada y consensuada, que bien podría quedar asociada al Derecho Internacional o que, cuando menos, debería quedar asentada entre Estados cubriendo las máximas posibilidades. Para lograr sentar fundamentos que aporten seguridad jurídica, la lucha contra la ciberdelincuencia necesita avanzar partiendo de la línea de consenso con el Convenio de Budapest, del Consejo de Europa[23].

Esto queda patente con los datos presentados por el informe de cibercriminalidad de 2014, de la Secretaría de Estado de Seguridad del Ministerio del Interior, que señala que un más del 90% de los delitos cibernéticos quedan impunes. Parece, por tanto, que deben buscarse mecanismos globales armonizados comúnmente aceptados, que permitan atajar esta problemática que –lejos de serlo aisladamente- es una problemática internacional.

[23]https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf

Regulación de la gestión de crisis

El hecho de regular la participación de prestadores y administración pública es de vital importancia para la gestión de crisis cibernéticas. Una normativa clara, preferiblemente unificada, en cuanto a los organismos responsables en materias de ciberseguridad facilitaría la organización de la seguridad a todos los niveles. El ciberespacio como bien común de la humanidad sufre las dificultades de una gobernanza global de Internet sin una adecuada regulación internacional. Esto hace que de por sí las crisis provocadas por ataques cibernéticos deban solucionarse a una escala estatal cuya eficacia viene limitada. El incremento de la ciberdelincuencia, el ciberespionaje, ciberterrorismo y las actividades antisociales hacen que los recursos públicos destinados a las fuerzas de seguridad encargadas de la ciberseguridad sean insuficientes.

En definitiva, se necesita una regulación clara, un refuerzo en los recursos de seguridad pública y la participación activa de empresas privadas, asociaciones profesionales globales e instituciones académicas para la organización de los sistemas de gestión de crisis.

Fuera del impulso o necesidad de una regulación más fuerte y enfocada a promover la ciberseguridad y ciberresiliencia es también muy crítico trabajar en un esquema que potencie la I+D+i y el fomento del talento en ciberseguridad, necesidades también detectadas y enfocadas como área de trabajo y mejora en la Estrategia Nacional de Ciberseguridad y en la Agenda Digital para España en su Plan de Confianza en el ámbito Digital (Eje 6), iniciativas gubernamentales que inciden en incrementar la capacidad de la industria de ciberseguridad, pero también de aumentar las habilidades de nuestros profesionales TIC y de ciberseguridad para desarrollar e innovar en servicios más ciberseguros y confiables.

3 | 3 Iniciativas regulatorias relevantes en 2014

Durante el pasado año se han desarrollado algunas iniciativas regulatorias que tendrán grandes repercusiones en los años venideros. No se trata aquí de una recopilación exhaustiva, sino que se pretende subrayar la repercusión de la regulación en cuanto a ciberseguridad se refiere y por ende, en la Sociedad de la Información.

3 | 3 | 1 Unión Europea

Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (eIDAS)[24]

La creación de un mercado único digital de identidades y servicios de confianza es una de las medidas clave identificadas en la Agenda Digital para Europa[25] para aprovechar al máximo las Tecnologías de la Información y la Comunicación (TIC), acelerar la recuperación económica y sentar las bases de un futuro digital sostenible.

Éste es el objetivo del Reglamento eIDAS, que entró en vigor el 17 de septiembre de 2014, siendo su fecha de aplicación efectiva a partir del 1 de julio de 2016, previéndose asimismo su desarrollo a través de legislación secundaria europea que consistirá en al menos 28 actos de implementación o delegados, muchos de los cuales referenciarán normas técnicas en desarrollo por ETSI/CEN.

En relación con la identificación electrónica, el Reglamento establece un marco de reconocimiento mutuo de cierto tipo de esquemas de identidad electrónica que los Estados Miembros notifiquen a la Comisión. Para ello los Estados Miembros intercambiarán información a través de un marco de interoperabilidad, cooperación y revisión conjunta de los esquemas de identificación sujetos a reconocimiento mutuo, que engloban tanto a personas físicas como a jurídicas. Por su parte, los servicios de confianza regulados en el Reglamento son la firma electrónica, el sello electrónico, el sello de tiempo electrónico, la entrega certificada electrónica y el servicio de autenticación web.

[24] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:JOL_2014_257_R_0002&from=EN

[25] http://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:52010DC0245

En relación con la identificación electrónica, el Reglamento establece un marco de reconocimiento mutuo de cierto tipo de esquemas de identidad electrónica que los Estados Miembros notifiquen a la Comisión. Para ello los Estados Miembros intercambiarán información a través de un marco de interoperabilidad, cooperación y revisión conjunta de los esquemas de identificación sujetos a reconocimiento mutuo, que engloban tanto a personas físicas como a jurídicas. Por su parte, los servicios de confianza regulados en el Reglamento son la firma electrónica, el sello electrónico, el sello de tiempo electrónico, la entrega certificada electrónica y el servicio de autenticación web.

En relación con la dualidad entre firma y sello electrónicos, el Reglamento separa claramente los sujetos activos en cada caso, al señalar que las personas físicas firman y las personas jurídicas sellan electrónicamente. El Reglamento regula adicionalmente la validación y preservación de firmas y sellos electrónicos. Del mismo modo, es destacable que el Reglamento abra la posibilidad de prestación de servicios innovadores basados en soluciones móviles y en la nube, como la firma remota, en respuesta a la evolución de la tecnología y el mercado. Asimismo, establece la obligatoriedad de la certificación de los dispositivos cualificados de creación de firmas y sellos electrónicos. Los servicios de sello de tiempo y entrega certificada electrónica, que venían siendo ya prestados, son regulados en cuanto a sus requisitos y efectos jurídicos. Se debe remarcar en relación con los servicios de autenticación web que el reconocimiento de los certificados provenientes de terceros países se ha de producir a través de un acuerdo bilateral entre el país y la UE.

Todos estos servicios cualificados serán oportunamente listados en la Lista de Servicios de Confianza (TSL) mantenida por cada uno de los Estados Miembros.

Se decidió adoptar un Reglamento, de aplicación directa en los Estados Miembros, en lugar de la revisión de la directiva vigente para reforzar la seguridad jurídica en la UE, acabando con la dispersión normativa provocada por las diferentes transposiciones de la Directiva en cada ordenamiento jurídico. Se debe remarcar que la Ley de firma electrónica española no se deroga, sino que sufre un desplazamiento jurídico en favor del Reglamento, manteniéndose en vigor las disposiciones que no se ven afectadas por el nuevo Reglamento.

Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión (NIS)[26]

La Comisión Europea presentó en febrero de 2013 la propuesta de Directiva sobre Seguridad de las Redes y de la Información para su consideración por el Consejo de la Unión Europea y el Parlamento Europeo. La propuesta de Directiva NIS es una de las medidas de la "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro"[27]. La tramitación en las instituciones europeas está realizándose por el procedimiento legislativo ordinario[28].

El objetivo de esta propuesta es facilitar un elevado nivel común de seguridad de las redes y de la información en el Mercado Único Digital. Se trata de una Directiva de Mercado Interior y, por tanto, su contenido no afecta a políticas nacionales en las que la Comisión Europea no es competente, como seguridad y defensa. Por otro lado, es importante notar que las obligaciones de la Directiva serán adicionales a las establecidas en otras disposiciones de carácter transversal, en particular las derivadas de la normativa de Protección de Datos personales[29] y de protección de infraestructuras críticas.

Para aumentar la seguridad de Internet y de las redes y los sistemas de información que sustentan el funcionamiento de nuestras sociedades y economías, es necesario, por una parte, instar a los EEMM a estar más preparados e incrementar la cooperación entre ellos, y, por otra, exigir a los operadores de servicios esenciales, sean entidades privadas o administraciones públicas, que adopten las medidas oportunas para gestionar los riesgos de seguridad y notificar los incidentes graves a las autoridades nacionales competentes.
Cabe puntualizar que se configura como una "Directiva de mínimos" al identificar una relación mínima de "sectores esenciales", común para toda la UE, que puede ampliarse dentro de cada Estado miembro extendiendo las obligaciones previstas en la Directiva a operadores de otros sectores que se consideren esenciales. Dentro de cada sector de servicios esenciales, corresponde a cada Estado miembro designar los operadores que, por la importancia de los servicios que ofrecen en el país, estarán sometidos a las obligaciones previstas en la Directiva, así como una Autoridad Competente encargada de supervisar la aplicación de dichas obligaciones y un Equipo de Respuesta a Incidentes de Ciberseguridad (CERT o CSIRT) responsable de gestionar incidentes y riesgos, si bien no se prohíbe la existencia de varias autoridades competentes o CERTs en cada Estado.

[26]http://data.consilium.europa.eu/doc/document/ST-6788-2015-INIT/en/pdf

[27]http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

[28]En marzo del 2015 se adoptó un mandato de negociación en el Coreper del texto elaborado en el seno del Grupo de Trabajo del Consejo de Telecomunicaciones

[29]Actualmente en revisión en la UE a través de una propuesta de Reglamento que sustituirá a la Directiva 95/46/CE

Propuesta 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[30]

Con esta propuesta la Comisión actualiza y moderniza los principios de la Directiva de protección de datos de 1995. La propuesta de Reglamento de protección de datos se presentó al Consejo en enero de 2012 y está siendo examinada en el Grupo del Consejo de Intercambio de Información y Protección de Datos. Entre las cuestiones más importantes que el Consejo ha debatido en el año 2014, están el mecanismo de ventanilla única para los casos transnacionales importantes y las competencias de la Comisión para adoptar actos delegados y de ejecución.

El Reglamento recoge los derechos de los interesados, como por ejemplo el derecho de acceso a sus datos personales, el derecho de rectificación, el derecho al olvido, el derecho a la supresión, el derecho a la oposición y el derecho a la portabilidad de los datos.

Asimismo, especifica las obligaciones generales de los responsables y encargados del tratamiento, por ejemplo, la aplicación de las medidas de seguridad pertinentes y la notificación de las violaciones de datos personales. La Comisión, a través de este Reglamento, aborda otras cuestiones fundamentales, como la obligación existente para los Estados miembros de crear una autoridad de control independiente a nivel nacional y el establecimiento de mecanismos para lograr una aplicación coherente de la legislación sobre protección de datos en toda la UE.

También se reconoce el derecho de los interesados a presentar una reclamación a la autoridad de control, así como su derecho al recurso judicial, la compensación y la responsabilidad. Por otro lado, se establecen los métodos para el cumplimiento de lo dispuesto en el Reglamento y el alcance de las sanciones para quienes infrinjan las normas.

[30]http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf

3 | 3 | 2 España

Los legisladores en España son conscientes de la importancia de la ciberseguridad en el desarrollo de la economía y de la sociedad digital y por ello se adapta la normativa a las nuevas necesidades.

La Estrategia de Seguridad Nacional 2013[31] preveía la necesidad de una norma para perfeccionar los instrumentos de gestión de crisis del Sistema de Seguridad Nacional para responder a los nuevos desafíos, entre otros, en relación con la ciberseguridad. Así, a finales del año 2014, el Consejo de Seguridad Nacional remitió la propuesta de anteproyecto de Ley Orgánica de Seguridad Nacional[32], que ha sido objeto de Informe para el Consejo de Ministros previo a su tramitación como proyecto de ley.

También se elaboró el anteproyecto de Ley Orgánica de Modificación de la Ley de Enjuiciamiento Criminal para la agilización de la Justicia penal[33], el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas, que fortalece los derechos procesales en el ámbito de los derechos a la intimidad, al secreto de las comunicaciones y a los datos personales regulando las medidas de investigación tecnológica en los sistemas de comunicación telemática.

Otra iniciativas legislativas acontecidas en el ámbito de la ciberseguridad en estos dos últimos años son la Agenda Digital para España, con el Plan de Confianza en el ámbito Digital, y la Disposición adicional novena introducida en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico por el apartado dieciséis de la disposición final segunda de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
Esta disposición establece que los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las obligaciones de seguridad indicadas.

El desarrollo de estas obligaciones se confía a un esquema de colaboración público-privada, los denominados códigos de conducta. En esta disposición se hace referencia al tratamiento de direcciones IP, información que inevitablemente será necesario compartir entre los equipos de respuesta de incidentes con las autoridades competentes cuando se trata de identificar el origen de ataques y equipos afectados.

Finalmente conviene señalar la Ley Orgánica de modificación del Código Penal[34], que contempla aspectos como la ciberdelincuencia económica y delitos contra menores de edad potenciados por el uso generalizado de las TIC.

[31] http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

[32] http://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/160115-anteproyleyorg.aspx

[33] Su tramitación parlamentaria comenzó en marzo del 2015 (http://www.congreso.es/public_oficiales/L10/CONG/BOCG/A/BOCG-10-A-139-1.PDF#page=1)

[34] Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal

Capítulo 4

Privacidad y vigilancia

Coordinación: **Ricard Martínez Martínez y José Leandro Núñez García**

Editores/Autores: **Emilio Aced Félez, Urko Fernández Román, Ricard Martínez Martínez, José Leandro Núñez García y Fernando Suárez Lorenzo**

Grupo de Trabajo:

Emilio Aced Félez (Agencia Española de Protección de Datos)

Borja Adsuara Varela (Enatic)

Nacho Alamillo Domingo (Astrea)

Urko Fernández Román (Pantallas Amigas)

Roberto Ferrer Serrano (Aralegis)

Norman Heckh (Ramón y Cajal Abogados)

Esperanza Ibáñez Lozano (Google)

Ricard Martínez Martínez (APEP)

José Leandro Núñez García (Audens Abogados)

Paula Ortiz López (IAB Spain)

Alejandro Perales Albert (AUC)

Fernando Suárez Lorenzo (Vicepresidente/Consejo de Colegios de Ingenieros en Informática)

Ofelia Tejerina Rodríguez (Asociación de Internautas)

Paloma Villa Mateos (Telefónica)

4 | 1 Introducción

La garantía de la privacidad constituye un elemento capital para la construcción presente y futura de Internet. Sea este concepto, o el más propiamente europeo de derecho fundamental a la protección de datos, la realidad acredita la importancia de su protección para disponer de un gobierno democrático de Internet que asegure el pleno respeto de la libertad.

Podría definirse 2014 como el año en que perdimos la inocencia, en el que la sociedad global cayó en la cuenta de que salvaguardar la vida privada en las redes frente a la injerencia de terceros constituye sin duda un derecho humano básico. Distintos acontecimientos han contribuido a promover un escenario social cada vez más concienciado. Ciertamente las alertas sobre el control totalitario de las redes se vienen sucediendo desde las Primaveras Árabes. Sin embargo, el detonante de esta inquietud social se sitúa singularmente en el caso Snowden. El espionaje masivo de Internet, llevado a cabo por las autoridades en y por el país de la democracia, sin límites internos o externos, y desde la legalidad, ha hecho saltar todas las alarmas.

Por otra parte, en el último bienio parecen haber cuajado un conjunto de tecnologías y despejado la Terra Incognita a la que se referían las autoridades de protección de datos en su Conferencia de 2007. Así, enfrentamos un provenir cuajado de oportunidades, una sociedad en la que la combinación de altas capacidades de almacenamiento y computación, la multiplicación de los sensores en todo tipo de objetos y contextos, o la versatilidad funcional de los periféricos concebidos cómo una suerte de vivienda virtual móvil hiperconectada a nuestra casa, nuestra ropa y a nuestros medios de pago, auguran una revolución económica, cultural y social.

Sin embargo, esta realidad tecnológica neutral en su ADN puede verse profundamente alterada en sus resultados por factores epigenéticos. Así Big Data promete ser una herramienta esencial para la medicina, pero podría ser la fuente de discriminaciones si se aplica inadecuadamente a la predictibilidad del comportamiento si se asocia a medidas de control de la peligrosidad social. Nuestros teléfonos inteligentes, las tecnologías ponibles y el Internet de las cosas, pueden ser un instrumento liberador que optimicen nuestra gestión del tiempo y faciliten nuestra vida, o la puerta de entrada al control ideológico o a la manipulación de nuestras preferencias. En el mundo celular, incluso cuando la secuencia genética es correcta una influencia externa puede conducir a errores en su expresión, a la enfermedad. En el mundo de las redes, la privacidad opera sin duda como el catalizador que contribuye a salvaguardar un uso correcto dela tecnología. La privacidad en las redes se erige sin duda en el pilar que sustenta las libertades.

4 | 2 La privacidad 2014-2015. Acontecimientos relevantes

En este periodo acontecimientos de distinto signo han marcado la evolución de la privacidad en Internet y definido las bases del escenario que se anuncia. Destacamos aquí los más significativos.

4 | 2 | 1 El año del Tribunal de Justicia de la Unión Europea

Históricamente, salvo en lo que se refiere a la significativa sentencia del caso Linqdvist, ha sido el Tribunal Europeo de Derechos Humanos el que venía fijando de algún modo las líneas que trazaban la evolución de la protección de datos, como derecho fundamental de los europeos. Halford, Leander, Gaskin, Rotaru, Z c. Finlandia y Marper son casos que han conformado una doctrina europea sobre la materia.

Sin embargo, y con prácticamente un mes de diferencia, -abril y mayo de 2014, han emanado del Tribunal de Justicia de la Unión Europea (TJUE) dos sentencias determinantes. Los asuntos Digital Rights Ireland y Costeja han cambiado por completo el panorama. Y lo han hecho no tanto por operar cambios significativos en un derecho perfectamente definido en sus rasgos constitucionales, como por definir un nuevo rol de la Corte, e insertar en nuestro sistema elementos sustanciales en términos de eficacia normativa y de establecimiento de un modelo europeo de privacidad en tiempos de guerra contra el terror.

La pseudoconstitucionalización de la Carta de los Derechos Fundamentales de la Unión Europea, que pasa de ser un documento programático a poseer valor jurídico, ha sido determinante para que el TJUE opere como un tribunal europeo de constitucionalidad asumiendo retos jurídicos impensables hace un lustro a los que nos referimos de inmediato.

Conservación de datos en las comunicaciones. Caso Digital Rights Ireland Ltd. et alii

La sentencia de 8 de abril de 2014, dictada en Gran Sala por el Tribunal de Justicia de la Unión Europea en los asuntos acumulados C-293/12 y C-594/12, supone en la práctica la derogación de la Directiva sobre conservación de datos en las telecomunicaciones.[1] La norma se dictó en un contexto de máxima tensión, tras los atentados terroristas de Madrid de 2004 y Londres de 2005. Del mismo modo que en Estados Unidos se dictó la USA Patriot Act, la Directiva pretendía ofrecer herramientas para facilitar la investigación de delitos graves.

Para contribuir a la lucha antiterrorista la UE abordó un cambio radical en el modo de entender la interceptación de las comunicaciones. Y para ello se desarrolla una estrategia de "comptage" preventivo, habilitando a la legislación nacional para ordenar la conservación de un amplio conjunto de datos personales vinculados a las comunicaciones[2] por un periodo de seis meses a dos años. Es fundamental entender que no sólo se trata del impacto de estos tratamientos en los datos personales, ya que no se afecta únicamente a este derecho fundamental. De una parte, el "comptage", - esto es, la averiguación automatizada del número telefónico asociado a las líneas llamadas desde el terminal interferido y de las llamantes -por cuanto no se accede a lo comunicado-, se integra por el Tribunal Europeo de Derechos Humanos en el secreto de las comunicaciones. De otra, algunos datos como los relativos a la geolocalización pueden incidir directamente en la intimidad u ofrecer información relacionada con otros derechos, como las libertades ideológica y de reunión o manifestación.

El TJUE afirma con rotundidad en la sentencia que conservar los datos de tráfico en las comunicaciones, además de una excepción a los deberes de cancelación de las Directivas 95/46/CE[3] y 2002/58/CE[4], constituye una injerencia en los derechos a la vida privada de una persona y a sus comunicaciones, y también en el derecho fundamental a la protección de datos, previstos en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea.

En opinión del TJUE, si bien es cierto que el impacto en el contenido esencial de los derechos es limitado -por cuanto no se accede a lo comunicado-, es en la proporcionalidad donde la norma quiebra con la garantía de los derechos fundamentales. Este principio exige «que los actos de las instituciones de la Unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos».

[1]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.

[2]Las categorías de datos pueden consultarse en el artículo 5 de la Directiva y comprende los datos necesarios para rastrear e identificar el origen, el destino, la fecha, hora y duración, el tipo y el equipo, de una comunicación. Se trata de un conjunto de datos técnicos que se relacionan con la telefonía de red fija y a la telefonía móvil, el acceso a Internet, correo electrónico por Internet y telefonía por Internet, datos necesarios para identificar la localización del equipo de comunicación móvil.

[3]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.

[4]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 (Directiva sobre la privacidad y las comunicaciones electrónicas).

En primer lugar, es necesario señalar que los datos objeto de conservación constituyen una herramienta útil para las investigaciones penales. El Tribunal se centra muy particularmente en la necesidad de «establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión y establezcan unas exigencias mínimas de modo que las personas cuyos datos se hayan conservado dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos respecto de tales datos».

Y aquí es donde existen problemas. Primero por el ámbito de aplicación, ya que «constituye una injerencia en los derechos fundamentales de prácticamente toda la población europea» sin que se establezca ninguna diferenciación, limitación o excepción en función del objetivo de lucha contra los delitos graves. Además la conservación de datos no exige ninguna relación entre estos y una amenaza para la seguridad pública, ni se acota a un grupo de personas o ámbito geográfico determinado. En segundo lugar, la propia indefinición de la norma constituye un problema en la medida en la que se limita a remitir a los delitos graves tal como se definen en la legislación nacional de cada Estado miembro. Y no sólo esto sino que la indefinición se proyecta tanto sobre las condiciones materiales y de procedimiento para el acceso, -al no acotar el tipo de sujetos legitimados-, como sobre el establecimiento de límites expresos vinculados a la finalidad que justifica la directiva, que no prevé controles y garantías previas jurisdiccionales o administrativas.

Por último, el tribunal invoca dos razones adicionales para concluir con la vulneración del principio de proporcionalidad: el periodo de conservación no se basa en criterios objetivos y justificados, y la carencia de reglas precisas en términos de medidas de seguridad, incluida la ausencia de limitación para el almacenamiento y tratamiento en países terceros.

El impacto de la sentencia en el Derecho nacional se prevé limitado. Si bien no es descartable que la cuestión sea considerada interpretativamente, mediante el procedimiento de apertura del artículo 10.2CE a los tratados internacionales en materia de derechos humanos, existen razones de orden competencial y material que apuntarían en la línea de su no aplicación.

En primer lugar, parece evidente a la luz de los Tratados y de la Constitución que la regulación de aspectos relativos a la seguridad pública y de orden penal constituye una competencia de los Estados miembros. Ello excluye por tanto la inaplicación de la norma española en virtud del principio de primacía.

En segundo lugar, la ley española sortea los escollos que plantea la sentencia[5]. Así, se definen los sujetos que pueden acceder a los datos, -los agentes facultados-, se establecen controles judiciales previos, los tratamientos se encuentran sometidos a la competencia y control de la Agencia Española de Protección de Datos, y el Reglamento de desarrollo de la LOPD establece para estos ficheros un nivel medio de seguridad reforzado con la aplicación de medidas de trazabilidad en los controles de acceso y en las acciones de los usuarios de los sistemas de información propios del nivel alto[6].

Será en la determinación del concepto de delito grave, que debe hacerse mediante integración de conceptos ínsitos en la legislación penal, o en el carácter indiscriminado de la interceptación que afecta a todo el territorio y población dónde podría plantearse alguna objeción de coherencia entre el Ordenamiento interno y la Carta de los Derechos Fundamentales de la Unión Europea.

[5]Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

[6]Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

El derecho al olvido. Caso Google c. AEPD y Costeja

La sentencia de 13 de mayo de 2014, dictada en Gran Sala por el Tribunal de Justicia de la Unión Europea en el asunto C-131/12 define un nuevo escenario en la aplicación del Derecho de la unión en el contexto de Internet. Como es sabido, el llamado "caso Costeja" ilustra un conjunto de supuestos en los que el denominador común es el impacto que causa el resultado de una búsqueda en Internet cuando el criterio de la misma es el nombre y apellidos de una persona.

En la práctica, este tratamiento de datos puede resultar tan beneficioso, -cuando es autoritativo o confiere prestigio-, como dañoso si la información atañe a la vida privada, o menoscaba el honor o la imagen del afectado. En este sentido, los buscadores han dado lugar a un nuevo fenómeno, conocido en inglés como life logging, y que definiría una tendencia tanto autónoma como heterónoma a generar y guardar rastros digitales de las personas.

La sentencia resulta innovadora por distintas razones. En primer lugar, partiendo del precedente Lindqvist se considera que las tareas de búsqueda, indexación, conservación y posterior edición de la información por un buscador constituyen un tratamiento. Sería el interés legítimo en ofrecer información el criterio que habilitaría el tratamiento, siendo el buscador el que, en calidad de responsable, decide los fines y medios para las búsquedas y fija los criterios que asociarán una consulta por nombre y apellido con un determinado resultado. Por ello, y con independencia de la instalación en origen de etiquetas de desindexación, corresponde al buscador establecer condiciones de cumplimiento normativo de la Directiva. Por otra parte, y en la medida en que se considera que la tarea de contratación publicitaria de la filial del buscador es indispensable para la empresa matriz, se aplicará la Directiva en virtud del criterio de establecimiento.

El resultado práctico es cuando una persona realice una consulta por nombre y apellidos y ésta arroje un resultado sensible para la vida privada, el afectado podrá ejercer un derecho de oposición frente al buscador con independencia de la página de origen (incluso cuando el tratamiento en ésta sea legítimo), ya que lo relevante es el efecto magnificador que produce el resultado de la búsqueda. Corresponderá entonces al buscador:

a. Verificar si efectivamente el afectado invoca un motivo legítimo y fundado, referido a su concreta situación personal.

b. Establecer si la justificación invocada constituye una base adecuada para el ejercicio del derecho de acceso.

c. Verificar si existe una obligación legal respecto de la publicación de este dato.

Por tanto, no existen soluciones globales. En cada caso hay que determinar el carácter dañoso, o banal, de la información o si por el contrario concurre un interés público prevalente, se enmarca en el ejercicio legítimo de la libertad de expresión o prevalece el valor histórico o científico de los resultados publicados. Resultados que, en todo caso, no se eliminarían ni del índice del buscador ni de la página de origen: simplemente dejarían de aflorar al emplear el nombre y los apellidos del afectado como criterio de búsqueda, siguiendo a disposición de los usuarios que empleen otro término para tratar de localizar la información en cuestión.

La sentencia pone sin duda de manifiesto un estado de Internet caracterizado por una doble tensión normativa. De una parte, parece que al menos los tribunales si han decidido “poner puertas al campo”. En este sentido, y con las dificultades propias de una evolución acelerada de las tecnologías de la información, el Derecho tiende a colonizar Internet. El segundo conflicto deriva de un desacuerdo central a ambos lados del atlántico, no tanto en la importancia de la privacidad, como en los métodos para garantizar su tutela y el alcance la misma.

Debe destacarse que esta resolución trae causa de una cuestión prejudicial del Tribunal Supremo español en un recurso contra una resolución de la Agencia Española de Protección de Datos, y que (en esencia) refrenda los argumentos del supervisor español, confirmando una larga doctrina, iniciada en noviembre de 2007.

4 | 2 | 2 Agenda normativa

La agenda normativa viene marcada sin duda por el desarrollo del Proyecto de Reglamento General de Protección de Datos, presentado en 2012 por la Comisión. Esta norma está siendo objeto de una lenta tramitación. En este sentido, la ponencia de la Comisión LIBE en el Parlamento Europeo fue objeto de centenares de enmiendas, y la postura definitiva de éste no vio la luz hasta el 12 de marzo de 2014,[7] siendo objeto de debates en el seno del Consejo los distintos capítulos hasta el día de la fecha.[8]

Sin perjuicio del resultado final, este proyecto incluye muchos aspectos relevantes susceptibles de cambiar las condiciones de aplicación de la normativa, adaptándola al momento actual. En una lista que no pretende ser exhaustiva, cabe subrayar algunas aportaciones de la normativa que, o bien constituyen un cambio significativo, o bien tendrán la capacidad de influir en la cultura de protección de datos.

En primer lugar, la noción del concepto de "accountability"[9] supone el reforzamiento de las metodologías de "compliance" iniciadas en los últimos años. En tal sentido, que la mera falta de diligencia en la implementación de procedimientos ordenados a la garantía del cumplimiento normativo genere responsabilidad constituye una novedad cultural de primer orden. Por otra parte, esta exigencia de responsabilidad es instrumental, y debe entenderse completada con los requisitos de documentación de los procesos de tratamiento de datos personales, más exigentes en su contenido que el existente deber de inscripción.

Por otra parte, la Propuesta otorga carta de naturaleza a procedimientos de privacidad por defecto y privacidad basada en el diseño. No se trata de una novedad en sí misma. Los profesionales españoles, si bien de modo intuitivo ya llevaban a cabo muchas de estas tareas en su labor diaria de asesoramiento. Asimismo, no hay que olvidar que estas metodologías habían sido ya teorizadas y sistematizadas bajo el liderazgo de la autoridad de protección de datos de Ontario[10] y la definición de los siete principios de la privacidad en el diseño[11]. Lo que resulta sin embargo destacable es que, tras la entrada en vigor de la norma, optar por minimizar el volumen de datos personales objeto de tratamiento e insertar la privacidad en todos los estadios del ciclo de vida de un proceso o aplicación desde su génesis, van a pasar a constituir una obligación jurídica de carácter imperativo.

[7] Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta 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 (Reglamento general de protección de datos). Disponible en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//ES

[8] Para una cronología documentada véase http://eur-lex.europa.eu/procedure/ES/201286

[9] Este término no tiene una traducción clara al español, si bien suele interpretarse como "rendición de cuentas". En este contexto, se corresponde más con un compromiso ético de las organizaciones de respetar la privacidad en todas sus actuaciones, hasta el punto de ir más allá del mero cumplimiento.

[10] Véase https://www.privacybydesign.ca/

[11] Véase https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-spanish.pdf

En directa relación con ello se encuentra el concepto de Análisis de Impacto en la Privacidad (Privacy Impact Assessment). La obligación de desarrollar un análisis específico de los riesgos asociados a un determinado tratamiento ha ido sufriendo vaivenes en las distintas versiones de la Propuesta. No obstante la sensibilidad de los datos, el impacto en categorías específicas de personas o su volumen parecen criterios que orientarán el deber de realizar un PIA. Esta es una metodología asentada en el mundo anglosajón y cuya importación a la Unión Europea debe asignarse sin duda al Information Commissioner's Officce de Reino Unido[12].

Otro de los elementos destacados es la definición normativa del delegado de protección de datos -data protection officcer o DPO-, al que se asignan tareas precisas, pero cambiantes según la versión del documento que se maneje. Se trata de una figura llamada a ser determinante en tres planos: como garante interno e impulsor de condiciones de cumplimiento normativo, como órgano de atención de los derechos de acceso, rectificación, cancelación y oposición al tratamiento y de tutela corporativa de los afectados, y como interlocutor natural con la autoridad de protección de datos personales.

Por último, en una lista que no pretende ser exhaustiva, puede citarse como muy relevante la alusión, en distintos momentos, a la certificación, llamada a ofrecer potenciales resultados positivos a la hora de proporcionar confianza en los proveedores, la seguridad, y las capacidades de los profesionales. En segundo lugar, debe señalarse la búsqueda de mecanismos de simplificación de algunos procedimientos, y singularmente de la información al afectado, que podría basarse en sistemas estandarizados mediante símbolos. Finalmente, se amplía el ámbito de aplicación territorial de la norma, independientemente de que el tratamiento tenga lugar en la UE o no; o cuando un responsable o un encargado del tratamiento no establecido en la Unión dirija sus actividades de tratamiento a interesados en la Unión, independientemente de si media o no contraprestación económica.

Por otra parte, existen elementos que suscitarán a buen seguro controversia. Entre ellos, el más destacado es el relativo al establecimiento de un sistema de ventanilla única que podría suponer que procedimientos de todo tipo sean objeto de tramitación en un solo país. En tal sentido, salvo que se establezca (al igual que en la legislación sobre derechos del consumidor) un sistema de elección del fuero por el afectado, un potencial incumplimiento que afecte a un ciudadano español podría sustanciarse en otro territorio. Del mismo modo, los costes de tramitación de los responsables se incrementarán cuando requieran de apoyo y servicios jurídicos en país distinto al de su establecimiento.

En el plano internacional debe destacarse la significativa evolución de la materia en el continente Americano. De una parte, se produce una constante afirmación de un modelo compartido de protección de datos personales en el contexto de la Red Iberoamericana de protección de datos[13] con países que cuentan con legislación específica, - Argentina, Costa Rica, Ecuador, El Salvador, México, Nicaragua, Perú-, otros Estados que han desarrollado algún tipo de legislación sectorial, -Bolivia, Brasil-, y finalmente Honduras y Chile, próximos a unirse al primer grupo, con su normativa en tramitación. Ello permite la creación de una identidad cultural compartida en protección de datos que fomenta relaciones de confianza mutua y permite la obtención por estos países de la condición de país seguro, desde el punto de vista de la Unión Europea.

[12]Véase https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

[13]Véase http://www.redipd.org/legislacion/andorra-ides-idphp.php

En el plano internacional debe destacarse la recuperación por el Gobierno Obama del proyecto de ley ordenado a garantizar el derecho a la privacidad de los consumidores, Consumer Privacy Bill of Rights Act-2015[14] En su primer planteamiento en 2012 esta propuesta se basaba en siete principios[15]:

1. **Transparencia.** La información debería ser concisa, bien visible y de fácil comprensión ofreciendo información precisa, clara y oportuna sobre las prácticas de privacidad y de seguridad de las entidades.

2. **Control individual.** Los responsables deben proporcionar a las personas medios razonables para controlar el tratamiento de sus datos personales y proporcionales a los riesgos de privacidad. Ello incluye también medios para retirar su consentimiento.

3. **Definición de condiciones de tratamiento en función del contexto.** Lo que comportará desarrollar análisis de riesgos de privacidad (PIA) y proporcionar a las personas transparencia y mayor control individual en relación con tales riesgos.

4. **Proporcionalidad en la recogida y uso Responsable.** Se trata de que un responsable pueda recoger, conservar y utilizar los datos personales "razonables" a la luz de su contexto. Asimismo el principio de finalidad determinaría la destrucción o anonimización de los datos personales dentro de un tiempo razonable después de cumplir con los fines para los que fueron recogidos.

5. **Seguridad.** Contempla el adoptar medidas para proteger los datos personales frene a la pérdida, puesta en riesgo, la alteración y el uso no autorizado o divulgación. Incorpora el análisis riesgos e implementar medidas de seguridad razonables a la luz de esa evaluación.

6. **Acceso y veracidad.** Contempla tanto la satisfacción del derecho de acceso como las medidas ordenadas a restaurar o garantizar la veracidad de los datos.

7. **Rendición de cuentas (responsabilidad o accountability).** Implicaría tareas como formar al personal, realizar PIAs, adoptar estrategias de privacidad en el diseño, vincular a los cesionarios para usar los datos de manera coherente con las obligaciones del cedente y adoptar otras medidas razonables para garantizar el cumplimiento de la Ley.

Por otra parte, la capacidad de control sobre el cumplimiento normativo o "enforcement" se atribuye a la Federal Trade Commission, el Fiscal General de cada Estado de la Unión en el plano de la interposición de acciones civiles, y un elenco de sanciones civiles. La norma prevé, por último, el impulso de códigos corporativos de cumplimiento normativo.

Si bien, no puede afirmarse que se trate de una norma comparable al modelo europeo en su concepción, se aprecia una tímida evolución hacía una cierta cultura compartida de garantía de los derechos fundamentales de los ciudadanos.

[14]Véase https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf

[15]N. del A. Se ha buscado una traducción coherente con los términos usuales en protección de datos en nuestro idioma.

4 | 3 La privacidad en España

La garantía del derecho a la vida privada en España posee una enorme importancia, ya sea por leyes específicas en relación con la intimidad, la propia imagen, o el secreto de las comunicaciones, ya sea por el efecto fundamental de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Y ellos se manifiesta de diversas formas.

4 | 3 | 1 Crónica de jurisprudencia

En el plano constitucional nuestro Alto Tribunal ha abordado en distintas sentencias, -SSTC 13/2014, 14/2014, 15/2014, 16/2014, 23/2014, 43/2014, y 135/2014-, la cuestión del tratamiento de datos de ADN en la investigación policial y penal. En las mismas considera que una «muestra biológica del demandante de amparo supone una injerencia en el derecho a la privacidad por los riesgos potenciales que de tal análisis pudieran derivarse».

El Tribunal incorpora la jurisprudencia del Tribunal Europeo de Derechos Humanos en el caso S y Marper c. Reino Unido que afirma que «la obtención de una muestra bucal puede constituir una intromisión en la intimidad del demandante, dado que la sistemática retención de este material y el perfil de ADN excede del ámbito de la identificación neutra de caracteres tales como las huellas digitales y es suficientemente invasiva para considerarla una intromisión en la vida privada en los términos del art. 8.1 del Convenio europeo para la protección de los derechos humanos y de las libertades fundamentales».

En materia de protección de datos se minimiza el impacto de los análisis de ADN con fines de identificación al establecer que «el perfil de ADN obtenido a partir de una muestra biológica identifica a la persona, pero que no puede decirse que en el indicado perfil genético (el obtenido con efecto identificativo mental) se incorporen otro tipo de datos que puedan contribuir a configurar un perfil o caracterización de la persona en sus aspectos "ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo" (STC 292/2000, FJ 6), que es el ámbito de protección dispensada por el art. 18.4 CE» recordando además que el derecho a la protección de datos no es ilimitado. Ello, sin perjuicio de que el afectado pueda ejercer sus derechos, entre ellos el de cancelación.

4 | 3 | 2 Crónica legislativa

En el plano legislativo hay dos normas que merecen ser brevemente destacadas. En primer lugar, cabe referirse a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información cuyo Título I, sobre "Transparencia de la actividad pública" entró en vigor en diciembre de 2014. En el desarrollo y cumplimiento de esta norma va a ser crucial cómo se aplique el artículo 15 sobre protección de datos personales. Se han incorporado criterios limitativos de todo tipo basados tanto en la sensibilidad de los datos como en la identificabilidad de las personas, tratando de establecer límites y ponderaciones basadas en criterios como el interés público de los datos personales, y la posibilidad de anonimizar parcial o totalmente la documentación[16]

Por otra parte, será fundamental observar la manera en que se van definiendo las limitaciones a la transparencia que implica el respeto al derecho fundamental a la protección de datos y la evolución de las relaciones y la coordinación institucional entre el Consejo de Transparencia y la Agencia Española de Protección de Datos. La segunda norma a considerar es la Ley 5/2014, de 4 de abril, de Seguridad Privada. Lo más relevante en esta materia deriva del hecho que el artículo 42 de la Ley establece que, cuando la finalidad de los servicios de videovigilancia sea prevenir infracciones y evitar daños a las personas o bienes objeto de protección, o impedir accesos no autorizados, éstos «serán prestados necesariamente por vigilantes de seguridad o, en su caso, por guardas rurales». No obstante, y según el criterio manifestado por la AEPD en su Séptima Sesión Abierta, las garantías en relación con la videovigilancia no han sufrido cambios relevantes desde el punto de vista de la protección de datos, por lo que la doctrina de la Agencia no ha sufrido modificaciones.

Deben destacarse por último sendas comisiones parlamentarias. En primer lugar, la Subcomisión de Estudio sobre las Redes Sociales de la Comisión de Interior del Congreso de los Diputados, que aprobó su Informe el 24 de marzo de 2015[17], y entre cuyas recomendaciones se encuentra el reclamar la definición de «parámetros de edad y privacidad y herramientas de denuncia en las redes sociales» así como medidas orientadas a facilitar el control y retirada de la información en Internet, impedir ciertos tratamientos publicitarios y garantizar la seguridad.

En la misma línea ha trabajado el Senado con la Ponencia conjunta de estudio sobre los riesgos derivados del uso de la Red por parte de los menores[18]. Destacan las medidas que desde las redes sociales pueden adoptarse «en relación con la verificación de la edad y la configuración de los parámetros de privacidad, ámbito en el que el poder público debe promover el mayor nivel de avance posible a través de la autorregulación, al tiempo que su acción normativa, en un país como España, miembro de la Unión Europea, debe situarse en el marco que en este nivel se establezca».

[16]Expertos en la materia apuntan igualmente ciertas carencias, como el mantenimiento de los criterios previstos en la Ley de Patrimonio Histórico, aprobada en una sociedad con una mortalidad a edades más tempranas que las actuales, o el recurso a conceptos jurídicos indeterminados como el de "menor perjuicio de los derechos de los afectados".

Disponible en http://www.congreso.es/public_oficiales/L10/CONG/BOCG/D/BOCG-10-D-643.PDF

Disponible en http://www.senado.es/legis10/publicaciones/pdf/senado/bocg/BOCG_D_10_410_2763.PDF

4 | 3 | 3 El gobierno

En lo que se refiere a la acción gubernamental en el plano de la iniciativa legislativa, debe destacarse la reciente presentación del Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial[19] La propuesta incorporará a la ley vigente un capítulo sobre protección de datos de carácter personal en el ámbito de la Administración de Justicia. El proyecto consolida la diferenciación entre ficheros jurisdiccionales y no jurisdiccionales. El responsable de los primeros es el órgano jurisdiccional y se rigen por las leyes procesales en libertad relativo a los derechos de acceso, rectificación, cancelación y oposición al tratamiento. La autoridad de control de tales ficheros será el Consejo General del Poder Judicial. Por otro lado, el responsable de los ficheros no jurisdiccionales es la Oficina Judicial, al frente de la cual está un Letrado de la Administración de Justicia. Ese tipo de ficheros se regirán por la normativa existente en materia de protección de datos de carácter personal y la autoridad de control de estos ficheros será la Agencia Española de Protección de Datos.

Por otra parte, deben destacarse dos foros creados por el Gobierno con incidencia en ámbitos especializados con impacto en la privacidad.
En primer lugar, el Foro Nacional para la Confianza Digital (FNCD)[20] que se define como «un instrumento de cooperación de la industria TIC española en materia de confianza digital, en el que colaboran los agentes más relevantes del sector privado, realizando funciones de asesoramiento a la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información en el ejercicio de sus competencias». Entre las tareas desarrolladas por el Foro las cuestiones relacionadas con el binomio privacidad-seguridad ocupan un espacio de trabajo importante.

Por otro lado se ha constituido el Grupo de Trabajo Público-Privado de Menores e Internet bajo la coordinación de Red.es que integra a miembros de la Administración General del Estado, diferentes instituciones y representantes de la sociedad civil. Se estructura a su vez en grupos de trabajo de los cuales dos de ellos abordarán cuestiones relacionadas con la privacidad. Serán coordinados por el Ministerio de Justicia (marco normativo) y el Ministerio de Interior (seguridad y privacidad).

[19]Véase http://www.congreso.es/portal/page/portal/Congreso/Congreso/Iniciativas?_piref73_2148295_73_1335437_1335437.next_page=/wc/servidorCGI&CMD=VERLST&BASE=IW10&PIECE=IWA0&FMT=INITXD1S.fmt&FORM1=INITXLUS.fmt&DOCS=2-2&QUERY=%28I%29.ACIN1.+%26+%28PROTECCION+DE+DATOS%29.ALL

[20]Véase http://www.agendadigital.gob.es/FNCD/Paginas/foro-nacional-confianza-digital.aspx

4 | 3 | 4 La actividad de la Agencia Española de Protección de Datos en el ámbito de Internet

En este apartado se pretende hacer una breve relación de las acciones que se consideran más relevantes o novedosas entre las que ha llevado a cabo la Agencia Española de Protección de Datos a lo largo del año 2014 señalando que hay muchos aspectos que no se van a reseñar y que pueden ser consultados, así como todo el conjunto de indicadores de su actividad, en su Memoria correspondiente al pasado ejercicio.

Concienciación y formación

En este apartado merece la pena resaltar la presentación, coincidiendo con el Día Europeo de Protección de Datos, el 28 de enero de 2014, del canal de vídeos 'Protege tus datos en Internet' (www.agpd.es/protegetuprivacidad), un proyecto online que ha contabilizado 116.257 accesos en su primer año. Incluye diez vídeos didácticos en formato de videotutorial en los que se explica, paso a paso, cómo configurar las opciones de privacidad de los principales navegadores, redes sociales y sistemas operativos móviles.

También se celebró la XVII Edición de los Premios Protección de Datos, gran parte de los cuales recayeron, un año más, en trabajos dedicados a Internet, especialmente en la modalidad de comunicación. Así, fueron premiadas ex aequo las periodistas Marimar Jiménez, de Cinco Días (por sus trabajos dedicados, entre otros aspectos, a los cambios en la política de privacidad de Google o la ciberseguridad) y Beatriz Navarro, de La Vanguardia (por sus informaciones relacionadas con temas como el "derecho al olvido" o el nuevo marco europeo de protección de datos). La también informadora Carmen Jané recibió un accésit por sus artículos publicados en El Periódico de Cataluña, relacionados con las nuevas amenazas contra la privacidad o las cookies.

La AEPD también organizó el curso 'Protección de datos y nuevas tecnologías' en el marco de las Actividades de Verano 2014 de la Universidad Internacional Menéndez Pelayo y que analizó el impacto y los retos que las nuevas tecnologías y los servicios de Internet plantean en relación con el derecho a la protección de datos de carácter personal, abordando en profundidad diferentes cuestiones relacionadas con el denominado derecho al olvido, la aplicación de la normativa de cookies o el creciente fenómeno del Big Data. El curso dedicó también un amplio espacio a exponer las claves del futuro Reglamento europeo de protección de datos, así como a las evaluaciones de impacto, un instrumento para trabajar de forma preventiva sobre los posibles riesgos que puede plantear para la privacidad un producto o servicio.

Consultas y Resoluciones sobre internet

Entre los informes jurídicos evacuados por la Agencia Española de Protección de Datos, Internet ocupó igualmente un lugar destacado. Dejando a un lado los importantes informes preceptivos, que contribuyen a sistematizar nuestra normativa en lo relativo a protección de datos, merece la pena destacar las respuestas a consultas relacionadas con la aplicación de la normativa de telecomunicaciones; la legitimación para la instalación y uso de sistemas de videovigilancia; la información y consentimiento en relación con el uso de cookies y cuestiones relativas a la interacción entre el derecho a la protección de datos y la transparencia administrativa.

Resoluciones

Este apartado debe iniciarse mencionando las numerosas resoluciones relativas al "derecho al olvido" que se han producido, en particular tras la sentencia del TJUE del mes de mayo de 2014. En este sentido, hay que destacar que no siempre se atienden automáticamente las pretensiones del reclamante, pues la Agencia debe ponderar la aplicabilidad de esta doctrina caso por caso: no en vano, en muchas ocasiones se ha considerado que se trata de ocultar información de interés público y no obsoleta, por lo que no se ha estimado la reclamación y la Agencia no ha impuesto al buscador la retirada del enlace.

Por otro lado, se han venido dictando numerosas resoluciones en sectores como la videovigilancia por cuestiones como la captación no proporcional de vía pública al colocar dichas cámaras o por no ofrecer la información que marca la ley (cartel informativo). También han sido frecuentes las resoluciones en torno a cámaras en comunidades de vecinos y garajes así como sobre la utilización con fines de control laboral de cámaras instaladas con fines de seguridad y sin información previa a los trabajadores.

También ha habido sanciones por publicar indebidamente datos en Internet; por proceder al alta en servicios de diversos tipos de manera fraudulenta y sin que la entidad denunciada obrara con la necesaria diligencia para verificar la identidad del afectado; por la utilización de cookies sin informar suficientemente o sin habilitar los mecanismos necesarios para verificar el consentimiento inequívoco; por no respetar la obligación de consentimiento previo en las comunicaciones comerciales electrónicas no solicitadas o por no proporcionar los medios de baja que establece la LSSI o por no respetar el deseo de cancelación de los afectados; por incumplimiento de las medidas de seguridad establecidas en el Título VIII del RLOPD y por el incumplimiento del deber de secreto, en particular, al enviar correos-e a múltiples destinatarios sin utilizar el campo de copia oculta.

Cuestiones estratégicas

Aun sin entrar en su contenido, que ya se trata en otros puntos de este informe, no puede dejarse de mencionar en este apartado la intensa labor realizada por la AEPD para la defensa del derecho fundamental a la protección de datos de los ciudadanos europeos, que culminó con la Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014, en el asunto Google v. AEPD, Costeja, sobre el llamado "derecho al olvido" y que continúa en la actualidad con su aplicación a los casos que llegan a la misma sobre este tema.

En otro orden de cosas, los graves atentados terroristas en París contra el semanario satírico Charlie Hebdo y contra establecimientos de la comunidad judía reabrieron los debates sobre el tratamiento de datos de viajeros, que reflejan la compleja relación que mantienen seguridad y derechos y libertades fundamentales. Estos debates sin duda van a continuar en los próximos años con respecto a datos de las reservas de pasajeros de avión (PNR), pero también en el creciente número de ámbitos en que las exigencias de seguridad determinan el tratamiento de datos personales como en la retención de datos de tráfico de las comunicaciones electrónicas. La AEPD, junto al resto de autoridades de protección de datos europeas, ha expresado repetidamente sus dudas sobre la eficacia de este tipo de medidas, por su impacto sobre los derechos fundamentales de las personas.

Por otra parte, el año 2014 ha sido el del despegue definitivo del Internet de las Cosas, el año en que esta tecnología ha empezado a integrarse, de forma definitiva, como parte de la actividad diaria de los ciudadanos. Así, en paralelo al desarrollo de numerosas iniciativas públicas y privadas se han empezado a introducir en el léxico común conceptos como contador o termostato inteligente, tecnología vestible o wearable, ciudades inteligentes y otros muchos relacionados no sólo con el entorno corporativo o institucional sino con nuestra propia actividad individual, sea profesional, familiar o de ocio.

La Agencia Española de Protección de Datos actuó como ponente junto con Comisión Nacional de Informática y Libertades francesa (CNIL), del dictamen que sobre estos temas adoptó el Grupo de Trabajo del Artículo 29 (GT29) en el que, utilizando algunos de los desarrollos más recientes en dicho ámbito, se presentaba un análisis general de las implicaciones de este fenómeno, incluyendo los riesgos en protección de datos de carácter personal. El documento también desarrollaba un conjunto de recomendaciones dirigidas a los diversos actores con interés en la puesta en marcha de sistemas integrados en el Internet de las Cosas.

La Agencia está prestando también especial atención al desarrollo del Big Data o Datos Masivos (gigantescas cantidades de datos digitalizados que son controlados por las empresas, autoridades públicas y otras grandes organizaciones que poseen la tecnología para realizar un análisis extenso de los mismos basado en el uso de algoritmos) pues sin duda va a ser uno de los grandes retos de los próximos años.

Así, además de trabajar internamente para evaluar sus implicaciones en materia de protección de datos, la AEPD ha sido partícipe en el ámbito internacional de los dictámenes y documentos de trabajo elaborados conjuntamente para analizar este fenómeno.

Igualmente, la Agencia Española de Protección de Datos participó en un análisis conjunto realizado por la Red Global de Control de la Privacidad (GPEN, Global Privacy Enforcement Network), en el cual se han estudiado los procedimientos utilizados por los desarrolladores de aplicaciones para garantizar la privacidad y la protección de los datos de usuarios de aplicaciones móviles. En particular, el análisis se centró en estudiar los procedimientos utilizados para informar al usuario de aplicaciones móviles sobre los tratamientos realizados así como los orientados a obtener su consentimiento para el acceso a la información almacenada en los dispositivos.

Privacidad desde el diseño

Abundando en la protección de datos desde el diseño y en los enfoques proactivos, la Agencia presentó a finales de octubre de 2014 la Guía para una Evaluación de Impacto en la Protección de Datos Personales, tras someter a consulta pública un primer borrador de la misma. La publicación de esta guía y el hecho de haber tenido en cuenta los comentarios y sugerencias recibidas para su redacción final supone diseñar un marco de referencia flexible contando con la voz de unas organizaciones que, más allá del mero cumplimiento normativo, también deben asumir un compromiso activo y responsable con la protección de datos.
El objetivo del análisis de los riesgos que un nuevo sistema, producto o servicio puede implicar para la protección de datos y su posterior eliminación o mitigación, que es lo en esencia es una evaluación de impacto en la protección de datos, es, por un lado, conseguir una tutela más activa del derecho fundamental a la protección de datos y, por otro, potenciar las políticas preventivas entre las organizaciones para evitar tanto costosos rediseños de los sistemas una vez han sido desarrollados como posibles daños a su reputación e imagen por un tratamiento inadecuado de los datos personales.

Por otra parte, es necesario resaltar que la tendencia que se observa en las propuestas y recomendaciones de la Comisión Europea es la implantación obligatoria de esta herramienta, por lo que todos aquellos que comiencen a avanzar en su implantación, con la ayuda de la Guía, estarán en una buena situación cuando se concrete la obligatoriedad de las mismas.

Actividad internacional

En 2014 han continuado los procesos de actualización y modernización de algunos de los principales instrumentos internacionales de protección de datos que se iniciaron en años anteriores. En relación con el nuevo Reglamento General de Protección de Datos de la UE, la AEPD, como órgano independiente de la Administración del Estado, no asume la representación española en las discusiones que sobre este nuevo marco normativo se desarrollan en el Consejo.
No obstante, ha seguido, a lo largo de 2014, prestando asesoramiento y asistencia a los departamentos responsables en el marco de los mecanismos de coordinación que se han establecido para la tramitación de este paquete normativo, así como participando activamente en la preparación de las reacciones de las Autoridades de protección de datos de los Estados miembros de la UE, reunidas en el GT29, a estas iniciativas normativas.

Además, aunque su impacto directo en el derecho español de protección de datos sea aparentemente menor, no puede obviarse la importancia del segundo de los instrumentos europeos actualmente en proceso de revisión. Se trata del Convenio 108 del Consejo de Europa, cuya reforma se abordó al cumplirse los 30 años de su adopción en 1981.

La AEPD ha participado activamente en los trabajos de revisión del Convenio desde sus inicios en 2011 y, específicamente en un comité ad hoc (CAHDATA) creado al efecto, que ha elevado ya una propuesta de texto al Comité de Ministros.

Finalmente, hay que resaltar la participación de la AEPD en todas las actividades del GT29 y, obviamente, de forma muy destacada, en todas las relativas a la Sentencia del caso Google c. AEPD y Costejaz sobre el “derecho al olvido”, mereciendo especial atención la aprobación de un documento que establece criterios comunes de interpretación y aplicación de la misma. Asimismo, se ha continuado con la actuación coordinada e iniciada en años anteriores en relación con la nueva política de privacidad de Google.

La Agencia ha mantenido su participación en el Grupo de Expertos en Conservación de Datos en Telecomunicaciones, auspiciado por la Comisión Europea y, junto con Alemania, Francia, Holanda y Reino Unido, en el Grupo de Expertos que, a propuesta de la Comisión Europea y en el marco del proceso dirigido a un eventual reconocimiento como país con nivel de protección adecuado, asesorará a las autoridades de la India en materia de protección de datos.

En el marco de los proyectos del programa marco de investigación FP7 de la Unión Europea, la Agencia ha participado con un papel asesor en el ámbito de la protección de datos en los proyectos CIRRUS y PACT, relacionados con la certificación en el ámbito de la computación en nube y en el estudio de la percepción pública del uso de nuevas tecnologías en seguridad, respectivamente.

Finalmente, es necesario hacer una referencia particular a la participación de la Agencia en las tareas del Grupo Internacional de Protección de Datos en las Telecomunicaciones, conocido como Grupo de Berlín y la incorporación de la misma a los trabajos del Privacy Risk Framework Project Workshop, que pretende analizar el papel que la noción de riesgo puede desempeñar en el diseño y la ejecución de políticas de privacidad en las organizaciones. También es obligado señalar la labor de la AEPD en la Red Iberoamericana de Protección de Datos (RIPD), de la que fue fundadora y de la que ostenta la secretaría general y, en particular, sobre los temas tratados en el XII Encuentro Iberoamericano de Protección de Datos celebrado en la ciudad de México en noviembre de 2014 por la relevancia de los temas sobre privacidad e internet que en el mismo se abordaron incluyendo el derecho al olvido, las transferencias internacionales y el impacto de las nuevas tecnologías como big data o internet de las cosas en la protección de datos personales.

4 | 3 | 5 La sociedad civil

En nuestro país debe destacarse la presencia de un amplio elenco de organizaciones que desarrollan tareas directa o indirectamente relacionadas con distintos ámbitos de la privacidad. La narración de su actividad resultaría extensísima.

No obstante resulta fundamental destacar la pujanza del tejido social y la existencia de muy distintas iniciativas que mantienen en el primer plano del debate público la agenda de la privacidad bien en alguna de sus distintas manifestaciones, -la seguridad[21], los derechos de los usuarios[22], el derecho de Internet[23], la protección de los menores[24], - bien desde una perspectiva global y profesional[25].

[21]ISACA, con capítulos en Barcelona, Valencia y Madrid (http://www.isaca.org/spanish/Pages/default.aspx)
ISMS-Forum, que integra a su vez el Data Privacy Institute. (https://www.ismsforum.es/)

[22]Asociación de Usuarios de Internet (http://www.aui.es/) - Asociación de Internautas (http://www.internautas.org/) - Asociación de usuarios de la comunicación (www.auc.es/)

[23]Asociación Española de Derecho del Entretenimiento (http://denae.es/).
ENATIC-Abogacía Digital (http://www.enatic.org/).

[24]Padres 2.0 (http://padres20.org/).
Pantallas Amigas (http://www.pantallasamigas.net/)

[25]Asociación Profesional Española de Privacidad (http://www.apep.es/).

4 | 4 El futuro de la privacidad

El derecho a la protección de datos personales nace como reacción al impacto de una tecnología, la cámara fotográfica, capaz de obtener información sin la participación del afectado y ha sido históricamente permeable al influjo de la evolución tecnológica. La informática, y posteriormente Internet fueron fundamentales para su concepción como control sobre la información, y la aparición de la llamada libertad informática, habeas data y autodeterminación informativa y su consolidación en el derecho fundamental a la protección de datos.

La privacidad no sólo es sensible a la innovación tecnológica sino que está llamada a erigirse en su sustrato jurídico básico. En las tecnologías emergentes se da una relación altamente compleja respecto del derecho a la vida privada. De un lado, para su funcionamiento y rentabilidad resulta esencial el tratamiento de grandes volúmenes de información no sólo desde un punto de vista cuantitativo sino esencialmente cualitativo, con el consiguiente impacto en este derecho. De otro, la integración de la privacidad en el diseño y la asunción de este valor como requisito previo indispensable constituyen un elemento fundamental para la garantía del entero sistema de derechos fundamentales.

Garantizar la privacidad constituirá no sólo una precondición para ganar la seguridad y confianza de los usuarios. De hecho podría decirse que el funcionamiento democrático de la sociedad de la información dependerá en gran medida de la garantía de la vida privada.

4 | 4 | 1 Big data (gestión de la Inteligencia Colectiva)

Big Data ha llegado para quedarse. En 2011 McKinsey se refería a esta tecnología como la próxima tecnología para la innovación, la competitividad y la productividad[26] A título de ejemplo, la misma compañía explica cómo Big Data revolucionará la investigación de la industria farmacéutica[27]. El universo de datos disponible crece, las fuentes se multiplican, y con ello las rigideces vinculadas a conjuntos de datos limitados desaparecen. Acelerar los procesos de decisión basados en datos generará nuevos modelos de investigación y nuevos procesos de descubrimiento, se asociará a nuevos sensores como los teléfonos inteligentes y las aplicaciones móviles y podrá afinar el foco a partir de evidencias obtenidas del mundo real, elevará la eficiencia de los ensayos clínicos y contribuirá a una mejor gestión del riesgo y la seguridad de los mismos.

Se ha definido Big Data como una suerte de estadística del todo. El significativo incremento de la capacidad de almacenamiento y proceso permiten tratar grandes Volúmenes de información, a partir de una gran Variedad de fuentes y con una gran Velocidad de proceso y decisión, las llamadas tres V.

Este futuro prometedor debe sin embargo convivir con el Derecho. Debe ser capaz de afrontar con éxito las prescripciones legales existentes y, singularmente, aquellas que regulan la garantía del derecho fundamental a la protección de datos. En este sentido se plantean distintas cuestiones.

- El uso de los llamados datos masivos interactúa con realidades en red, es funcional al complejo entramado en red que caracteriza no sólo a las redes sociales en todas sus dimensiones, sino también a múltiples fenómenos de orden físico.

- Uno de los resultados determinantes de este tipo de herramientas consiste en ofrecer algo más que los datawharehouse, o los sistemas de bussiness intelligence, no ofrece resultados estáticos, es capaz de proporcionar patrones dinámicos. Y ello tanto para identificar tendencias, como desviaciones.

- Big data no sólo mira al pasado se asocia a predictibilidad y apunta al futuro.

[26]Véase http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

[27]Véase http://www.mckinsey.com/insights/health_systems_and_services/how_big_data_can_revolutionize_pharmaceutical_r_and_d

Por todo ello, tanto la obtención de determinados resultados o patrones, como sobre todo su aplicación pueden generar dudas esenciales de índole ética y jurídica. En materia de privacidad el elemento fundamental residirá en la aplicabilidad de las normas sobre protección de datos personales. En principio, la Directiva, y las leyes nacionales de transposición permiten eludir estas obligaciones mediante la anonimización, puesto que ello excluye la presencia de datos de carácter personal.

Sin embargo, el Dictamen 5/2014 del Grupo de Trabajo del artículo 29 de la Directiva (GT29) muestra que ésta no es una operación ni tan sencilla, ni precisamente banal. En esencia la anonimización desde un punto de vista material exige:

- Que no pueda ser establecido vínculo alguno entre el dato y su titular sin un esfuerzo desproporcionado.
- Que sea irreversible.
- Que en la práctica sea equivalente al de un borrado permanente.

El problema reside en que no existe un estándar comúnmente aceptado y seguro. Desde un punto de vista jurídico para el GT29 estamos ante un tratamiento ulterior para el que sería necesario:

- Disponer de un fundamento que lo legitime, como por ejemplo el interés legítimo.
- Verificar la relación de compatibilidad entre la finalidad para la recogida inicial y un tratamiento posterior como la anonimización.
- Las expectativas del titular sobre usos posteriores.
- El impacto en el titular de los datos.
- Las cautelas adoptadas por el responsable para salvaguardar los derechos de los afectados.
- El deber de cumplir con el principio de transparencia.

Sin embargo, desde el punto de vista de la protección de datos personales en la anonimización existen riesgos cuando ésta no sea completa o adecuada y permita la reidentificación. Esto puede producirse por ejemplo por la persistencia de datos, por la posibilidad de reidentificar mediante inferencias, o por vinculación (link) con otros paquetes de datos personales. Por otra parte es fundamental no confundir pseudonimización y anonimización. Y, por si esto no fuera poco, ha de tenerse en cuenta que las autoridades de supervisión plantean la anonimización como una modalidad de "uso posterior" de los datos personales, afectado de lleno por nuestra legislación, según se desprende del artículo 2 de la LOPD.

Sin embargo, las cuestiones de privacidad que esta tecnología plantea van más allá de decidir si se aplica la legislación, e inciden en cómo las costuras de la privacidad se ven desbordadas de un modo significativo por los retos que de ella se derivan. En tal sentido, las principales categorías vigentes en materia de protección de datos pueden verse moduladas, bien por fenómenos preexistentes instrumentales a Big Data, bien por la propia influencia de este fenómeno.

En primer lugar, hay que referirse al dilema del consentimiento en Internet. El escenario más visible para el tratamiento de los datos personales es el de servicios aparentemente gratuitos cuyo modelo de negocio se basa, precisamente, en el tratamiento masivo de datos personales. Sus prestadores, gracias los avances tecnológicos en materia de análisis comportamental y predictibilidad, se erigen en los nuevos gurús capaces de predecir el comportamiento del consumidor, y de influir en su toma de decisiones.

Por otra parte, la garantía de la calidad de los datos será fundamental desde un doble punto de vista. De un lado, la fe en el resultado que ofrezca un determinado patrón no puede ser a día de hoy absoluta. Del otro, si en un contexto anterior la veracidad de los datos era muy relevante, ahora incluso que un determinado sujeto falsee sus preferencias puede aportar valor añadido al resultado.

Desde el punto de vista de la finalidad se produce un cambio significativo. Este principio comporta la cancelación de los datos cuando cesa la finalidad para la que se recabaron. Sin embargo ahora, aunque su sustrato material pueda quedar anticuado, la vida útil del dato no se agota con el uso: cualquier información es susceptible de ser reutilizada. Y lo que resulta más peculiar, la finalidad para la que la información fue recogida, si bien puede ser determinante desde un punto de vista jurídico, no lo es en absoluto desde un punto de vista práctico, ante el potencial del Big Data para obtener resultados inesperados, y en ocasiones no buscados. Por tanto, el concepto de finalidad puede verse por completo alterado, no ya durante el uso o respecto la información trasladada a los usuarios al requerir su consentimiento, sino ante el riesgo de alcanzar resultados inesperados.

Por otra parte, esta tecnología obliga a reconsiderar la sensibilidad de los datos y la categoría de los datos especialmente protegidos. Primero, dada la profundidad de análisis que proporcionan las técnicas de Big Data, puede bastar con trazar a un sujeto en una red social, o en el uso de una aplicación móvil, para obtener resultados relevantes. Segundo, porque hay datos como la geolocalización, las interacciones en redes sociales, el análisis semántico de expresiones emocionales, los hábitos sociales o el Internet de las cosas, que pueden aportar información relevante susceptible de ser usada con fines discriminatorios. Y también con fines de control social y policial.

Esta complejidad convive con el carácter estratégico que puede tener Big Data para desarrollo de la economía digital. Por ello, el reto determinante para la privacidad residirá en que seamos capaces de encontrar modelos de cumplimiento normativo susceptibles de ser a la vez soporte para la innovación y garantía de los derechos del individuo, tanto respecto de su información personal como frente a la toda posible capacidad en el manejo de las preferencias sociales e individuales.

4 | 4 | 2 Internet de las cosas

La evolución de Internet en el último lustro ha ido indisolublemente unida al incremento de los periféricos capaces de conectarse en la red. No sólo se trata de la revolución de las tabletas y de los teléfonos inteligentes sino de un fenómeno más profundo. Videocámaras, sistemas de gestión logística que suman el potencial de trazabilidad que proporcionan las etiquetas de identificación por radiofrecuencia, electrodomésticos de todo tipo asociados a la gestión domótica del hogar, sensores distribuidos por toda la ciudad, tecnología ponible… Prácticamente cualquier objeto capaz de albergar un chip y conectarse a una red física o inalámbrica podría formar parte del universo del Internet de las cosas (o, por sus acrónimo en inglés, IoT).

Las aplicaciones de IoT son amplísimas y su potencial de crecimiento enorme. Por ejemplo, Mckinsey lo ha estimado en 6.2 billones de dólares en 2025[28]. En este sentido, en entrevistas a esta entidad los expertos[29] subrayan como IoT pone los objetos, "el producto" en el centro de la cadena de valor, ya que le permite comunicar información directa a los gestores: el producto deja de ser mudo, pasa a ser un protagonista que proporciona información.

En otro estudio Pew Research Center[30] destaca como la próxima revolución digital vendrá de la mano de la computación embebida y la tecnología ponible. Entre los ejemplos de IoT se citan sensores subcutáneos, aplicaciones móviles de control remoto para la gestión domótica de electrodomésticos calefacción, etc., sensores urbanos de todo tipo ya sea directos ya sea a través de los propios usuarios como la gestión del tráfico vinculada a los GPS de los conductores, sensores en carreteras e infraestructuras de todo tipo, vinculados a cadenas logísticas, e incluso al papel higiénico en baños públicos.

Podría afirmarse casi con toda certeza que en 2005 cualquier cosa capaz de comunicarse a través de Internet y aportar algún tipo de valor añadido estará conectada aportando información de todo tipo en tiempo real. Una frase-eslogan de una conocida empresa indisoluble de la conectividad ejemplifica con precisión este fenómeno «Hoy en día, más del 99% de las cosas, en el mundo físico, aún no están conectadas a Internet. Un fenómeno llamado "The internet of Everything" despertará todo lo que usted puede imaginar».

[28]The Internet of Things: Sizing up the opportunity, Disponible en http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity

[29]James Heppelmann. How the Internet of Things could transform the value chain. Disponible en http://www.mckinsey.com/insights/high_tech_telecoms_internet/how_the_internet_of_things_could_transform_the_value_chain

[30]The Internet of Things Will Thrive by 2025. Disponible en http://www.pewinternet.org/2014/05/14/internet-of-things/

IoT coincide en el tiempo y se retroalimenta de tres líneas de evolución cruciales para la sociedad de la información como son la computación en la nube, el Big Data y las ciudades inteligentes. Las bases tecnológicas que han hecho posible la miniaturización de los dispositivos de conexión se encontraban bien establecidas por Gordon Moore desde 1968, y no han hecho sino maximizarse gracias a la ingeniería de los materiales y la nanotecnología. La Nube proporciona un modelo flexible y ubicuo de almacenamiento y gestión de la información que elimina las restricciones físicas. De algún modo se difuminan las barreras entre bits y átomos con las que Negroponte explicaba en su día la sociedad de la información. Los átomos, "el hierro", ya no son una barrera, no es necesario contratar un servidor adicional. El almacenamiento y el procesado se convierten en un mero suministro, en una utility accesible en tiempo real que incluso se puede obtener contratando en régimen de subasta en un mercado global.

Por su parte, Big Data aporta la inteligencia y multiplica el valor añadido de la información obtenida por los sensores, combina lecturas distintas, establece correlaciones imposibles y alcanza conclusiones impensables. Sin Big Data el fenómeno IoT probablemente se hubiera producido de idéntico modo ya que proporciona soluciones estratégicas funcionales a la gestión de dispositivos en un mundo hiperconectado. Pero con Big Data el internet de las cosas se enfrenta al salto cualitativo de la "inteligencia".

Por último, las ciudades inteligentes se erigirán en el crisol en el que todos los elementos anteriores se recombinan y alcanzan su máxima expresión. La Internet de las cosas permitirá disponer de ciudades más habitables y probablemente ecológicamente sostenibles. Pero ello exigirá el manejo de ingentes volúmenes de información, mucha de la cual impactará de modo directo en la esfera de la personalidad. La gestión del tráfico exige poner en un mapa a cada conductor, y la prevención identificar a aquellos potencialmente peligrosos. La gestión ambiental puede suponer que el municipio conozca cuanta electricidad consumimos, -y con ello hábitos incluso íntimos-, o que tipo de residuos generamos y con qué frecuencia. La frontera entre la ciudad "gestionada" y la ciudad "vigilada" podría difuminarse.

Esta compleja realidad plantea cuestiones de primer orden desde el punto de vista de la privacidad. Como punto de partida, es fundamental recordar como, prácticamente desde su primera definición, un dato de carácter personal se concibe como una información relativa a una persona identificada o identificable. Por otra parte, es esencial entender como el concepto dato, en realidad, abarca cualquier cualidad predicable de un sujeto. Incluso partiendo de las ya "ancianas categorías" formuladas por nuestro Tribunal Constitucional en la STC 292/2000, es necesario subrayar que el derecho fundamental a la protección de datos tutela frente a la capacidad de incidir en la esfera privada de las personas, mediante el tratamiento de cualquier información pública o privada.

Por ello, IoT debe ser abordada con mucha cautela desde el punto de vista de la privacidad en al menos tres dimensiones: su diseño, el tratamiento de datos personales y la finalidad, y finalmente la seguridad de los dispositivos.

En este sentido constituye un ejemplo muy gráfico uno de los primeros impactos en la privacidad que se produjo con la aparición de las videocámaras conectadas a través del protocolo TCP/IP. Mediante una inspección sectorial de oficio la Agencia Española de Protección de Datos[31] constató en 2009 la presencia de cámaras gestionables desde Internet que permitían un acceso remoto a través de la Red al visionado de las imágenes en tiempo real. La Agencia destacó los siguientes puntos:

- Se ha detectado que parte importante de estas cámaras carecen de controles de acceso y captan y difunden imágenes de personas identificables en la vía pública, el lugar de trabajo o en el interior de establecimientos comerciales.
- Se ha comprobado que la visualización de las imágenes captadas puede hacerse desde cualquier ordenador conectado a Internet, y en algunos casos se permite incluso manejar remotamente la cámara y grabar las imágenes.
- Se han iniciado 7 procedimientos sancionadores, a particulares y a empresas por la captación de imágenes de personas identificables accesibles a cualquier usuario en Internet.
- El plan alerta de que el riesgo de acceso por parte de intrusos es muy elevado debido a la existencia de buscadores que, al rastrear periódicamente la Red, proporcionan mecanismos de búsqueda muy eficaces.

[31] Disponible en https://www.agpd.es/portalwebAGPD/canaldocumentacion/recomendaciones/common/pdfs/plan_sectorial_camaras_internet_2009.pdf

Este ejemplo pone de manifiesto como el uso masivo de una tecnología que funciona en el marco del Internet de las cosas puede generar riesgos para la privacidad. Sistemas de esta naturaleza pueden rendir enormes beneficios, por ejemplo permitiendo su control remoto desde centrales de alarmas, reduciendo los costes de personal, o incluso combinados con sensores de movimiento advertir de intrusiones en tiempo real. Sin embargo, no contemplar los elementos esenciales las convierte en herramientas cuyo diseño es inadecuado, susceptibles de ser usadas para finalidades indebidas, o simplemente inadecuadas, y particularmente vulnerables a las intrusiones.

Por ello el primer reto al que debe enfrentarse el internet de las cosas, como señala el Grupo de Trabajo del artículo 29[32], es al de adoptar estrategias de privacidad en el diseño. Y esta técnica debe aplicarse en sentido amplio, ya que los agentes concernidos pueden ser muy variados. No se trata únicamente del proveedor del dispositivo y el usuario final: existen múltiples agentes que deben ser considerados. Así, si la gestión del dispositivo requiere por ejemplo de una aplicación móvil, el acceso a datos se multiplica e incorpora al proveedor del sistema operativo, al de la aplicación móvil e incluso a terceros a los que los datos se ceden, anonimizados o no, y anunciantes que interactúan con la App. Y no sería obviamente este el único supuesto: en muchos casos habrá que contar con sujetos como el productor del dispositivo o el vendedor del mismo, interesados respectivamente en monitorizar el funcionamiento o establecer perfiles y hábitos del comprador.

En segundo lugar, en Internet de las cosas la ineludible relación entre las nociones de finalidad-transparencia-consentimiento no puede ser obviada. Y con toda seguridad planteará importantes retos de diseño. El usuario de cualquier objeto conectado a Internet debería saber en todo momento qué datos se van a tratar, para qué finalidad y qué tipo de terceros puede acceder a esa información. Pero a esta manifestación clásica de los principios de protección de datos se unen nuevas necesidades. De una parte, la transparencia debe alcanzar al empleo de datos en el universo Big Data desde al menos dos puntos de vista. Primero, respecto del establecimiento de patrones de conducta, su uso y su repercusión en la esfera de privacidad del individuo.
En segundo lugar, fenómenos como el de las ciudades inteligentes obligarán a redimensionar las estrategias de transparencia, y a buscar metodología de información al usuario, al consumidor y al ciudadano, que sean capaces de transmitir con claridad no solo qué se va a hacer con sus datos sino también la confianza en que el tratamiento será legítimo y adecuado.

Por último, la garantía de la seguridad adquiere un valor crucial a la vista de las noticias sobre espionaje masivo publicadas en el último año. En realidad el usuario reclamará del proveedor algo bastante más obvio: debe garantizar que sus dispositivos son seguros frente a intrusiones. Pero además, debe asegurar que no le abre las puertas a cualquier tercero, y singularmente al Estado. En el desarrollo del Internet de las cosas en España se jugará seguro un elemento de desarrollo de nuestra economía digital.
Y en este diseño la garantía de la privacidad debe operar como un requerimiento de primer orden para que el universo IoT contribuya a una sociedad mejor en lugar de una sociedad vigilada.

[32]Opinión 8/2014 on the on Recent Developments on the Internet of Things. Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

4 | 4 | 3 Seguridad y privacidad en la era Snowden

La relación de privacidad y seguridad se encuentra sin duda en la génesis de las primeras leyes de privacidad. La evolución del derecho a la vida privada como derecho constitucional en EE.UU se encuentra históricamente vinculada a la garantía de los derechos de la Cuarta Enmienda, en relación con las entradas y registros policiales.

En el contexto europeo, la garantía frente a la acción estatal inspiró leyes y constituciones, y singularmente la española. Aunque resulte anecdótico, la primera ley española en la materia, -la LORTAD-, se aprobó al ser requisito contar con una norma de esta naturaleza para ratificar el Acuerdo de Schengen.

En el periodo 2013-2014 y en los primeros meses de 2015 dos acontecimientos han puesto sobre la mesa de nuevo la necesidad de cohonestar dos valores no necesariamente excluyentes. Por un lado, las revelaciones por Edward Snowden[33] sobre la vigilancia masiva sobre Internet de la inteligencia norteamericana han puesto en cuestión la confianza de los ciudadanos de todo el planeta sobre la seguridad, confiabilidad y privacidad de las comunicaciones. De otro, los atentados contra Charlie Hebdo, y una serie de pequeños atentados realizados o frustrados en el entorno de las bases del terrorismo Yihadista en Europa han reactivado en el seno del Consejo de la Unión Europea el debate sobre los medios de investigación y control.

El caso Snowden comportó la constitución prácticamente inmediata de una comisión de investigación en el seno de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) del Parlamento Europeo[34]. Las tareas de la Comisión han finalizado con la Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior[35].

[33]Véase el periódico “The Guardian”, NSA Files. Decoded. Disponible en http://www.theguardian.com/us-news/the-nsa-files

[34]Véase LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens. Disponible en http://www.europarl.europa.eu/committees/es/libe/subject-files.html?id=20130923CDT71796

[35]Disponible en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//ES

En sus conclusiones la Comisión LIBE, además de considerar la necesidad de que la legislación norteamericana ofrezca mayores garantías, pone en cuestión la licitud de las transferencias internacionales de datos personales a EE.UU. Y lo hace tanto en el contexto de la cooperación policial, en el marco del Acuerdo de Puerto Seguro, en relación con países terceros como Nueva Zelanda, Canadá y Australia en tanto que colaboradores con los Estados Unidos en la vigilancia masiva a gran escala de comunicaciones electrónicas y en el programa denominado «Cinco Ojos», y las relacionadas con los acuerdos, TFT, sobre pagos financieros, y PNR, sobre registro de pasajeros en transportes aéreos. Por otra parte, el Comité manifiesta sus sospechas respecto de los servicios de Cloud señalando que «en virtud de los acuerdos de servicios en nube con los principales proveedores estadounidenses de servicios en nube, las actividades de vigilancia masiva proporcionan a las agencias de inteligencia acceso a los datos personales almacenados o tratados de otra forma por los ciudadanos de la UE».

En sede de conclusiones y recomendaciones el Comité cuestiona profundamente el Estado de cosas. Probablemente su conclusión número 10 es la que expresa mejor el sentido general del Informe LIBE:

> **10.**Condena la recopilación generalizada extensa y sistemática de los datos personales de personas inocentes que, a menudo, incluyen información personal íntima; enfatiza que los sistemas de vigilancia masiva indiscriminada por parte de los servicios de inteligencia constituyen una seria injerencia en los derechos fundamentales de los ciudadanos; destaca que la intimidad no es un lujo, sino la piedra angular de una sociedad libre y democrática; señala, asimismo, que la vigilancia masiva repercute de manera potencialmente grave en la libertad de prensa, de pensamiento y de expresión y en la libertad de reunión y asociación, e implica un potencial significativo para el uso abusivo de la información recogida contra adversarios políticos; enfatiza que estas actividades de vigilancia masiva también implican acciones ilegales por parte de los servicios de inteligencia y plantean interrogantes por lo que se refiere a la extraterritorialidad de las legislaciones nacionales.

Como coralario lógico el Comité pide «a las autoridades estadounidenses y a los Estados miembros de la UE que aún no lo hayan hecho que prohíban las actividades de vigilancia masiva generalizada». Así como acciones muy concretas como solicitar a la Comisión medidas que prevean la suspensión inmediata de la Decisión 2000/520/CE de la Comisión, que establecía la adecuación de los principios de puerto seguro relativos a la protección de la intimidad, y de las preguntas más frecuentes relacionadas emitidas por el Departamento de Comercio de los Estados Unidos, que evalúe en profundidad del Acuerdo de Asistencia Judicial con EE.UU., y la suspensión y/o revisión de los acuerdos TFT y PNR. Por último, considera que la aprobación de la totalidad del paquete de protección de datos permitirá que los ciudadanos de la UE puedan disfrutar de un nivel elevado de protección de sus datos en un futuro muy cercano ya que «son necesarios para proteger los derechos fundamentales de las personas».

En esta materia el Grupo de Trabajo ha publicado su opinión en dos documentos de trabajo titulados respectivamente «Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes»[36] y «Document on surveillance of electronic communications for intelligence and national security purposes»[37]. Ambos documentos proponen el siguiente conjunto de medidas:

[36]Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_es.pdf

[37]Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf

a Mayor transparencia

1. Es necesaria una mayor transparencia sobre el funcionamiento de los programas y sobre lo que hacen y deciden las autoridades de control.
2. Una mayor transparencia por parte de los responsables del tratamiento de los datos.
3. Aumentar al máximo la sensibilización de la población.

b Supervisión más significativa

1. Mantener un sistema jurídico coherente para los servicios de inteligencia que incluya normas en materia de protección de datos.
2. Garantizar la supervisión efectiva de los servicios de inteligencia.

c Aplicación efectiva de la legislación vigente

1. Observar las obligaciones de los Estados miembros de la UE y de las Partes en el CEDH en materia de protección de los derechos relativos al respeto de la vida privada y a la protección de datos personales.
2. Los responsables del tratamiento de datos sujetos a la jurisdicción de la UE deben cumplir la legislación de protección de datos de la UE.

d Mejora de la protección a nivel europeo

1. Adopción del paquete de reformas de la protección de datos.
2. Precisar el ámbito de aplicación de la excepción por motivos de seguridad nacional.

e Protección internacional para los residentes en la UE

1. Insistir en salvaguardias adecuadas en lo relativo a la comunicación de datos de inteligencia.
2. Negociar acuerdos internacionales a fin de conceder garantías adecuadas de protección de datos.
3. Fomentar un instrumento mundial de protección de la vida privada y de los datos personales.

Por otra parte, el crecimiento del terrorismo yihadista ha llevado a plantear la mejora de los instrumentos al servicio de las Fuerzas y Cuerpos de Seguridad, e incluso en el caso español, la reivindicación de una mayor colaboración por parte de las redes sociales. En este debate, la cuestión central estriba en cómo resolver la compleja ecuación de facilitar la labor policial garantizando las libertades. Una monitorización global del mundo online y las comunicaciones no resulta ni jurídica, ni política ni materialmente defendible. Pero a la vez, la garantía de la seguridad y de nuestro modelo de libertades exige proveer de herramientas de prevención, investigación y reacción eficientes.

Por ello, y desde el punto de vista de la privacidad resultan recomendable el establecimiento de frenos y contrapesos que ofrezcan garantías a las personas. Además cuando se trate de obtener datos personales por medios tecnológicos podría ser conveniente integrar algunas garantías jurídicas en nuestro sistema. Ello comporta necesariamente un reforzamiento de la normativa y su actualización tanto en lo que afecta a lo arriba definido como “paquete de protección de datos” como a la regulación procesal del secreto de las comunicaciones.

La evolución de la normativa incorpora obligaciones de documentación, y procedimientos como los análisis de impacto en la protección de datos (también conocidos por su acrónimo en inglés, PIA) obligatorios, cuya aplicación en el ámbito policial favorecería el control jurídico de los tratamientos. Y lo mismo sucede con el nombramiento de garantes internos en esta materia, llámense o no “delegados de protección de datos”, sin renunciar en ningún caso al control judicial. Podrían existir otras herramientas jurídicas como la obligación de realizar PIAs y/o auditorías o informes anuales de actividad, susceptibles de ser revisados por las Cortes Generales, el Defensor del Pueblo o la Agencia Española de Protección de Datos. Y ello sin perjuicio de la tutela administrativa o judicial de los derechos de las personas.

Es obvio que para la investigación policial se requiere tratar información personal. Pero si realmente como parece caminamos hacia una sociedad vigilada en nombre de la democracia, tal decisión debería tomarse de modo muy meditado en los planos tecnológico o jurídico y poniendo el acento en las garantías. Cualquier otra opción podría ser peligrosa para la misma libertad que todos deseamos defender.

Capítulo 5

Identidad en red de niñ@s y jóvenes

Coordinación: **Ana Moreno**

Editores/Autores: **Maialen Garmendia** (Epígrafe 1), **Lorena Rivera** (Epígrafe 2) **Ana Moreno** (Epígrafes 3, 6, 7), **Carlos Represa** (Epígrafe 4), **Alberto Urueña** (Epígrafe 5.1), **Mª Angustias Salmerón Ruiz** (Epígrafe 5.2), **María José Cantarino** (Epígrafe 6)

Grupo de Trabajo:

Maite Arcos Sánchez (Directora de Relaciones Institucionales/ Orange)

María José Cantarino de Frías (Jefe de Innovación Sostenible/ Telefónica)

Maialen Garmendia (Profesora de la Universidad del País Vasco/ EHU - EU Kids Online)

Ana Moreno (Profesora del Departamento Organización, ETSII- Universidad Politécnica de Madrid)

Carlos Represa Estrada (Director General del Instituto para la Competencia Digital)

Lorena Rivera Novillo (Investigadora colaboradora en Syntagma)

Ángel Sallé (Enred Consultoría)

Mª Angustias Salmerón Ruiz, (Coordinadora del grupo TIC de la Sociedad Española de Medicina del Adolescente. Pediatra de la Unidad de Medicina de la Adolescencia del Hospital Universitario La Paz. Pediatra de la unidad de TIC del Hospital Ruber Internacional)

Alberto Urueña (Subdirector Adjunto de Estudios/ Red.es)

Antonio Vargas (Senior Policy Analyst / Google)

5 | 1 Marcos de referencia para analizar los retos y oportunidades de niños y jóvenes en la red

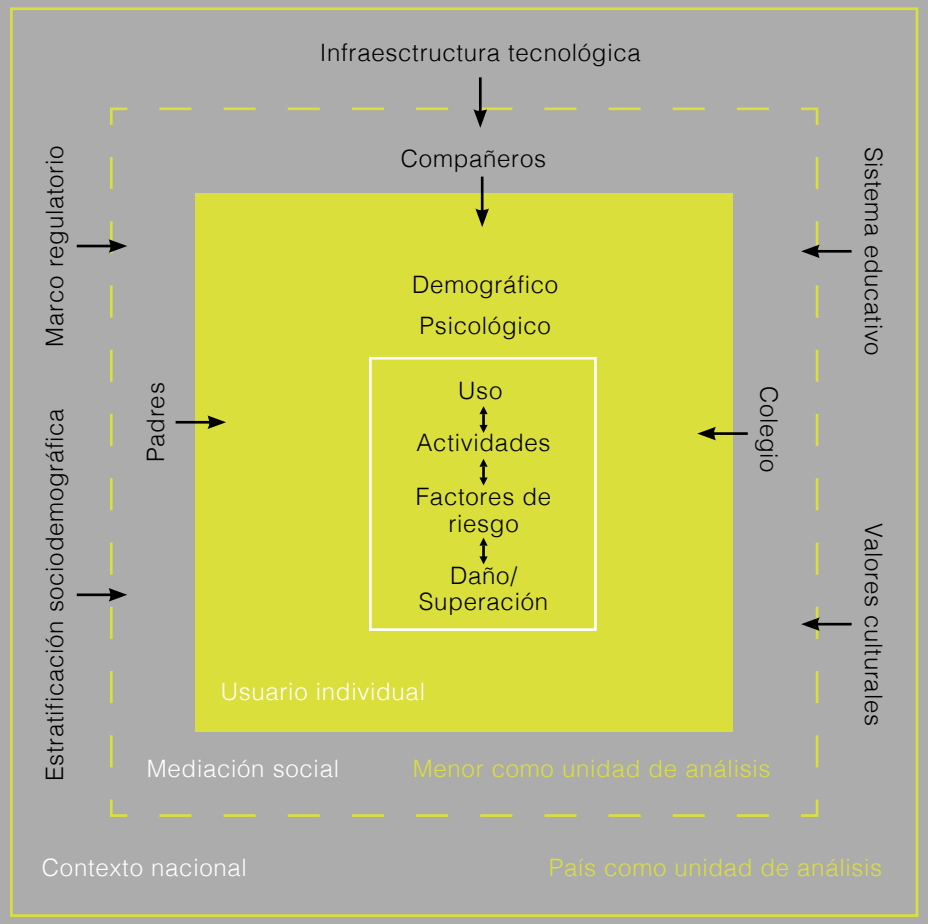
El análisis de los riesgos y oportunidades que las experiencias online pueden proporcionar a los niños y jóvenes requiere, en primer lugar, la contextualización de las actividades que ellos desarrollan, ya que éstas no son por sí mismas "beneficiosas" o "dañinas". El tipo de calificación asignado a una actividad no proviene de la actividad realizada sino de su resultado. Evidentemente, ciertas actividades tenderán a ser beneficiosas (ej. hacer las tareas escolares), mientras otras serán negativas (ej. acosar a sus iguales). Sin embargo, el carácter de muchas otras no estará tan claro (ej. descargas de música o hacer nuevos amigos online).

No podemos obviar que cuando los menores se conectan a internet lo hacen en un entorno particular. Se conectan a determinados servidores que tiene su propio carácter. Algunos tipos de contenidos pueden ser más fácilmente accesibles que otros. Muchas otras personas están también online y la actividad de éstas puede influir sobre la de los menores. Todos estos "elementos ambientales" interactúan con las actividades de los menores y contribuyen a conformar sus experiencias online. La gráfica 1 muestra los factores externos que influyen sobre las experiencias de los niños y jóvenes. Básicamente, se pueden diferenciar tres niveles de influencia al trazar la secuencia entre el uso de internet y las consecuencias que se puedan derivar del mismo:

1. El contexto nacional: en el que intervienen una gama de factores relacionados con la estructura socio-económica, el marco legal, la infraestructura tecnológica, el sistema educativo y los valores culturales. En este nivel los grupos de interés responsables podríamos denominarlos grupos de interés institucionales.

2. La mediación social: relacionada con el tipo de uso de internet que se promueve entre los menores así como con la supervisión de ese uso. En este nivel destacan tres grupos de actores: los padres y madres, las instituciones educativas –principalmente el profesorado- y las amistades de los menores. En este nivel los grupos de interés relevantes podríamos denominarlos grupos de interés del entorno cotidiano.

3. El usuario individual: que tiene unas características demográficas determinadas como son su edad y género, su estatus socio-económico y factores psicológicos como por ejemplo problemas emocionales, o la tendencia a correr riesgos.



Gráfica 1: Relación entre uso, actividades y factores de riesgo online
Fuente: EU Kids Online, Livingstone et. al (2011)

En suma, todos estos elementos influyen en el uso que hacen los jóvenes de internet condicionando la probabilidad de que su resultado sea beneficioso o dañino para ellas y ellos. Por ejemplo, es evidente que un niño o niña de 10 años en Reino Unido u Holanda tendrá mayores facilidades de acceder a internet –desde su hogar y/o entorno escolar, y de encontrar contenidos adecuados a su edad e intereses. Del mismo modo que a medida que aumenta la edad de los menores tienden a tener más habilidades para bloquear mensajes o configurar su privacidad en internet, aspectos todos ellos que inciden en el resultado del uso de internet.

Además de tener en cuenta el contexto, también es necesario focalizar la atención sobre los diversos tipos de uso y las consecuencias que se puedan derivar los mismos. Tal y como muestra la gráfica 2, determinados usos les proporcionan oportunidades para el desarrollo de relaciones sociales, las actividades de ocio o el aprendizaje, mientras otros tienden a tener efectos negativos.

La posibilidad de comunicarse con sus amistades y de ampliar ese círculo a personas con quienes se comparten intereses y/o aficiones, así como la de participar en juegos, constituye una oportunidad para el desarrollo de la identidad de los jóvenes. Asimismo, internet puede también ofrecer inmejorables oportunidades para el aprendizaje.
Sin embargo, no podemos obviar que para que los niños y jóvenes puedan optimizar estas oportunidades es necesaria la incorporación de las TIC en su currículum de forma transversal para que puedan llegar a ser ciudadanos activos, críticos y creativos. De lo contrario, puede ocurrir que los usos para el aprendizaje se limiten al “corta y pega” y carezcan de las competencias para discriminar la información relevante de aquella que no lo es. Entre los posibles usos negativos, algunos están relacionados con la privacidad. Ésta es muy valorada por los y las jóvenes. Sin embargo, lamentablemente, no siempre la gestionan correctamente. Ya que muchos de ellos muestran una tendencia manifiesta a comunicar sus inquietudes, estados de ánimo, y actividades de tiempo libre -ilustrándolas con abundantes fotografías- a sus numerosos amigos en las redes sociales o aplicaciones.

Uso	Reto	Dimensión		
		Relaciones sociales	**Ocio**	**Aprendizaje**
Positivo	No perder estas oportunidades	• Contacto más amplio (compartir gustos, aficiones, enlaces… • Contacto con más personas.	• Juegos en red • Juegos educativos, de habilidades	• Acceso a mayor número de recursos multimedia, y con mayor calidad • Entorno equiparable al laboral, trabajo cooperativo • Talento extendido por la tecnología
Negativo	Evitar esas consecuencias negativas	• Uso excesivo • Superficialidad en las relaciones • Pérdida de privacidad • «No olvido» • Ciberacoso • Aislamiento de padre/madre • “Malas compañías” • Acceso a contenidos/ comunidades perjudiciales (drogas, sexo, anorexia)	• Juegos inadecuados • Uso excesivo • Descargas ilegales • Juegos de pago	• Dispersión de la atención • Copia y “mínimo esfuerzo” • Contenidos inadecuados (racismo, sexo, incitación al odio)
Delictivo (ajeno)	Prevenir estos delitos	• Contactos no deseados • Violación de la privacidad • Extorsión • Pederastia	• Compras sin control • Estafas económicas	

Gráfica 2: Usos de niños y niñas y jóvenes en la red
Fuente: Mesa Niñ@s y jóvenes en Internet, 2011, Documento de posición, Congreso IGF España 2011.

Para ellos “saber mostrarse” en internet es un valor indiscutible, y generalmente, no son conscientes de las consecuencias negativas que para ellos puede tener mostrar su intimidad. Para la mayoría captar una foto y enviarla en cuestión de segundos, es un impulso inconsciente y la foto enviada es ya irrecuperable. No perciben que los “amigos de amigos” que incluyen entre los numerosos contactos de su perfil no son necesariamente sus amigos y este tipo de información puede hacer que sean más vulnerables y lleguen a ser, en algunos casos, víctimas de acoso o ciberbullying que según las evidencias es el riesgo más dañino de todos.

Además, el uso combinado de diversos dispositivos de acceso a internet les proporciona una conectividad permanente, con el consiguiente riesgo de caer en el uso excesivo. También hay retos que atender relacionados con el acceso a información inexacta. Algunos de los jóvenes son conscientes de la necesidad de limitar su uso del Smartphone, pero hay también quienes sienten ansiedad cuando no lo tienen “a mano”. Por último, cabe la posibilidad de que los jóvenes sean objeto de usos delictivos protagonizados por terceras personas como estafas económicas, suplantación de la personalidad o extorsión.

Ante estos riesgos, la prevención requiere también medidas de carácter educativo (por parte de los padres, madres y educadores) que proporcionen a los menores las habilidades y el apoyo necesarios para afrontar tales situaciones de manera que les ocasionen el menor daño posible.

5 | 2 Principios para la protección de la infancia. Categorización de riesgos

Antes de empezar, hay que situar el texto en su propio ámbito, en el de riesgos existentes. Es posible que al hablar sólo de los riesgos, se pueda mostrar internet como una fuente inagotable de peligros, por lo que es necesario dejar constancia que, hoy en día, internet, además, es una herramienta imprescindible y ofrece múltiples oportunidades.

5 | 2 | 1 Derechos fundamentales de la infancia en internet

Existe una relativamente amplia regulación de los derechos de los menores, todos ellos basados en el instrumento internacional más importante relativo a este tema, la Convención de las Naciones Unidas sobre los Derechos del Niño, que tiene su reflejo, en nuestro ordenamiento jurídico, en la Ley Orgánica 1/1996, de 15 de enero, de protección jurídica del menor, de modificación del Código Civil y de la Ley de Enjuiciamiento Civil.

Dentro del elenco de derechos reconocido a los menores, podemos destacar, de forma resumida, por su relación estrecha con el uso de internet por parte de estos, los siguientes:

- Libertad de expresión, derecho a buscar, recibir y difundir informaciones e ideas.
- Protección de su propia imagen, intimidad personal y familiar y honor.
- Protección al niño contra toda información y material perjudicial para su bienestar.
- Protección contra todas las formas de explotación y abuso sexuales.

5 | 2 | 2 Riesgos: Categorización

A pesar del reconocimiento de estos derechos, existen, en Internet, situaciones de riesgo hacen que la protección de los menores no sea del todo efectiva. Para clasificar estos riesgos en la red para los menores, se seguirá el esquema propuesto por la ponencia conjunta de estudio sobre los riesgos derivados del uso de la Red por parte de los menores, constituida en el seno de la Comisión conjunta de las Comisiones de Interior, de Educación y Deporte, y de Industria, Energía y Turismo, y publicada el 3 de octubre de 2014, en el Boletín Oficial de las Cortes. Acompañándolo, además, con datos de este último año para contextualizarlos.

Riesgos de internet

Son aquellos riesgos que existen únicamente debidos a internet, y que sin la existencia de este medio no podrían darse.

- Cambio en el modelo de comportamiento y comunicación de los menores.
- Adicción. Existe cierta alarma sobre la potencialidad de los niños y jóvenes españoles a sufrir adicción a internet (que ocurre cuando el menor pierde el control sobre su uso). En los países asiáticos este problema ya se ha desarrollado y, por ejemplo, Taiwan, ha intentado solucionarlo multando a los padres que permitan que sus hijos estén conectados demasiado tiempo.
- Ataques a los sistemas de información a través de software malicioso.

Riesgos en internet

Son aquellos riesgos que existen fuera de internet, pero que adquieren una dimensión especial en este medio. Dentro de este apartado aparece una nueva clasificación:

Riesgos de contenido:
Derivados de la difusión de contenidos en la red.

- **Pornografía infantil.** Para el intercambio de archivos con este tipo de contenidos, empiezan a ganar terreno sistemas privados y de acceso restringido frente a las redes P2P, tradicionalmente utilizadas. Los sistemas de mensajería instantánea se están utilizando para la redistribución posterior.

- **Incitación al odio y al terrorismo y difusión de contenidos no apropiados o inexactos:** Según el último informe de EU Kids Online, va en aumento la exposición a mensajes de incitación al odio, páginas pro-anorexia y pro-bulimia y páginas sobre autolesión.

Riesgos de contacto: Derivados de acciones en las que el menor tiene cierto grado de participación.

- **Ciberbullying,** acoso entre menores a través de medios telemáticos: Este tipo de acoso está encontrando en los dispositivos móviles su medio más idóneo. El estudio «Menores de Edad y Conectividad Móvil en España», elaborado por la Línea de Atención sobre Ciberbullying, red europea para la denuncia de casos de acoso en la Red entre menores, dice que el 5.4% de los niños españoles de 11 a 14 años ha sido víctima de algún tipo de acoso a través del teléfono móvil.

- **Cibergrooming,** acciones realizadas a través de medios telemáticos por un adulto para establecer cierto control sobre un menor con la finalidad de facilitar futuros abusos sexuales. Las plataformas utilizadas son diversas, desde las redes sociales, pasando por programas como Skype, hasta las establecidas por videoconsolas.

- **Violencia de género digital.** Sobre este tema, varias organizaciones e iniciativas, entre ellas, "Pantallas Amigas" se preocupan de la incidencia que ha tenido la aparición de los smartphones en la violencia de género entre los adolescentes, facilitando que se ejerza el control sobre la intimidad, y las actitudes machistas y sexistas.

- **Juego online.** Expertos opinan que la ludopatía se desarrolla antes en el entorno digital que en el real. A eso hay que añadir que el entorno online ofrece a los menores un menor control de acceso.
  Privacidad y protección de los datos del menor. En un entorno en el que cada vez los datos tienen más valor, y los menores son usuarios muy activos, generando muchos datos, conviene tener este riesgo presente.

- **Sexting,** intercambio de imágenes o texto generados, en este caso, por el propio menor, para compartirlo en el marco de una relación privada. Este fenómeno se ha visto acentuado por aplicaciones como Snapchat, en el que un mensaje se autodestruye pasado un cierto tiempo, lo que ofrece cierta garantía de mandar imágenes de forma privada, aunque existen, a su vez, otros sistemas para capturar la imagen de forma permanente.

- **Propiedad intelectual.** Lo que más preocupa en esta vertiente es el acceso a contenidos descargados ilegalmente, que se incrementa cada año entre los más jóvenes.

Fuera de esta clasificación podría tenerse en cuenta otro riesgo, el futuro, o ya no tan futuro, desarrollo de la llamada "internet de las cosas". Sin ánimo de ser alarmistas, la posibilidad de que muchos objetos cotidianos estén conectados a la red y puedan generar datos, nos abre la posibilidad de otros riesgos que puede que hoy ni siquiera imaginemos.

5 | 2 | 3 Próxima reforma en el ámbito penal. Implicaciones

El Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica10/1995, de 23 de noviembre, del Código Penal, da respuesta a la necesidad de incorporar a nuestro ordenamiento jurídico ciertas obligaciones que exige la normativa europea. En relación a menores e internet, se pueden prever los siguientes cambios:

La realización de cualquier acto de carácter sexual con menores de dieciséis años será considerado un hecho delictivo, salvo que se trate de relaciones sexuales consentidas entre personas de similar grado de madurez y desarrollo, que en ningún caso serán penalizadas.

- Será delito hacer presenciar a un menor de 16 años relaciones de terceros o abusos cometidos sobre terceros.
- Se tipifica como delito, asimismo, contactar con menores a través de medios tecnológicos para conseguir material pornográfico.
- Se elevan las penas de los delitos de prostitución que afectan a menores o personas discapacitadas.
- Se considerará pornografía infantil imágenes realistas de menores participando en conductas sexuales explícitas, aunque no sean reales.
- Se amplía la jurisdicción de los tribunales españoles para perseguir a los clientes de prostitución infantil, aunque cometan el delito fuera de España cuando sean españoles o residan habitualmente en nuestro país.
- Se considera delictivo la difusión de imágenes obtenidas de manera consentida sin la autorización de la persona que las emitió.
- Los Jueces y Tribunales tendrán el reconocimiento expreso para retirar o bloquear el acceso de contenidos de pornografía infantil.
- Se considera delito el visionado de pornografía infantil en “streaming”.
- Se castiga la difusión por Internet de escritos que inciten al odio con motivos racistas o xenófobos.

5 | 2 | 4 Agentes intervinientes, alerta temprana, autorregulación

Agentes intervinientes

Sin ánimo de exhaustividad, se describirán los agentes intervinientes en la prevención de las situaciones que puedan crearse a partir de los riesgos descritos. Los primeros son grupos de interés institucionales y se corresponden con los tres sectores, público, privado y tercer sector; los dos últimos son grupos de interés del entorno cotidiano de los niños y jóvenes. Este epígrafe será completado en los puntos 5 y 6 del propio informe.

Estado:

Quizás, la reforma del Código Penal sea el mayor exponente de los avances que se están realizando desde el Estado, pero muchos de los cambios propuestos por esta reforma vienen impuestos desde Europa, y con retraso. La legislación española, se dedica a otorgar herramientas para poner remedio a los problemas ya generados, pero no es capaz de adelantarse a los que están por venir. Dentro del Estado cabe destacar los Cuerpos y Fuerzas de Seguridad del Estado y la sanidad (si bien, en la medida en que se vayan trasladando las políticas a la atención primaria, debiera pasar a ser un grupo de interés del entorno cotidiano.

Sector privado:

El sector privado debería cumplir no sólo la función de informar, sino también la de prevenir y establecer mecanismos que eviten que los riesgos existentes se materialicen. Teniendo en cuenta la realidad itinerante del acceso a internet de hoy en día, el método al que más se está recurriendo es el lanzamiento de aplicaciones para los fines anteriormente dichos. A título de ejemplo, los principales operadores de telefonía móvil, junto con “Protégeles”, han lanzado la aplicación “Protégete”, que se puede utilizar para informar de manera anónima de aquellos contenidos ilegales o nocivos para menores. Otra de las formas en la que las empresas están colaborando para evitar estos riesgos es la elaboración de informes sobre los hábitos de los menores, que hacen públicos, como ha hecho la empresa BQ.

Agrupaciones de carácter civil:

A raíz de la creciente preocupación por estos temas, están surgiendo múltiples pequeñas agrupaciones de carácter civil, cuya finalidad, principalmente, es la labor informativa.

Centros educativos

Los centros educativos cumplen, en cuanto a menores e internet, una función informativa. En este sentido, muchos centros llevan a cabo iniciativas propias para informar, tanto a los menores como a sus padres, de los riesgos existentes en la red y de cómo prevenir sus consecuencias. En cuanto a los estudios, las nuevas formas de comunicación se pueden convertir en una ayuda al estudio (información mucho más accesible) o en un elemento que "estorba" a la concentración. A este efecto, el informe "Evaluación del Programa Escuela 2.0 a partir de los resultados en Matemáticas de PISA 2012" extrae dos conclusiones (bastante discutidas), a saber, que no parece que la inversión en equipamiento informático haya revertido en un mejor rendimiento académico, y que el número de computador por alumno ejerce un efecto significativo y negativo sobre la nota en Matemáticas para todos los alumnos.

Padres

Los padres se han visto sorprendidos por la aparición de los dispositivos móviles, dejando sin efecto consejos como "que el menor se conecte a internet a través de un ordenador situado en un lugar concurrido de la casa". Ante ello, uno de los sistemas que más se están utilizando son los sistemas de control parental. Por otro lado, según datos del INE y del último informe de EU Kids Online, todavía no se ha reducido la brecha digital entre padres e hijos, especialmente en hijos adolescentes. Por último, me gustaría sacar a debate la siguiente pregunta: ¿proteger a los menores de los propios padres, o de los padres de otros niños? Algunos padres empiezan a compartir la vida de sus hijos menores en las redes sociales, solos o con sus amigos, y esto está generando controversias entre padres divorciados, o padres cuyos hijos son amigos. ¿Generará controversia entre padres y los propios hijos cuando estos alcancen la mayoría de edad?

Alerta temprana

La protección de la infancia, si se quiere llevar a cabo, debe adelantarse a los riesgos. En este sentido es muy importante el concepto de alerta temprana, es decir, detección rápida de riesgos. Los últimos avances en la materia versan en el tratamiento masivo de datos. A título de ejemplo, la organización Pantallas Amigas ha creado un sistema llamado “Ciberalerta”, que busca riesgos a través del tratamiento de los datos. Estos datos pueden empezar a ser más adecuados y veraces gracias a los sistemas de denuncia anónima que pueden recogerse de líneas como la establecida por “Protégeles”.

Autorregulación

Lejos de la regulación establecida únicamente por el poder público, se puede comprobar que se está optando por la responsabilidad compartida a través de la autorregulación, propuesta por el poder público y llevada a cabo por las empresas del sector implicadas en el ámbito del que trata este informe. En concreto, están sometidos, de algún modo, a la autorregulación, los operadores de telecomunicaciones, las plataformas web, y, de modo especial, las dedicadas al sector audiovisual.

En España el artículo 18 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico considera el fomento de la autorregulación como una obligación de las Administraciones Públicas.

En este sentido, el sector más destacado es el audiovisual, con el problema que surge a raíz de la autorregulación de los contenidos “a demanda”, por lo que el sistema de restricción basado en el horario de la regulación audiovisual actual quedaría obsoleto en el actual y futuro modelo de consumo en este medio.

5 | 3 Lecciones aprendidas en 6 años de debates Wen IGF España: dinamismo de los cambios y falta de madurez en las respuestas

Contar la historia de un proceso de cambio de seis años puede parecer pretencioso, pues es un periodo corto que no permite tener perspectiva. Sin embargo, si hablamos de tecnologías de la información y la comunicación, en seis años ha habido cambios profundos, y si la historia tiene que ver con niños, entonces no hay duda de que el niño/a que se incorporó a la red en 2009, con 14 años, ha vivido una historia completamente distinta que el/la adolescente que se incorpora en 2015.

El repaso de los congresos anuales de IGF España, es una buena forma de contar esa historia, porque todos los años hubo una mesa de debate con expertos y expertas sobre los retos de Internet y las TIC para niños y jóvenes.

Antes de recorrer los mensajes clave del periodo 2009-2014 de IGF Spain, es interesante anticipar algunas conclusiones de carácter general, que pueden orientar al lector en el análisis de los cambios de un año a otro.

Los tres grandes ejes de debate han sido:

- Los peligros de Internet como fantasma que todo lo cubre, dejando en un plano secundario el análisis de las oportunidades que permite y de los usos reales que los jóvenes hacen de la red.

- La responsabilidad de los distintos grupos de interés en el adecuado desarrollo de los niños y jóvenes en su vida en la red (colegios, familias, justicia-marco legal, administraciones públicas competentes…)

- La velocidad de los cambios tecnológicos y de usos de la red que hace que las pautas que se generan queden obsoletas a la misma velocidad.

Recomendaciones del 2009 como “mejor el ordenador en el salón y vigilar sus conversaciones de Messenger”, resultan cómicas en 2015, con niños con smartphones desde los 12 años, accediendo a todo tipo de redes sociales, e hiperconectados con el whatsapp. Ahora el mensaje cae por su peso: “Los niños tienen que tener una educación y unos valores que les permitan manejarse solos de forma satisfactoria en la red”.

A continuación se destacan las ideas más relevantes de cada uno de los congresos de IGF, tratando de mantener la máxima fidelidad a los textos originales.

5 | 3 | 1 2009: Protección de la infancia en Internet

Esta primera mesa fue un debate entre un amplio grupo de expertos procedentes de casi todos los grupos de interés relevantes. Las siguientes ideas recogen la esencia del debate:

> Alarmismo de los medios que consideran noticiable lo extraño y subraya el impacto que este tipo de cosas tiene entre los niños. Con los datos de que se dispone a día de hoy se puede extraer una primera y esencial idea: que los riesgos de los niños en el mundo online no son muy diferentes de los riesgos a los que se enfrentan en el mundo real, fuera de internet. Al menos en esencia. De hecho, hay estudios que ponen de manifiesto que, al igual que en entornos tradicionales, los factores que mejor actúan como medida de exposición al riesgo son las características psico-sociales de los niños y el entorno familiar que rodea a los menores. Sin embargo, algunas dimensiones del riesgo sí difieren sustancialmente: la gravedad de las consecuencias, la probabilidad de que ocurra, la facilidad de prevenirlo y/o resolverlo…

> El informe de Internet Safety Technical Task Force aboga por fomentar una navegación que suponga una experiencia familiar, de tal manera que sean los padres quienes decidan qué contenidos son adecuados para sus hijos. Es fundamental crear los mecanismos adecuados para, poco a poco, cambiar esta situación de tal manera que los responsables de la educación de los niños adquieran conocimiento y habilidad para enfrentarse al problema.

> Para las empresas, con más o menos matices y sin ser sustitutivo de la legislación vigente o de las iniciativas que en el futuro puedan tomar los Gobiernos, los asistentes abogan mayoritariamente por un modelo de autorregulación de contenidos y prácticas de buena conducta.

> Una visión al problema desde las instituciones públicas: dos vías de actuación, prevención y protección. Se habla de una "libertad vigilada". Soluciones creativas y originales en materia legislativa.

> Necesidad de estudiar detenidamente cuáles son los hábitos de los menores cuando manejan las nuevas tecnologías, para conocer mejor cuáles son los riesgos y las amenazas a las que se enfrentan. Las herramientas tecnológicas que contribuyan a la protección respondan a un diagnóstico. El always on que afecta a los adultos en la vida laboral es para ellos un modo de vida cuyos impactos no han sido suficientemente estudiados.

Exceso de alarmismo, supervisión directa de la navegación, claridad en el rol público, autoregulación de las empresas y estudios en profundidad de los hábitos de niños y jóvenes... Los años siguientes mostraron que esas cinco ideas no eran sólidas.

5 | 3 | 2 2010: Children and social media – opportunities and risks, rules and responsibilities. Opportunities and risks (Eurodig en España)

Este Segundo año Madrid fue la sede de EuroDig. La mesa de los niños hizo un análisis detallado de oportunidades y riesgos, y trataba de asignar responsabilidades:

Opportunities

- *ICTs provide children with an unprecedented possibility of having their voice heard and in participating in the public discourse of society.*
- *Technologically savvy children and young people can use the Internet to advance positive changes in society.*

Risks:

- *Children are not always aware of all the positive opportunities of the Internet or of the threats to their rights and security online.*
- *Children are excluded from discussions on Internet governance.*
- *Digital generation gap: parents and teachers are often not fully informed about technological developments in order to teach children about using the Internet.*
- *Many parents are not always available to teach their children about using the Internet.*
- *Young people who are most at risk from online harm are those who are most at risk from offline harm.*
- *Protectionist educational approaches to the use of Internet often produce negative results. They do not allow young people to apply the principles of autonomy and critical reflection to negative messages nor do they let them develop self-defence communication against politically incorrect messages.*

What?

- *Media literacy should be considered as one of the priority issues of Internet Governance.*
- *Measures to increase child participation through the use of ICTs should be increased – this includes child participation in discussions on Internet governance.*
- *New pedagogies of communication should help children to develop social and technological skills that allow them in their online as well as offline lives.*
- *Digital literacy programmes should also be provided for parents and teachers.*

How?

- *Media literacy means to develop the skills needed to read and produce thoughtful, creative and critical "online prosumers" (producers and consumers) in different media and languages.*
- *Media literacy needs to be improved, for example through educommunication, i.e. teaching children a thoughtful and critical use of the Internet making them not passive consumers but also active producers of media content.*
- *Minimum competencies to be Internet literate includes knowing and understanding the convergence of media and languages, to analyse levels and patterns of interactivity and navigation, understanding and applying the criteria of usability and accessibility in a context of collaborative and participative learning.*

El protagonismo de padres y colegios se iba consolidando como dos pilares de la agenda, y para ello había que asumir que sin competencias digitales es difícil guiar el proceso educativo. ¿Cómo acompañar ese protagonismo, en positivo, que se busca para los nativos digitales?

5 | 3 | 3 2011: Niñ@s y jóvenes en la red

En el 2011 se preparó un documento de posición.
Los informantes clave fueron niños y jóvenes que acudieron a sesiones de debate.

Internet es una fuente indudable de oportunidades para niñ@s y jóvenes y, es cierto, que además existen algunos riesgos vinculados a las TIC y a los nuevos usos de Internet a los que hay que prestar atención. Focalizar el debate y la acción excesivamente en los riesgos puede no ser el mejor camino para evitarlos, a la vez que se deja de lado el potencial de Internet como herramienta para el progreso personal y profesional. Es necesario generar modelos de referencia claros y positivos de usuarios medios, recogiendo las oportunidades y desafíos a los que se enfrenta la mayoría de la población infantil y juvenil.

Desde el grupo de trabajo de la mesa "El mundo de Internet para niñ@s y jóvenes", se ha querido realizar una aproximación objetiva, por medio de un planteamiento integral, y la integración de la visión de chicos y chicas, a través de un taller específico[1]. El planteamiento integral parte de considerar el impacto de Internet en tres esferas de la vida de niñ@s y jóvenes (relaciones sociales, ocio y aprendizaje), considerando así mismo tres tipos de usos (positivo, negativo y delictivo). (Ver gráfica 2 del epígrafe 1) Internet está poniendo de manifiesto carencias educativas (en sentido amplio) preexistentes entre la comunidad educativa pero, sobre todo, entre los padres.

Una idea a destacar en este objetivo de educar en el uso moderado y responsable de la vida en Internet de los niñ@s, es la extensión en el uso de los smartphones (Iphone, Blacberry los más habituales), especialmente sabiendo que en cuanto más pequeños son más claras y supervisables deben ser la pautas de tiempo de conexión.

En 2011[1] se quiso dar el protagonismo a las oportunidades para el aprendizaje, la creación, la socialización y el juego, los valores en la red, la corresponsabilidad de la industria, la colaboración multiactor… Pero la agenda se tambaleaba ante el cambio de terreno de juego que suponían los smartphones.

[1]Taller celebrado el 05/05/11 con un grupo de 16 chicos y chicas de entre 8 y 16 años, en el CIBALL (http://www.lacatedralonline.es/ciball/).

5 | 3 | 4 2012: Niñ@s y jóvenes en la red: el auge de los smartphone

En el 2012 los debates dejaron a un lado las voces críticas. Las empresas lideraron la reflexión y muchos de los optimistas en foros anteriores empezaban tener serias dudas de que los riesgos fueran pequeños y estuvieran bajo control.

Para los jóvenes, los smartphones constituyen un espacio privado propio que quieren gestionar ellos mismos sin intromisiones de terceras personas. Fundamentalmente, es un espacio que utilizan para la comunicación y el ocio. Demuestran tener un grado de madurez superior a la que se les atribuye en la sociedad en general y se ha comprobado que el excesivo paternalismo no funciona.

En cuanto al uso que hacen de los nuevos dispositivos móviles inteligentes, los servicios que más utilizan son el chat y subir fotos. Demandan poder comunicarse en cualquier sitio en movilidad. El reto que se deriva de estos hábitos de uso es que el Internet que vamos a disfrutar dentro de unos años lo están diseñando ahora mismo nuestros menores y es por ello que la industria se tendrá que adecuar a lo que demandan los que más utilizan los TIC, que son los jóvenes.

Nuestros jóvenes utilizan los smartphones para todo; no es una moda, es su mejor herramienta de comunicación. Los menores consideran que tener un dispositivo de estas características es normal, con lo cual no les genera ansiedad. El problema, en cambio, puede residir en los adultos cuando empiezan a utilizar las TIC: ¿las utilizarán de forma correcta?

En el caso de la aplicación "Clan", dirigida a menores de 10 años, revela que éstos discriminan el uso de los smartphones y los tablets: los primeros los utilizan para dibujar y como cámara, mientras los tablets lo utilizan para ver vídeos.

Se ha comprobado que cuando más se utiliza la aplicación es cuando los niños están con los padres. De lo que se pueden derivar dos lecturas: que los padres utilizan la aplicación como "aparca-niños" o lo comparten con ellos.

Aunque demandan auto-regularse, no por ello dejan de demandar formación. Aunque les gusta llevar la delantera, no quieren estar solos. De alguna manera están pidiendo interacción con sus padres. Sobre todo es necesario trabajar con ellos su responsabilidad, darles a conocer las normas que rigen las relaciones en internet y las posibles consecuencias de sus actos.

Para el mundo educativo uno de los principales retos consiste en la integración de estos dispositivos en las aulas. Hay experiencias en Tailandia, Turquía, la India, Corea del Sur e Israel, donde los menores trabajan con tablets en la clase. El uso está regulado tanto en relación con el horario de acceso como en relación a los contenidos.

También se ha destacado que la industria puede ofrecer una amplia variedad de soluciones para ayudar a los padres a supervisar la actividad de sus hijos: herramientas de control de contenidos, de control de consumo, herramientas de filtrado, etc. En este sentido se demanda y se valora muy positivamente trabajar en un entorno colaborativo entre los diversos actores.

La declaración completa de ese año es la mejor muestra de la posición de la industria en el debate. Quizás por ello, y ante los riesgos cotidianos que avanzaban a gran velocidad, el año siguiente la agenda dio un viraje de 180º.

5 | 3 | 5 2013: Ciberbullying

El grupo de trabajo que estudió el ciberacoso hizo, bajo la dirección de Inteco, un trabajo técnico de preparación y generación de debate de gran alcance y rigor. El problema se vio que era de gran relevancia, estaban cambiando las reglas del juego de las relaciones sociales en una edad muy complicada: la adolescencia. La conclusión final de la mesa, es solo una pequeña parte del mucho conocimiento que se generó:

> Siendo el ciberacoso concepto expresión que abarca una multiplicidad de conflictos y riesgos con consecuencias lesivas para el menor, se elevan al diputado Conrado Escobar de las Heras para su introducción en la subcomisión parlamentaria las siguientes peticiones:
>
> 1. Análisis y definición de las "actualizaciones normativas necesarias para la adecuada protección de los menores frente al ciberacoso y los riesgos derivados de su concepto amplio"
> 2. Definición indubitada de las responsabilidades de docentes y centros educativos en los conflictos y riesgos derivados del uso de la red.
> 3. ¿Hay cibervalientes sociales que ayuden a los más desprotegidos? O la necesidad de estudiar desde una perspectiva científica o analítica la formación de la identidad digital en el nuevo entorno social.
> 4. Creación de una plataforma de coordinación que permita aglutinar los esfuerzos de todos los agentes implicados en la detección y prevención del ciberacoso priorizando la educación en los centros escolares como herramienta fundamental y básica

La sensación al final del foro de 2013, es que no era sencillo hablar de una agenda de protección de la infancia, sino de reaccionar a los hechos según te los vas encontrando. ¿Y quiénes son los que se los encuentran en primera persona? Los niños, los jóvenes… tienen que estar preparados para afrontarlos… tenemos que entender la identidad red de las nuevas generaciones. El resto de los actores, tenemos que garantizar sus derechos.

5 | 3 | 6 2014: Niños e Internet

En el último foro se intentó analizar con perspectiva la evolución de las oportunidades y riesgos en la red para los niños. Intentar encontrar pautas claras en un entorno tan cambiante, con tantos intereses y sin rumbo definido parece misión imposible. Cada año, en los debates, las conclusiones del año anterior parecía que perdían sentido. En 2014 se trató de ampliar la perspectiva para no tener en 2015 la misma sensación de perplejidad.

Tal y como se consagra en el artículo 25 de la Declaración Universal: la infancia "tiene derecho a cuidados y asistencia especiales". Tal como se consagra en el artículo 5 de la Convención de las Naciones Unidas sobre los Derechos del Niño, los jóvenes tienen derecho al respeto de su "etapa de desarrollo".

En términos de Internet, esto significa que niños y niñas deben tener la libertad de usar y aprovechar todas las ventajas y beneficios que les aporta Internet para desarrollarse como personas, a la vez que deben estar protegidos de los peligros asociados con Internet.

El equilibrio entre estas prioridades dependerá de las capacidades de los jóvenes, del conocimiento que su entorno tenga de ello especialmente los padres y educadores y de las herramientas legales y técnicas que los estados y las empresas ponen a disposición de unos y otros. En Internet, el derecho a cuidados y asistencia especiales y el respeto al desarrollo de las capacidades de los niños incluyen:

- **a** *Derecho a beneficiarse de Internet y de las nuevas tecnologías*
- **b** *Protección contra la explotación y las imágenes de abuso infantil*
- **c** *Derecho a ser escuchado*
- **d** *El interés superior del niño*

También nos encontramos con normas y leyes que protegen al menor que en Internet son imposible de aplicar y esto en un momento en el que los niños conviven con pantallas y smartphones cada vez más potentes, cada vez a edades tempranas y con un uso intensivo que supera ya las 6 horas diarias las que pasan delante de una pantalla. Oportunidades conviven con un número importante de riesgos.

En este sentido se ha señalado la necesidad de ordenar el marco jurídico actual para adaptarlo a la realidad que impone Internet y de que las aplicaciones y herramientas que utilizan Internet estén cada vez más adaptadas a los usos que se hace de la red.

Las conclusiones del debate son nuestro punto de partida para este informe:

Nuestros jóvenes nacen y viven en la red y pasan en media más de 7 horas al día delante de una pantalla, el reto más importante que tenemos como sociedad es conseguir que este tiempo que es fundamentalmente consumista y comunicativo sea cada vez más creativo y formativo.

Falta compromiso y conocimiento de padres y educadores que siguen viendo a Internet como algo peligroso y desconocen su potencialidad. Seguimos decidiendo por ellos sin contar con su voz, faltan canales que nos permitan a los mayores hacer una escucha activa, aprenderíamos mucho y les animaríamos a usar más y mejor porque su futuro estará condicionado por las TIC.

Solo el 1% de los delitos que afectan a los menores tienen una componente tecnológica y de estos la mayoría tienen que ver con otros problemas ajenos a las TIC.

Una llamada de atención para el entorno móvil en la contratación e instalación de muchas APPs que en muchos casos se hacen con todos los datos de nuestros móviles sin ser necesario para el servicio que ofrecen. Se debe de estudiar y perseguir este fenómeno.

El legislador debería de actualizar el marco legal que afecta al menor para tener en cuenta las nuevas situaciones que provoca Internet y darles un tratamiento adecuado y equilibrado.

5 | 4 Aprendizaje, relaciones sociales y ocio en red: las bases para las competencias de los gestores del conocimiento

5 | 4 | 1 Competencias digitales

Partiremos de una hipótesis inicial sobre educación y ciberespacio compartiendo los principios de Daniel Innenarity (2011); que define la sociedad del conocimiento como sigue:

> "La sociedad del conocimiento es aquella en la que se han institucionalizado mecanismos reflexivos en todos los ámbitos funcionales. Estos mecanismos reflexivos se diferencian de los procedimientos de acumulación de experiencia propios de otras formas sociales del pasado por el hecho de que las experiencias se hacen y se reciben no "pasivamente", sino de manera prospectiva e innovadora, selectiva y reflexivamente."

El gran desafío de la sociedad del conocimiento es la generación de inteligencia colectiva. En la sociedad, y en las organizaciones, hay un exceso de información que impide a los miembros de la sociedad, o de la organización, tener una visión general de los asuntos y comprender y asimilarlos de forma eficiente. En muchas ocasiones es difícil de distinguir la información relevante de la información menos relevante. La respuesta que Innerarity da para gobernar el conocimiento, teniendo en cuenta las inconvenientes, es el diseño del conocimiento. El diseño del conocimiento es algo más que la elaboración de datos o intercambio de información[2] .

Y es que la competencia digital (por ser una competencia educativa) no puede reducirse al ámbito instrumental, no es mero adiestramiento en dispositivos o programas con una orientación laboral (uso); también supone un núcleo ético que es necesario descifrar y asimilar (sentido) y que tiene que ver con el pleno desarrollo de la personalidad humana y su apertura a la totalidad de lo real.

[2]Vid. Innerarity, D. (2011). La democracia del conocimiento: Por una sociedad inteligente. Paidós

La competencia digital es una de las 8 competencias clave que cualquier joven debe haber desarrollado al finalizar la enseñanza obligatoria para poder incorporarse a la vida adulta de manera satisfactoria y ser capaz de desarrollar un aprendizaje permanente a lo largo de la vida, según las indicaciones del Parlamento Europeo sobre competencias clave para el aprendizaje permanente (Recomendación 2006/962/CE del Parlamento Europeo y del Consejo, de 18 de diciembre de 2006, sobre las competencias clave para el aprendizaje permanente, Diario Oficial L 394 de 30.12.2006). La competencia digital no sólo proporciona la capacidad de aprovechar la riqueza de las nuevas posibilidades asociadas a las tecnologías digitales y los retos que plantean, resulta cada vez más necesaria para poder participar de forma significativa en la nueva sociedad y economía del conocimiento del siglo XXI.

La competencia digital, por tanto, puede definirse como el uso creativo, crítico y seguro de las tecnologías de información y comunicación para alcanzar los objetivos relacionados con el trabajo, la empleabilidad, el aprendizaje, el tiempo libre, la inclusión y participación en la sociedad. Los retos educativos planteados por Internet y las redes sociales no residen únicamente en una cuestión del uso de los medios, y ni siquiera se trata de una cuestión meramente de seguridad dirigida a evitar el ciberbullying. Junto a ello, se nos plantean desafíos situados en el entorno de la ética que tienen que ver con la responsabilidad, la relación educativa, las normas de comunicación en la red, la honestidad en la presentación de la información tanto propia como ajena, etc. Conocer la realidad de nuestro entorno y las variables que en mayor medida generan situaciones de riesgo para los adolescentes, puede contribuir a identificar las estrategias educativas más acertadas.

5 | 4 | 2 Resiliencia y valores

Si abordamos la resiliencia cómo un proceso dinámico que permite optimizar los recursos humanos en situaciones de adversidad, encontramos en los menores una polaridad extrema, en ocasiones con enorme capacidad de resiliencia al maltrato, y en otras observamos enormes problemas de adaptación a diversas actividades de su vida.

Atendiendo a las últimas cifras aportadas por el Ministerio del Interior sobre casos de acoso y ciberacoso escolar (cerca de 500.000 casos) es evidente que algo se está haciendo mal y probablemente es no haber percibido la dimensión educacional en valores previa a la inmersión en la sociedad digital.

Atendiendo al supuesto concreto de las Redes Sociales como herramienta de socialización obligatoria para casi el 100 % de la juventud española, podrían contarse con los dedos de la mano los usos educativo – emocionales que se están realizando en el ámbito escolar.

Centrados en la sacralización instrumental de los proyectos 1:1 por los dirigentes y responsables educativos, ninguno de ellos se ha parado a pensar en la potencialidad que para la educación en valores representan este tipo de herramientas tras un procesos de entrenamiento adecuado de los docentes.

A título enunciativo pueden definirse:

1. Mejora de la comunicación con los alumnos.
2. Colaboración e interacción entre los alumnos por medio de foros y otras herramientas interactivas y colaborativas.
3. Creación de contenido propio y en colaboración con alumnos a través de todo tipo de herramientas digitales creativas.
4. Selección de contenidos, buscando información en función de los objetivos.
5. Compartir material en todo tipo de formatos (vídeos, libros virtuales, presentaciones interactivas, etc.) con docentes y alumnos de todo el mundo.
6. Grabar lecciones en formato de videotutorial y compartirlas.
7. Creación de blogs y edublogs enlazados a las RRSS educativas.
8. Incremento sustancial de la motivación fomentando capacidades como la interacción, la autonomía, y la colaboración.

Conceptos cómo “uso “ y “sentido” adquieren entonces su verdadera dimensión en el desarrollo de aprendizajes sociales digitales.

La positivación pedagógica en el uso de las RRSS conllevará dotar de sentido intelectual a actividades que hasta ahora sólo se sitúan en el campo de la socialización primaria y que no permiten aprovechar las enormes oportunidades que la red presenta para el desarrollo emocional de los menores.

Recientes pilotajes cómo el realizado por Facebook en escuelas de España e Inglaterra son clara muestra de las posibilidades que esta metodología proporciona a la educación[3].

[3]Puede estudiarse en:
https://www.facebook.com/education?_rdr

5 | 4 | 3 Resiliencia, ciberacoso y desarrollo emocional

La expectación levantada por la publicación del libro de ciberbullying “Bajo mi piel” y que fue presentado oficialmente en el SID 2015, trasciende el dato de ser un testimonio de superación de una adolescente que ahora estudia psicología y que ha podido descubrir el drama psicológico interno que viven los adolescentes acosados.

Cómo expone en sus presentaciones la autora en tono jovial “Me excluyeron y acosaron por ser diferente, un bicho raro. Pero en Internet encontré muchos bichos raros cómo yo que me ayudaron...”

El conocimiento, el dominio y el uso responsable de la red devolvió a esta persona todo lo que la red la robó en un momento previo de desconocimiento e incertidumbre.

Del pánico a la satisfacción, del terror al abrir una red social a encontrarse en un ecosistema digital de aprecio, cariño y satisfacción.

Pero fue un proceso en soledad, sin apoyo ni de comunidad educativa ni de agentes sociales, no doloso, pero si culpable en gran medida por desidia y sobre todo, incompetencia[4].

Urge, por tanto, no solo establecer descriptores de competencia de uso de los instrumentos digitales, sino evaluadores de adquisición de valores por parte de los alumnos a través de sus docentes.

[4]Más información en
https://www.facebook.com/Nidiaenlared?fref=nf

5 | 4 | 4 Identidad digital

La formación de la personalidad digital de los menores exige, por tanto, replantearse de manera urgente el papel a desempeñar por la competencia digital en el currículo educativo.

Los proyectos 1:1 en los centros educativos están siendo introducidos en los colegios cómo si fueran el paradigma de la revolución digital y nos están llevando a cometer los mismos errores del pasado. La llegada del aprendizaje cognitivo y las herramientas de big data aplicadas a la educación volverán a mostrar las carencias de cooperación que las dispersiones competenciales y la falta de una agenda digital educativa sólida están causando en el desarrollo de la personalidad de nuestros alumnos.

Debemos dejar de pensar y aplicar el término “enseñar con TIC” y evolucionar hacia interpretaciones conceptuales que integren “Tecnologías para el Aprendizaje y el Conocimiento”.

El “Aprendizaje Integrado de Contenidos Digitales “ se define cómo la capacidad que el docente debe desarrollar para procesos de aprendizaje natural en las aulas desde edades de educación infantil, integrando siempre el ¿ para qué? en vez del ¿cómo?, y eso a día de hoy es impensable en el actual estado de preparación docente.

La educación prosocial en las asambleas que los profesores realizan en las primeras etapas de desarrollo, son ya esenciales y deben estar también orientadas a esa inmersión digital que tantas carencias presenta.

Cuando un centro educativo aborda de manera definitiva un proyecto de digitalización o mochila digital, provoca de manera irreversible una serie de cambios intelectuales, emocionales y sociales en la personalidad del alumno cuyas consecuencias son directamente proporcionales al grado de madurez – o inmadurez – del menor, con condicionantes de riesgo siempre determinados por la vulnerabilidad ética y moral de las personas en formación.

Este condicionante adquiere dimensiones desconocidas valorando el requerimiento que el parlamento británico ha enviado al gobierno solicitando la inmediata priorización de la competencia digital como tercer gran pilar de la educación junto con las matemáticas y la lengua. Si ello es así, que lo va a ser, y desde tan temprana edad tenemos que dar la alfabetización digital la importancia reflejada en el informe, nos encontramos con un condicionante crítico ya que se fundamenta en las raíces más profundas del futuro de la sociedad de la información y la economía de mercado.

La competitividad y el liderazgo económico condicionarán el futuro de la educación y la competencia digital, y por tanto del estado de bienestar.

En este escenario resulta preocupante que el 90 % de los docentes apenas presente destrezas digitales; peor es que en la mayoría de los casos la adquisición de habilidades se realiza con finalidades mecánicas o de aprendizaje de uso de las herramientas en cumplimiento de objetivos materiales curriculares.

Si tenemos en cuenta que la verdadera dimensión ética del aprendizaje digital sólo podrá acometerse una vez adquiridas y comprendidas por los docentes las posibilidades pedagógicas de las nuevas herramientas, el panorama es, cuanto menos, desesperanzador.

Aunque debe acogerse con satisfacción la inclusión en los planes de estudio de la asignatura de programación en cuanto que es un avance respecto al currículo anterior, tremendamente reprochable es en muchos casos la instrumentación diseñada para su implantación. Porque hablamos de programación para aprender, y no de aprender a programar, en cuanto desarrollo de capacidades y habilidades transversales que pueden ser óptimas para cualquier asignatura y competencia básica.

- Porque la gamificación es altamente motivadora pero debe responder a trabajos pedagógicos con objetivos coordinados por docentes cualificados cualquiera que sea el nivel educativo en donde se utilicen.

- Porque la realidad aumentada y virtual en la educación pueden causar efectos contrarios de frustración al menor sino llega a comprender porque su dibujo cobra vida o cómo se combinan las valencias químicas en 3D.

Y porque tanto la programación, como la realidad aumentada, así como cualquier otra tecnología digital puede ser utilizada siempre y en todo lugar para crear y reforzar la identidad digital y la educación en valores en los centros educativos.

Que mejor manera de aprender a respetar las creaciones de los terceros en Internet, que aprendiendo a proteger y compartir tus propios contenidos, sean videojuegos o reflexiones poéticas.

Como conclusión, debe ser grande la preocupación por la no existencia de un plan nacional de formación y cualificación del profesorado en competencias digitales que contemple la doble dimensión aquí descrita. Preocupación agravada por la dispersión competencial y la endeblez de la agenda digital española en este campo.

5 | 4 | 5 Los millenials en el mercado de trabajo

La Agenda Digital para España establece la elaboración de un Plan de Inclusión Digital y Empleabilidad que integre al mayor número de agentes posible, sirva de paraguas a sus iniciativas, aúne esfuerzos y multiplique el efecto de las medidas que se adopten. El Plan es el resultado de las aportaciones de múltiples actores, públicos y privados, que se han incorporado para sumar esfuerzos en el objetivo común de mejora de la calidad de vida de los ciudadanos y de mejora de la competitividad y posicionamiento de nuestra PYME gracias al uso de las TIC.

Esta agenda es la base para el paradigma de los millenials:

- Prepararlos para puestos de trabajo que no han sido todavía creados.
- O prepararlos para crear esos puestos de trabajo.

Las decisiones y acciones adoptadas en materia educativa van encaminadas hacia el primer objetivo, y el debate es cómo lograr situar nuestro sistema educativo a la vanguardia de los países OCDE dando respuesta al segundo.

Hasta la fecha, cabe destacar la acreditación competencial oficial es la desarrollada por Proyecto Universidad Empresa en al marco del convenio suscrito con la CRUE a través del proyecto Certiuni[5].

[5]Ver certiuni-crue.org

Constatamos una iniciativa parlamentaria del Partido Popular que ha presentado en el Congreso de los Diputados una proposición no de ley con la finalidad de:

> "Nuestro país avanzaría en la empleabilidad de jóvenes y parados de larga duración, reduciría la brecha digital de género o en áreas rurales, las empresas podrían tener una cierta objetividad sobre las aptitudes digitales de las nuevas incorporaciones y unificaría los modelos desarrollados en algunas Comunidades Autónomas[6]"

La enseñanza reglada parece que está fuera de la proposición no de ley dando pie nuevamente a los problemas de dispersión competencial educativa en un ámbito de decisión que puede afectar de manera sistémica al futuro profesional de los millenials. El INTEF está desarrollando indicadores y evaluadores competenciales de manera unilateral que:

- Podrán ser aceptados o no por las Comunidades Autónomas.
- No serán validados por el sector empresarial, y menos para contratación internacional.
- Sólo vincularán a unos pocos miles de docentes que opositen a la función pública docente.

Es obvio por tanto concluir con la necesidad de que la Agenda Digital centralice tanto la descripción competencial como los modelos de acreditación que garanticen la empleabilidad de la generación millenial si se aspira a diseñar una economía digital en los puestos de cabeza de la OCDE.

[6]http://javierpuenteredondo.com/2015/02/18/el-pp-pide-establecer-en-espana-un-modelo-de-acreditacion-de-competencias-digitales/

5 | 5 Protección a la infancia

En este epígrafe se recogen las políticas en marcha que garantizan la protección de la infancia en España. A continuación se muestran las principales actuaciones en marcha de los grupos de interés institucionales públicos: Industria, Sanidad y Fuerzas y Cuerpos de Seguridad del Estado.

5 | 5 | 1 Actuaciones en materia de protección a la infancia en materia de Sociedad de la Información

El Gobierno es plenamente consciente de la importancia que presenta la protección de determinados colectivos en Internet, en especial los menores y siempre ha mostrado gran sensibilidad en esta materia.

Por este motivo y en el marco generado por la Agenda Digital para España, se están impulsando campañas informativas de formación en cuanto a los fenómenos vinculados con la seguridad TIC de los menores. Estas iniciativas responden a la necesidad de reforzar la confianza digital a través de diversos mecanismos contemplados en la medida nº 4 del Plan de Confianza de la Agenda Digital para España (ADpE), hoja de ruta del Gobierno en materia de sociedad de la información.

Uno de los instrumentos que se van a emplear desde el Ministerio de Industria, Energía y Turismo, a través de la Entidad Pública Empresarial Red.es, es la realización de un plan de formación consistente en servicios de capacitación en materia de seguridad TIC para padres, madres, tutores y educadores de menores de edad. Se pretende dotar de habilidades a padres, tutores y formadores, para que sean capaces de acompañar a los menores de edad en el uso de las TIC de una forma responsable. Para ello, este plan de formación se articulará en torno a las siguientes actuaciones:

- Diseño y elaboración de los materiales formativos, unidades didácticas y monográficas sobre los principales riesgos asociados a las actividades online de los menores, que se utilizarán en las acciones de capacitación del público objetivo.

- Desarrollo y ejecución de las acciones de capacitación tanto presenciales como online basadas en los materiales desarrollados. Dichas actuaciones serán llevadas a cabo en centros públicos con acceso a Internet (telecentros, bibliotecas, centros culturales, centros cívicos, centros educativos, etc.) o privados (empresas, ONGs…) distribuidos por la totalidad del territorio español.

Estos materiales formativos serán puestos a disposición de las Consejerías de Educación de las CCAA a través de la coordinación que lleve a efecto el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), adscrito al Ministerio de Educación, Cultura y Deporte.

Por último, y en el marco del Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos, liderado por el Ministerio del Interior, se prevé la utilización de los recursos formativos generados por Red.es para su aplicación en el entorno educativo.

Por otra parte, otra iniciativa a destacar es el Foro de colaboración público-privada de "Menores e Internet" impulsado por Red.es: un grupo de trabajo que tiene como misión aunar y coordinar esfuerzos y recursos legales, educativos, policiales y divulgativos para la protección de la infancia y adolescencia en Internet. En este Foro, además de los distintos Ministerios, están participando todas las asociaciones, fundaciones y entidades relacionadas con los menores e Internet y tiene como objetivos principales:

- Poner en común los proyectos e iniciativas públicas y privadas generadas en el ámbito de los menores a través de un portal en Internet agregador y colaborativo.
- Identificar líneas de actuación comunes, obtener sinergias y eludir duplicidades en los esfuerzos desplegados por la Administración y el sector privado.
- Consolidar a España como referente en el ámbito de la protección de los menores en Internet.
- Contribuir a alcanzar los objetivos de confianza digital señalados en los planes de acción gubernamentales contemplados en la Agenda Digital para España[7].
- Fomentar una cultura de la protección del menor en Internet entre la ciudadanía, el tejido empresarial, el ámbito investigador y la Administración.

[7]Eje I, medidas nº 3 y nº4: http://www.agendadigital.gob.es/planes-actuaciones/Bibliotecaconfianza/Plan/Plan-ADpE-5_Confianza.pdf

Adicionalmente, y de acuerdo con lo contemplado en la ADpE, Red.es está impulsando la elaboración y divulgación de diversas guías, materiales y recursos pedagógicos destinados a informar y garantizar la seguridad del menor en Internet, y estudia la viabilidad para implementar un mecanismo que permita el etiquetado de contenidos digitales para menores en la red. Entre las actuaciones en este ámbito destacan:

- Un convenio de colaboración con el Hospital de La Paz y la Sociedad Española de Medicina del Adolescente (SEMA) que ha permitido elaborar una Guía clínica sobre Ciberacoso para profesionales de la salud que permita a todos los profesionales que trabajen con los adolescentes a prevenir, detectar, tratar y evitar complicaciones relacionados con el ciberacoso.. La guía se encuentra disponible en http://www.chaval.es/chavales/sites/default/files/Guia_Ciberacoso_Profesionales_Salud_FBlanco.pdf

- En colaboración con la Comisión Nacional de Mercados y Competencia (CNMC) y el ICAA (Ministerio de Cultura), se va a realizar un proyecto piloto de etiquetado de contenidos digitales, tras haberse concluido en Red.es un estudio de viabilidad técnica de la iniciativa.

Además, el Plan de Menores en Internet reforzará el portal de chaval.es de Red.es (www.chaval.es), impulsando un grupo de trabajo específico para la protección del menor donde estén representados, entre otros, el Ministerio de Interior (Guardia Civil, Policía), el Ministerio de Justicia, el Ministerio de Educación, Cultura y Deporte y el Ministerio de Sanidad Servicios Sociales e Igualdad junto a las CCAA.

La protección integral de los menores constituye un escenario que presenta múltiples facetas (jurídicas, tecnológicas, educativas, policiales, etc.). En consecuencia, resulta de capital importancia la coordinación de las actuaciones, tanto públicas como de carácter privado, en esta materia. Dicha coordinación se articulará a través de la constitución de una plataforma o grupo de trabajo público-privado de menores e Internet integrado por representantes la AGE (Ministerios de Industria, Turismo y Comercio, Interior, Justicia, Educación Cultura y Deporte y de Sanidad, Servicios Sociales e Igualdad o la CNMC), así como CCAA, asociaciones y fundaciones de carácter privado más representativas y expertos reconocidos en el ámbito de la protección de los menores en la Red. Entre las actuaciones que se desarrollarán en el marco del Plan de menores en Internet se encuentran las siguientes:

- Creación de una plataforma segura para menores en Internet, con actuaciones divulgativas y preventivas, en la que se integrarán algunos de los portales actuales, como www.chaval.es o www.menores.osi.es, y que servirá de portal de referencia para el uso de recursos destinados a la protección de los menores en la red.
- Desarrollo de proyectos tecnológicos de innovación en la protección de la infancia y los menores en la Red.
- Impulso de acciones de sensibilización y formación.
- Realización de estudios para conocer el uso que niños y adolescentes hacen de Internet, las posibilidades que les ofrece y los riesgos y situaciones que pueden alterar su vivencia digital.

5 | 5 | 2 Actuaciones en materia de protección a la infancia en materia de Sanidad

Las TIC son un ítem novedoso en el campo sanitario, en los últimos cuatro años se han multiplicado exponencialmente las publicaciones internacionales relacionados con la salud, los riesgos de las TIC y los menores. Sin embargo, hay escasa documentación acerca de la función del personal sanitario como agente preventivo y de su papel en la educación para la salud, es decir, aún no se abordan las TIC en este ámbito como oportunidades, tan solo como riesgos. En España, es aún más escasa tanto la formación del personal sanitario en riesgos como en oportunidades de las TIC, así como la realización de investigaciones científicas de calidad en dicho campo.

Todo lo anterior denota que los esfuerzos realizados desde los diferentes ámbitos profesionales han sido muchos, específicos desde cada ámbito pero no de forma multidisciplinar; por ello, hay colectivos profesionales más avanzados, como educación, y otros que están dando los pasos iniciales, como los profesionales de la salud. Los profesionales de la salud deberían ser un colectivo prioritario y es urgente su formación para que puedan prevenir y detectar los problemas relacionados con las TIC.

El papel del personal sanitario en la protección de la infancia en el entorno de las TIC

El objetivo del pediatra ante los riesgos que los menores tienen en las TIC es prevenir y educar en salud y en el uso adecuado, responsable y seguro de las TIC, al igual que se realiza en otros ámbitos, como en la seguridad vial.
Las TIC deberían ser incluidas en los exámenes de salud, como un ítem más. La detección precoz de los casos, especialmente del ciberbullying (CB), es esencial para poder realizar un manejo adecuado de los pacientes y un tratamiento precoz, evitando la aparición de comorbilidad y el suicidio. La coordinación con otros profesionales como profesores, abogados, Cuerpos y Fuerzas de Seguridad del Estado y la familia, es otra labor fundamental del pediatra[8].

[8]Vid. Grupo de trabajo de la Guía Clínica de ciberacoso para profesionales de la salud. Guía clínica de ciberacoso para profesionales de la salud. Plan de confianza del ámbito digital del Ministerio de Industria, Energía y Turismo. Hospital Universitario La Paz, Sociedad Española de Medicina del Adolescente, Red.es. Madrid. 2015.

Las TIC y la salud en niños y adolescentes

La afectación de las TIC en la salud, es diferente según la edad del menor.

1 **En los menores de tres años**

En los tres primeros años de vida se realiza el mayor desarrollo tanto a nivel físico como psíquico.

En España se sitúa el inicio en el uso de las TIC entre el primer año y el segundo año de vida y está descendiendo. Se desconoce con exactitud el impacto que puede tener a esta edad el uso reiterado de pantallas. Sociedades científicas internacionales han puesto énfasis en la necesidad de restringir su uso en esta franja de edad[9].

Es necesario que los niños de 0 a 3 años tengan contacto con sus principales cuidadores el mayor tiempo posible al favorecerse de este modo el desarrollo de una figura de apego adecuada y el establecimiento apropiado del vínculo. El aprendizaje en esta edad viene determinado por el descubrimiento de su mundo directo, la experimentación, el desarrollo, la importancia del juego simbólico, el desarrollo adecuado de la psicomotricidad gruesa y el inicio del desarrollo de la psicomotricidad fina. El niño tiene que aprender el ritmo normal del mundo que le rodea, debe controlar sus frustraciones y manejar los tiempos de espera[10].

El uso abusivo de pantallas a esta edad se ha relacionado con el TDAH y los trastornos de conducta.

Muchos padres a esta edad realizan un uso de las TIC, fundamentalmente tabletas y smartphone, como falsos elementos activos de distracción de los hijos y para evitar que denoten sus frustraciones o comportamientos normales de niños que puedan resultar molestos a adultos en determinadas circunstancias.

[9]Vid. Paniagua Repetto H. Impacto de las tecnologías de la información y la comunicación. Pediatria Integral 2013; XVII(10): 686-693.

[10]Vid. Vanderloo LM. Screen-viewing among preschoolers in childcare: a systematic review. BMC Pediatr. 2014:16;14:205 Y Duch H, Fisher EM, Ensari I, Harrington A. Screen time use in children under 3 years old: a systematic review of correlates. Int J Behav Nutr Phys Act. 2013:23;10:102. Y Radesky JS, Silverstein M, Zuckerman B, Christakis DA. Infant self-regulation and early childhood media exposure. Pediatrics. 2014:133(5):e1172-8.

2 En los mayores de tres años, especialmente en los adolescentes

Un grupo especialmente vulnerable para tener conductas de riesgo en internet es el de los adolescentes, al estar en una edad que se caracteriza por tener dificultades para medir los riesgos, la sensación falsa de invulnerabilidad y la necesidad de intimidad, provocan que tengan la sensación de que ellos por sí mismos pueden resolver sus problemas sin ayuda de los adultos[11]. Asimismo, los adolescentes actuales no han recibido formación ni educación desde pequeños en las TIC porque ha sido en los últimos cinco años cuando se ha universalizado su uso y en el que internet ha tenido un mayor desarrollo y expansión, tanto en aplicaciones como en tipos de dispositivos disponibles conectados a la red y de pequeño tamaño.

• Acceso a información inadecuada o inexacta para la edad

Tanto el acceso a contenidos no contrastados, poco fiables o falsos, como la facilidad de acceso a páginas con información peligrosa o nociva. Tanto en acceso a contenidos pornográficos como violentos, lo que no está estudiado es el impacto en menores que no lo buscan y se los encuentran en ventanas emergentes, publicidad o al estar presentes cerca de contenidos infantiles en plataformas de difusión de vídeos.

a. Acceso a contenido pornográfico. Los adolescentes consultan internet, como fuente para obtener material pornográfico por su accesibilidad y gratuidad, no está relacionado con conductas sexuales de riesgo y es un comportamiento más frecuente en chicos. El consumo de pornografía es más frecuente en hombres adultos y en esta edad si está relacionado con conductas de riesgo fundamentalmente el consumo de drogas y las prácticas de sexo sin protección. Otro punto importante respecto a los contenidos pornográficos es el aumento de contenidos pornográficos cuyos protagonistas son menores, en algunos casos realizados bajo su consentimiento y difundidos por ellos mismos o por terceros. Este problema es creciente y de vital importancia ya que atenta directamente contra los derechos del menor y es un delito.

b. Acceso a contenidos violentos. El acceso a contenidos violentos se da fundamentalmente en plataformas de vídeos online y en juegos en línea. El impacto de los videojuegos violentos depende enormemente del estado anímico del menor, muy relacionado con los estados depresivos y de la personalidad del menor; en los adolescentes altruistas se moderan las reacciones hostiles, en los adolescentes egoístas aumentan los sentimientos agresivos. No existe un consenso sobre la relación entre videojuegos y agresividad. Sin embargo el fracaso escolar si está relacionada con el uso excesivo de videojuegos y especialmente en aquellos que consumen contenidos violentos[13].

[11]Vid. Grupo de Nuevas Tecnologías de la Información y la Comunicación (NTIC) de la Sociedad Española de Medicina de la Adolescencia (SEMA). Salmerón Ruiz M.A. Adolescere Vol III(1): 3-6,2015.

[12]Vid. Peter J, Valkenburg PM. The influence of sexually explicit Internet material on sexual risk behavior: a comparison of adolescents and adults. J Health Commun. 2011: 16(7) :750-65. Y Smith PK, Thompson F, Davidson J. Cyber safety for adolescent girls: bullying, harassment, sexting, pornography, and solicitation. Curr Opin Obstet Gynecol. 2014:26(5):360-5.

[13]Vid. Cornellà I Canals J. Adolescentes y videojuegos: una necesaria reflexión. Cuadernos de pediatría social. 2014:20:4-6.

2

Situaciones conflictivas

El ciberacoso es un tipo de maltrato ejercido contra los menores y por tanto es labor de la sociedad en general y de los profesionales de la salud en particular velar por los derechos del menor.

El ciberacoso no es el riesgo más frecuente en internet pero sí el que entraña más peligro al presentar la víctima con mayor frecuencia depresión grave y suicidio debido a la mayor exposición de la víctima al acoso (ver tabla 1, diferencias y similitudes entre el ciberacoso y el acoso cara a cara), por lo que es imprescindible el diagnóstico precoz.
En EE.UU. está considerado el ciberacoso un problema de salud pública.

El acoso ejercido por un menor, contra otro menor a través de medios digitales se denomina ciberbullying o ciberacoso escolar (CE). El acoso ejercido por un adulto contra un menor con fines sexuales por medios digitales se denomina Grooming (G).

El (G) clásico es en el que un adulto desconocido se pone en contacto con un menor desconocido a través de internet y tras una fase de amistad, en la que el acosador intenta obtener información del menor y fotografías, una segunda fase de chantaje en la que el acosador chantajea a la víctima para que envíe imágenes con contenido sexual o hará pública la información obtenida y una tercera fase de acoso y abuso sexual. En ocasiones, se inicia la fase de amistad y de relación cara a cara por una persona conocida previamente por el menor, que posteriormente continúa con el abuso sexual a través de los dispositivos electrónicos e internet como una herramienta más de dicho abuso.

Es muy importante que los menores no tengan canales de comunicación exclusivos con adultos en los cuales no participen los padres.
Los pederastas en muchas ocasiones eligen «un papel» que les permite un contacto más prolongado con menores como pueden ser los perfiles de entrenadores deportivos, monitores de ocio y tiempo libre, etc[8].

La clínica más frecuente son los síntomas físicos de origen psicosomático, tanto en víctimas y agresores como en los que sólo son observadores: dolor abdominal, trastornos del sueño, cefalea, fatiga, enuresis secundaria, pérdida de apetito, pérdida de peso, tics, mareos y vértigo. Los síntomas psicológicos de mayor prevalencia son: ansiedad, depresión, baja autoestima e ideación suicida. Algunas alteraciones conductuales pueden ser muy indicativas: dejar de conectarse a internet o conectarse con mayor frecuencia de la habitual, mostrarse frustrado, triste o enfadado después de usar el ordenador o el teléfono móvil o no querer hablar sobre el tema si se le interroga[8].

En el caso de (G), las principales consecuencias para el menor que ha sufrido grooming son: desconfianza hacia otros, alteración del autoconcepto y dificultades para establecer relaciones futuras de pareja y para establecer un apego seguro[6].

El motivo de consulta en el adolescente no es el ciberacoso sino los síntomas psicosomáticos físicos. Ante cualquier demanda de un adolescente hay que preguntar acerca del uso que hace de las TIC y si ha acosado, ha sido insultado o ha presenciado ciberacoso a terceros.

2

Adicciones

En la actualidad no existe consenso, no está recogida la adicción a internet o a pantallas en el DSM-V. Hay autores que afirman que se puede ser adicto al contenido de internet pero no a internet en sí, puesto que es una herramienta. Por otro lado existen síntomas compatibles con el abuso de internet, en los que el paciente busca en él un refugio, pasando mucho tiempo conectado pero sin ser realmente una conducta adictiva.

La conducta adictiva a internet es definida como un patrón de comportamiento caracterizado por la pérdida de control sobre su uso y aparición de síntomas ansiosos si se intenta regular o eliminar su uso. Esta conducta conduce paulatinamente al aislamiento y al descuido de las relaciones sociales, de las académicas, recreativas, de la salud y de la higiene personal[14].

TIC trastornos del sueño y atención

Es muy frecuente que los adolescentes tengan televisión en el dormitorio y que tengan el teléfono móvil encendido durante la noche. Las TIC influyen en la cantidad, calidad y la presencia de trastornos específicos del sueño que se traduce en un sueño no reparador, con sensación de cansancio diurno, disminución de la atención e irritabilidad[15].

El uso de pantallas antes de dormir disminuye significativamente el tiempo de sueño, aumenta la sensación de tener un sueño no reparador y aumenta la probabilidad de despertar precoz. El insomnio de conciliación se asoció significativamente con el uso frecuente de telefonía móvil, los videojuegos y las redes sociales. Escuchar música para quedarse dormido o durante el sueño se asocia al riesgo de tener pesadillas.

[14]Vid. Observatorio de la Seguridad de la Información. Instituto Nacional de Tecnologías de la Comunicación (INTECO) y Orange. Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles, 2010.

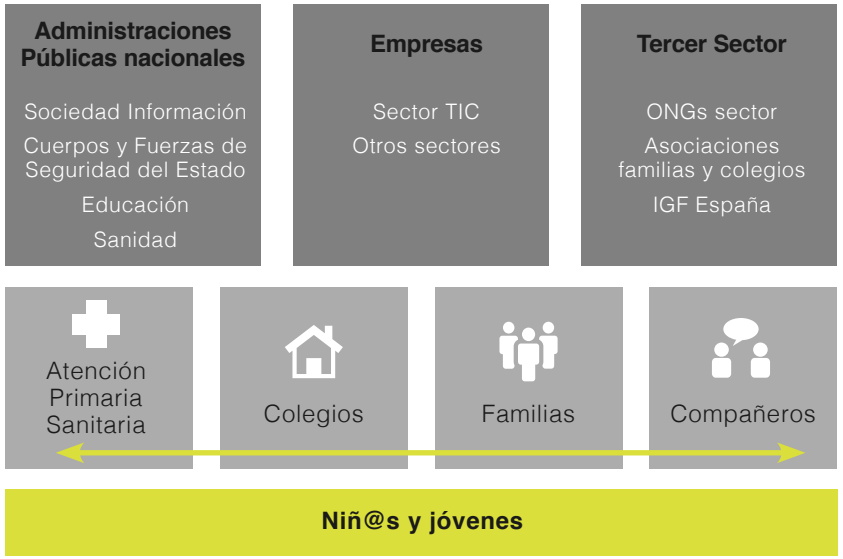
[15]Vid. Fossum IN1, Nordnes LT, Storemark SS, Bjorvatn B, Pallesen S. The association between use of electronic media in bed before going to sleep and insomnia symptoms, daytime sleepiness, morningness, and chronotype. Behav Sleep Med. 2014: 12(5):343-57. Y Arora T1, Broglia E2, Thomas GN3, Taheri S4. Associations between specific technologies and adolescent sleep quantity, sleep quality, and parasomnias. Sleep Med. 2014:15(2):240-7.

5 | 6 Los actores responsables

Para avanzar en la agenda que se ha dibujado en los epígrafes anteriores y que se resume en el último punto del capítulo “Identidad red de niñ@s y jóvenes”, es importante definir con la mayor claridad posible los actores que deben y pueden liderar las diferentes líneas de trabajo.

En el marco conceptual ya se identificaban a todos los grupos de interés (stakeholders): institucionales, responsables públicos (de regulación del sector, de educación, de sanidad y garantes del cumplimiento de la los derechos, leyes y normas), empresas (del sector TIC y de otros sectores), y organizaciones del tercer sector; y del entorno cotidiano, niños y niñas, familias, colegios.
Si pensamos en la responsabilidad de definir, liderar y hacer cumplir una agenda para la protección de la infancia y para el desarrollo armónico de la identidad red de niñ@s y jóvenes, la responsabilidad está en los actores con competencias y con poder. Los actores finales, niños-familias-colegios, son los protagonistas de su ejecución, de la identificación temprana de tendencias, de aportar la voz de los protagonistas que es la que permite una adecuada orientación de la agenda.

En el gráfico que sigue se muestra a todos los grupos de interés que, en distintos epígrafes, se han ido mencionando como corresponsables de la agenda de protección y desarrollo de los niños y jóvenes en la red.



Gráfica 3: Grupos de interés analizados en el capítulo

La protección de la infancia y juventud, como derecho, y como garantía de cumplimiento del marco normativo en vigor, es indudablemente responsabilidad pública. En el epígrafe anterior, “Protección a la infancia”, se ha trasladado esa visión de las responsabilidades de los actores públicos.

En este epígrafe se va a completar la visión con las responsabilidades de las empresas del sector TIC y de otros sectores; y con la descripción del rol que están jugando las organizaciones del tercer sector que, asociadamente, conlleva la asunción voluntaria de responsabilidades.

5 | 6 | 1 La perspectiva de las empresas

La relación de los niños y adolescentes con las nuevas tecnologías tiene unas complejidades que no se pueden enfocar desde una sola perspectiva o ángulo. Es necesario hacer una aproximación holística para poder entender el dimensionamiento de dicha relación.

Por norma general, y debido al impacto mediático que tiene todo lo que está relacionado con daños infligidos a niños, el uso de internet siempre se asocia a peligros, preocupaciones, adiciones, y en general siempre se adopta un tono negativo al respecto.

Sin embargo, se debería observar esta relación bajo un prima positivo por todas las ventajas que generan las nuevas tecnologías en nuestra vida cotidiana. Las TIC están aquí, han cambiado nuestras vidas, nuestros hijos nacieron y crecen con ellas, han cambiado nuestra forma de relacionarnos, de trabajar, de comunicarnos, de jugar, de aprender, de organizar nuestro tiempo de ocio y las actividades de asueto en si mismas, y un largo etcétera de cambios que han supuesto en nuestra vida la adopción de internet y de las herramientas y servicios que giran alrededor.

Los españoles somos líderes europeos en adopción de las nuevas tecnologías, lo fuimos en su día con la penetración de la telefonía móvil con respecto al resto de nuestros países vecinos y lo somos ahora en el uso de internet móvil y de smartphones. Pero el uso que hacemos está muy enfocado a ser consumidores de información y no tanto como productores de la misma.

Por otro lado, al hablar siempre de los “peligros” de internet, estamos desplazando todas los aspectos positivos y el uso constructivo que se puede hacer de esta maravillosa herramienta. En los casos aislados donde, por ejemplo, profesores innovadores están incorporando el uso de las nuevas tecnologías en las aulas, como por ejemplo las redes sociales, la percepción desde fuera es que no se entiende lo que está haciendo y se le observa con reticencia.

Otro detalle significativo que debemos tener en cuenta es la cada vez más temprana iniciación en el uso de internet por los niños, y que a menudo, a pesar de su corta edad, saben manejar con más destreza y agilidad las tabletas o los teléfonos inteligentes que nosotros mismos.

No obstante, los niños demandan unas necesidades específicas en relación con las diversas actividades que realizan con las nuevas tecnologías como soporte y acorde con su edad a su uso bien sea en grupo, de manera comunitaria o individual.

La industria tiene un papel importante que jugar para evitar la brecha entre los conocimientos que sobre las nuevas tecnologías tienen respectivamente los niños y sus padres pero la labor de educación y concienciación sobre el buen uso de las nuevas tecnologías es una tarea que se debe realizar conjuntamente entre todos los sectores de la sociedad, no sólo por la industria, ya que la industria por ella misma no puede atajar los problemas derivados del mal uso de la tecnología. Agentes como los gobiernos, las organizaciones del sector civil, los cuerpos y fuerzas de seguridad del Estado, los centros educativos, profesores, padres pero por supuesto y deberían ser los primeros de la lista, los propios niños grandes e intensivos usuarios de las nuevas tecnologías de la información y la comunicación tienen responsabilidades en este terreno que deben aceptar.

La industria, asumiendo su rol en este contexto, apuesta por la autorregulación como mecanismo para promover el buen uso de sus productos y servicios.

Así, cuando en febrero de 2007, la Comisión Europea promovió la firma del Acuerdo Marco para el uso seguro de la telefonía móvil por parte de los menores al que se adhirieron las principales operadoras de Europa, España fue el primer país europeo en trasladarlo a Código de Conducta nacional siendo los operadores españoles (Orange, Telefonica, Vodafone y Yoigo) los promotores del mismo firmándolo en diciembre de ese mismo año y desde entonces no han cesado de colaborar conjuntamente para desarrollar iniciativas dirigidas a fomentar un uso responsable del teléfono móvil y de internet.

Un año después, en febrero de 2008, la Comisión Europea lanzó un Acuerdo similar pero esta vez para promover el uso seguro de las Redes Sociales por parte de los menores. El acuerdo se declinó en una guía con recomendaciones entre las que cabe destacar: ofrecer información fácilmente comprensible por los menores, ofrecer mecanismos de verificación de edad robustos, mejorar las configuraciones de privacidad y proporcionar mecanismos de denuncia robustos. Finalmente 21 empresas de redes sociales y motores de búsqueda se comprometieron a implantarla.

No obstante, dado el avance de la tecnología, y la aparición de nuevas empresas en el ecosistema de las TIC, la colaboración de la industria ya no se podía limitar sólo a los operadores de telefonía móvil o a las redes sociales, sino que además se debían tener en cuenta todas las empresas del sector ya sean motores de búsquedas, fabricantes de videojuegos o de terminales o de ordenadores.

De estas colaboraciones son fruto la Coalición de los CEOs para un mejor internet para los niños auspiciada por la Comisión Europea y la Coalición de las empresas TIC, iniciativa promovida por la industria para proporcionar una experiencia satisfactoria online.

Aunque la función principal de la industria deba ser desarrollar productos y ofrecer las herramientas y los recursos necesarios a sus clientes para que sus servicios se usen con seguridad y responsabilidad, el sector TIC está particularmente sensibilizado e implicado en ofrecer educación, para favorecer el buen uso de la tecnología por parte de los menores.

Por último cabe destacar en este documento la Alianza promovida por el GSMA para luchar contra los contenidos de abusos sexuales a menores en la red, integrada por los principales operadoras de telefonía móvil del mundo, y que recibió el apoyo de la Comisión Europea durante World Mobile Congress organizado en Barcelona en febrero de 2010, donde Viviane Reding, entonces comisaria europea de la sociedad de la Información y Medios de Comunicación dio la bienvenida a este acuerdo, como muestra del compromiso de los operadores móviles para luchar contra los contenidos ilegales en internet y en especial para proteger a los niños víctimas de abusos sexuales.

Este acuerdo es una clara muestra de la proactividad de la industria en la lucha contra los contenidos de abusos sexuales a menores y que debería encontrar respaldo en España a través de la reforma del Código Penal en curso.

5 | 6 | 2 La perspectiva de la sociedad civil

Podría decirse que, en cierta medida, la voz de los niños y jóvenes, y de su entorno educativo (familias y colegios) es representada por las ONGs del sector y por las administraciones competentes en educación e infancia.

Sin ánimo de exhaustividad, se mencionan a continuación algunas de las organizaciones que tienen un papel relevante en el cuidado de niños y jóvenes en el mundo de las TIC: GSIA (Grupo de Sociología de la Infancia y la Adolescencia), Fundación Alia2, FAPMI (Federación de Asociaciones para la Prevención del Maltrato Infantil), Protégeles - Centro de Seguridad en Internet, Pantalla Amigas, Fundación Alia2 o Foro Generaciones Interactivas.

Podría decirse que las organizaciones del tercer sector son en gran medida la forma de canalizar las inquietudes de los grupos de interés del entorno cotidiano. Los colegios, las familias, los compañeros y los propios niños y jóvenes.

La articulación de canales de coordinación con los colegios es quizás el más estructurado hasta ahora porque actúan bajo el paraguas del Ministerio de Educación y las Consejerías competentes de las Comunidades Autónomas. Aun así, el establecimiento de protocolos ante problemas relacionados con las TIC se está demostrando muy complejo.

En los últimos tiempos, la atención primaria sanitaria va aumentando su protagonismo como grupo de interés cotidiano, y sus actuaciones también se coordinan desde el ámbito competencia público correspondiente en cada territorio. Pudiera ser que la sociedad civil, muy activa en asuntos de salud, promueva plataformas de diálogo nuevas.

5 | 7 Algunas claves para la agenda para el futuro

A lo largo de este capítulo se han repasado los ingredientes que los autores hemos considerado más relevantes para entender cómo se está desarrollando la identidad de los niños y jóvenes en la red y cómo, dentro de esta integración de Internet y las TIC en sus vidas, se ponen los cimientos para garantizar la protección de la infancia.

Naturalmente, en torno a este asunto hay mucho investigado, implementado, evaluado, en construcción…En el primer epígrafe se describen los marcos de referencia para analizar los retos y oportunidades de niños y jóvenes en la red, que nos parece que tienen mayor claridad conceptual y estabilidad para entender los fenómenos en marcha. Hay grandes oportunidades de innovación para el aprendizaje, el ocio y las relaciones sociales a través de las TIC. La primera conclusión de este capítulo es que hay que potenciar los usos positivos y maximizar los beneficios asociados. Quizás el mayor riesgo es desperdiciar el potencial que las TIC traen para el desarrollo de niños y jóvenes.

Sin embargo, también hay riesgos, y como en cualquier otro servicio básico con fundamentos tecnológicos complejos, es función de los Estados establecer las reglas para garantizar, directamente o a través de otros actores, unos mínimos de seguridad y calidad en los servicios de información y telecomunicaciones.

Esas garantías, atendidas por las leyes, por las políticas públicas, y por los acuerdos de organismos multilaterales, se enfrentan en el caso de Internet y la infancia, como se recoge en el epígrafe 2, a dos tipos de retos: los genéricos y los específicos de la infancia. Podría decirse que los retos planteados al marco jurídico actual en el resto de los capítulos del Informe IGF, en relación a la privacidad, al derecho al olvido, a la libertad de expresión…afectan a la infancia y a la juventud. Mientras no se encuentre una respuesta al problema general, de poco sirve analizar los riesgos desde la perspectiva de la infancia. Los específicos se analizan desde la Convención de las Naciones Unidas sobre los Derechos del Niño, y se ve que algunos requieren una revisión completa a la vista de los nuevos modelos de comunicación, como por ejemplo *la protección al niño contra toda información y material perjudicial para su bienestar*.
La categorización de riesgos que se recoge en el epígrafe 2, basada en la que ha hecho la citada Comisión de Las Cortes en 2014, es un pilar básico para desplegar los mecanismos de protección a través de los Ministerios y otros actores competentes. La segunda conclusión de este capítulo es que hace falta perspectiva y agilidad para estudiar, dialogar y reglamentar los riesgos detectados, y, posteriormente, poner en marcha los mecanismos protectores definidos. Harían falta unidades especializadas multidisciplinares con capacidades operativas mucho mayores que las actuales.

La clave es el equilibrio entre perspectiva y agilidad. Cuando se habla de las TIC hay que moverse entre dos extremos: el primero es dejarse arrastrar por los cambios coyunturales vinculados al avance tecnológico o de servicio concreto (Messenger, Tuenti, Ask, Whatspp…), lo que lleva a intensos análisis adhoc con una validez de meses; el segundo es ir a los asuntos esenciales en la vida de los niños y niñas (valores, sistema educativo, comunicación con los padres…), lo que puede llevarnos a la simplificación de que no hay nada significativamente nuevo con las TIC, y que como para tantas otras cosas, una buena educación es suficiente. En este capítulo hemos optado por situarnos más cerca del segundo extremo, ver las cosas con una perspectiva de varios años, y a eso nos ha animado el repaso en el tercer epígrafe 3 de los seis años de debates en IGF, que nos llevaron de coyuntura en coyuntura viendo como los acontecimientos de cada año pasaban por encima de las conclusiones del año anterior. La tercera conclusión es que existe una carencia de estudios sólidos, en los que participen todos los implicados, empezando por los niños y jóvenes, que permitan dar más solidez a la toma de decisiones. El rol del observatorio de sociedad de la información, para asuntos de infancia y juventud, y en permanente diálogo con los grupos de interés, es imprescindible, especialmente con los niños y jóvenes.

Y sí, esa es la cuarta conclusión, que lo más importante que tenemos que hacer es dotar de competencias a los protagonistas del cambio, para que sean, de verdad, constructores de conocimiento, sean capaces de relacionarse en red equilibradamente, y lideren la innovación en un mercado de trabajo al que se van incorporando con la visión de los nativos digitales.

Las competencias para manejar las tecnologías y las redes se van incorporando paulatinamente a la sociedad, los niños van por delante de sus educadores, colegios, profesores, familias, planes educativos…en el dominio de esas competencias red, pero carecen de valores para la vida red ni criterio para entender ni decidir las implicaciones de ese mundo. La transformación del sistema educativo en su conjunto va muy por detrás de lo que requieren los desafíos que afrontan los niños y jóvenes. Para afrontar sus relaciones red con respeto y prudencia, protegiendo su intimidad, sin dañar a otros, hay que formarles y darles guías que hoy solo recibe una minoría. El nuevo marco de competencias digitales es imprescindible.

En los epígrafes 5 y 6 se vuelven a repasar estas mismas ideas pero desde la perspectiva de las responsabilidades: de la administración pública, de las grandes empresas de tecnología, de los colegios, de la sociedad civil organizada. No hay duda de que la agenda de TIC e infancia y juventud es multiactor.

La Administración General del Estado tiene actuaciones de protección de la infancia en materia de Sociedad de la Información, desde las Fuerzas y Cuerpos de Seguridad del Estado, desde Sanidad, desde Educación. Quizás el ciberacoso, y esta es la quinta conclusión, es un excelente ejemplo de cómo se han puesto en marcha los mecanismos necesarios para afrontar la protección de los niños y niñas desde todos los ámbitos competenciales implicados. Los pasos de estudio, debate, normalización y operativización que se están siguiendo para el ciberacoso sean un camino abierto para otros de los riesgos que requieren intervención urgente. El ámbito sanitario se ha mostrado como un canal de acceso para la prevención, estudio y acompañamiento de los niños y jóvenes, por lo que la preparación de los médicos para poder jugar este papel y de herramientas de apoyo, es una prioridad.

Por último, pero no menos importante, hay que seguir asignando responsabilidades. No hay duda de que las garantías de protección tienen que ser lideradas por los Estados, pero no lo es menos, que la autorregulación que se espera de las empresas con más poder, y la implicación de las organizaciones de la sociedad civil son los otros dos pilares del taburete. Iniciativas de autoregulación del sector TIC, en el que las empresas sumen esfuerzos son fundamentales, tanto para ayudar en la resolución de los problemas detectados, como para anticipar y prevenir otros desde los observatorios de estrategia y de responsabilidad social. La influencia de Google, Facebook, Tuenti, Movistar o Whatsapp en el día a día tecnológico de niños y jóvenes es enorme, y el mirar para otro lado ante los malos usos que se desarrollan en el centro de sus "plataformas", y la priorización de intereses de negocio frente a otros valores, una barrera infranqueable para ningún otro actor. La implicación proactiva, creativa y responsable del sector, TIC es imprescindible. Si con estas ideas recogidas en el capítulo tuviéramos que contestar a la pregunta de si estamos preparados para acompañarles en su crecimiento entre tecnologías la respuesta es que no. Los talleres de trabajo y conversaciones con los niños y jóvenes nos confirman una y otra vez que, en lo fundamental, son autodidactas, y que no tienen canales de comunicación fluidos y con criterio con los grupos de interés de su entorno cotidiano: colegios y familias. Hay que insistir una vez más en la importancia de la formación de padres, madres y profesionales de la educación como mejor prevención y única forma de transmitir unos valores positivos para la identidad red. A estos grupos de cercanos se están sumando los profesionales de la salud, y esta es una gran noticia pues son el canal de prevención natural. Quizás, una novedad es que los chicos y chicas son cada vez más conscientes de las oportunidades de apoyo mutuo: de los mayores a los pequeños, de los amigos que saben más de tecnología a los que se atascan, y de los que crecen con madurez en su identidad red a los que adentran en conductas de riesgos.

Capítulo 6

Políticas de propiedad intelectual y Gobernanza

Coordinación: **Borja Adsuara**

Editores/Autores: **Borja Adsuara**

Grupo de Trabajo:

Borja Adsuara (Profesor y Abogado, Experto en Derecho Digital)

Antonio Fernández (Director General de ADEPI/Asociación para el Desarrollo de la Propiedad Intelectual)

Carlos Guervós (Subdirector General de Propiedad Intelectual/ Ministerio de Educación, Cultura y Deporte)

Cristina Morales (Subdirectora General de Contenidos de la S.I. / Ministerio de Industria, Energía y Turismo)

Natalia Moreno (Gerente / Telefónica)

Martín Pérez (Presidente/ Fundación España Digital)

Daniel Pero-Sanz González (Jefe de Servicio de Régimen Jurídico/ Subdirección General de Propiedad Intelectual)

Alejandro Puerto (Registrador de la Propiedad Intelectual de Madrid)

José Luis Zimmermann (Director General de ADIGITAL/Asociación Española de Economía Digital)

6 | 1 Principales hitos nacionales y europeos en 2014

6 | 1 | 1 En España

Modificación de la Ley de Propiedad Intelectual

El año 2014 fue el de la tramitación parlamentaria y la aprobación de la Ley 21/2014, de 4 de noviembre, por la que se modifica el Texto Refundido de la Ley de Propiedad Intelectual y la Ley de Enjuiciamiento Civil

a **Según la SE de Cultura**, impulsora del Proyecto, tiene entre otros objetivos:

- Incrementar la eficacia de los mecanismos procesales para la protección de los derechos de propiedad intelectual en el ámbito civil.
- Mejorar la eficacia de las notificaciones y la defensa de los interesados en el procedimiento de salvaguarda de derechos de propiedad intelectual en Internet regulado en la Ley 2/2011, de 4 de marzo, de Economía Sostenible.
- Reforzar las medidas de protección de los derechos de propiedad intelectual frente a su vulneración por parte de responsables de servicios de la sociedad de la información.
- Adaptar el límite legal de cita o reseña a los agregadores de contenidos en Internet, reconociendo el derecho irrenunciable de las empresas editoras y autores de noticias a ser compensados económicamente por ello y realizar los ajustes legales precisos que permitan acotar el ámbito del límite por copia privada adaptándolo a la actual realidad tecnológica con pleno respeto de la Directiva 2001/29/CE y de la jurisprudencia del Tribunal de Justicia de la Unión Europea.
- Garantizar la eficaz administración de los derechos de propiedad intelectual y la simplificación, para los usuarios de estos derechos, del acceso a su explotación y de los procedimientos de recaudación, posibilitando un control y vigilancia efectivos de las entidades de gestión de derechos de propiedad intelectual por las Administraciones Públicas, y reforzando la función social de las entidades de gestión, en línea con la que será la transposición de la Directiva 2014/26/UE.

b **Según Adigital:**

Restringe sustancialmente el límite de la copia privada, discriminando al entorno digital frente al analógico, ya que, por ejemplo, no está adaptada al entorno "cloud" y no ampara la copia privada con asistencia de un tercero, que sea un prestador de servicios en la nube.

Establece una responsabilidad secundaria de los intermediarios, medios de pago y agencias publicitarias, al establecer una obligación de colaboración, cuyo objetivo es cortar el acceso a la financiación al infractor.

c **Según Adepi:**

Cabe considerarse como un año casi perdido, ya que desde la aprobación del Anteproyecto de Ley, el 14 de febrero de 2014, hasta la publicación de la Ley 21/2014 en el BOE, el 5 de noviembre de 2014, y pese a que los grupos parlamentarios presentaron entre Congreso y Senado más de 400 enmiendas, las finalmente aprobadas, y por tanto incorporadas a la Ley, fueron escasísimas.

Podría calificarse la nueva redacción del TRLPI como una reforma parcial de muy poco recorrido, ya que su propia Disposición final cuarta prevé que en el plazo de un año se inicien los trabajos para preparar una reforma integral de la LPI. Además es una reforma fallida, ya que la regulación de la copia privada está gravemente cuestionada por el Tribunal Supremo, tal y como anticipó en su dictamen el Consejo de Estado y en su informe el Consejo General del Poder Judicial. También porque no se ha aprovechado la reforma para trasponer la Directiva 2014/26/UE sobre gestión colectiva de los derechos de autor y derechos afines y concesión de licencias multiterritoriales, porque impone una serie de obligaciones a las entidades de gestión que incrementaran fuertemente sus gastos de gestión y por tanto reducirán las cantidades destinadas a reparto.

Por último, no va a resolver el grave problema de la vulneración de derechos en internet, ya que sus mejoras son claramente insuficientes.

Cuestión prejudicial sobre el canon por copia privada (octubre 2014)

Durante 2014 se produjo un hito que puede afectar a la longevidad de una parte significativa de la Ley 21/2014, ya que en octubre de 2014 el Tribunal Supremo elevó una cuestión prejudicial ante el Tribunal de Justicia de la UE, cuestionándose si el modelo de compensación equitativa por copia privada establecido en el Real Decreto-ley 20/2012 y en el Real Decreto 1657/2013, viola el derecho comunitario. Este modelo cuestionado ha sido consolidado en la modificación del artículo 25 del texto refundido de la Ley de Propiedad Intelectual.

6 | 1 | 2 En Europa

Sentencia Svensson del Tribunal de Justicia de la UE (13.02.2014)

"No constituye un acto de "comunicación al público",…la presentación en una página de Internet de enlaces sobre los que se puede pulsar y que conducen a obras que pueden consultarse libremente en otra página de Internet".

Pero dicha actividad de enlaces sí puede constituir un acto de comunicación al público si concurren determinadas circunstancias (y, por lo tanto, una vulneración de derechos de propiedad intelectual si no existe autorización del titular de los derechos).

Directiva europea sobre gestión colectiva de derechos (26.02.2014)

Según Adepi, la Directiva 2014/26/UE sienta las bases para que la gestión colectiva de derechos se adapte más y mejor al entorno digital y tenga su lugar en el Mercado Único Digital.

Esta Directiva establece una serie de condiciones para que las entidades de gestión operen de manera más eficaz, en particular respecto a la distribución a sus socios de la remuneración percibida por el uso de sus obras y concedan más licencias multiterritoriales para los usos en línea de las obras musicales, directamente o a través de otras entidades.

Resolución del Parlamento Europeo sobre cánones por copia privada (27.02.2014)

Según Adepi es una iniciativa muy importante para la gestión colectiva de derechos, que vino a reforzar el sistema de remuneración por copia privada, y en especial el papel de la gestión colectiva de este derecho. Haciendo referencia a la Directiva de gestión colectiva de derechos de autor, la Resolución del Parlamento Europeo enfatiza el papel de las entidades de gestión en la percepción del canon por copia privada y destaca la importancia de que el flujo de dicha remuneración y posterior distribución a los titulares de derechos sea transparente. Asimismo la Resolución considera que el sistema de copia privada establece un equilibrio entre la excepción para realizar copias con fines privados y el derecho a remuneración equitativa de los titulares de derechos y opina que no existe a corto plazo ninguna alternativa a este sistema equilibrado.

Con respecto a los servicios de cloud computing, el Parlamento Europeo pide a la Comisión que evalúe las repercusiones que dichos servicios tienen para el sistema de copia privada que ofrecen posibilidades de grabación y almacenamiento con fines privados, a fin de determinar si esas copias privadas de obras protegidas deberían tenerse en cuenta en los mecanismos de compensación de la copia privada y, en caso afirmativo, de qué manera.

Comunicación de la Comisión Europea (01.07 2014)

"Hacia un consenso renovado sobre el respeto de los derechos de propiedad intelectual: Un Plan de Acción de la UE".

Informe sobre resultados de la consulta sobre copyright (Julio, 2014)

Lanzada por la Comisión Europea en diciembre 2013, hasta marzo 2014.

Auto caso Bestwater del Tribunal de Justicia de la UE (21.10.2014)

En donde se señala que: "El mero hecho de que una obra protegida, libremente disponible en un sitio de Internet, se inserte en otro sitio de Internet mediante un enlace utilizando la técnica de "transclusión" ("framing") no puede calificarse de "comunicación al público", en la medida en que la obra de que se trata no se transmite a un público nuevo, ni se comunica siguiendo un modo técnico particular, diferente del de la comunicación original".

Grupo de Expertos (4.11.2014)

La Comunicación de la Comisión Europea (COM (2014) 392) de 1 de julio de 2014 "Hacia un consenso renovado sobre el respeto de los derechos de propiedad intelectual: un Plan de Acción de la UE" recoge entre las acciones a acometer la constitución de un Grupo de Trabajo de Expertos de los Estados Miembros en materia de respeto de la propiedad intelectual para llevar a cabo un intercambio de información sobre mejores prácticas en los distintos Estados Miembros en esta materia y para ser informados sobre el grado de avance de dicho Plan de Acción. El Grupo de Trabajo de Expertos se constituyó el 4 de noviembre de 2014 y, desde entonces, se han celebrado varias reuniones de trabajo.

6 | 2.Avance del Año 2015: Principales hitos en España y Europa

6 | 2 | 1 En España

Autorregulación sectorial (10 de marzo 2015)

Según la SETSI: Con actuaciones de autorregulación y colaboración con actores relevantes en el mercado, encaminadas a eliminar incentivos a los modelos de negocio basados en la vulneración de los derechos de propiedad intelectual. En esa línea de acción, el pasado 10 de marzo de 2015 se firmó un Acuerdo entre la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, AMETIC y la Asociación de fabricantes de software BSA para reforzar la concienciación y sensibilización de la sociedad sobre los derechos de propiedad intelectual del software señalando la importancia actual de este sector para economía digital y su potencial para un desarrollo económico futuro. En el marco de este acuerdo, se ha constituido un grupo de trabajo que está estudiando diversas actuaciones a desarrollar en 2015.

Reforma del Código Penal (30 de marzo de 2015)

Tramitación y aprobación de la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica el Código Penal. Su entrada en vigor es el 1 de julio. Tipificación como delito de las páginas de enlaces.

Según Adepi esta reforma supone un reconociendo a los avances que aportan las reformas. El sector está a la expectativa y con cierto escepticismo, por los resultados que puedan arrojar las medidas contra la vulneración de derechos de propiedad intelectual en internet una vez entre en vigor la reforma del Código Penal, que se sumará las reformas de la Ley de Propiedad Intelectual y la Ley de Enjuiciamiento Civil.

Reglamentos de desarrollo de la LPI

El reto es la elaboración de hasta ocho reglamentos que deben aprobarse en virtud a lo dispuesto en la Ley 21/2014. Especialmente, son muy relevantes y ya se han iniciado los trabajos de:

- La Orden ministerial de metodología para la determinación de las tarifas generales que aplican las entidades de gestión
- El Real Decreto de regulación de las Funciones de la Sección primera de la Comisión de Propiedad Intelectual

Trabajos preparatorios para la reforma integral de la LPI

La Disposición final cuarta de la Ley 21/2014, de 4 de noviembre, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, prevé que:

> "El Gobierno, en el plazo de un año desde la entrada en vigor de esta ley, realizará los trabajos preliminares necesarios, en colaboración con todos los sectores y agentes interesados, para preparar una reforma integral de la Ley de Propiedad Intelectual ajustada plenamente a las necesidades y oportunidades de la sociedad del conocimiento. Con vistas a esa reforma deberán evaluarse, entre otros aspectos, el régimen aplicable a la gestión colectiva de derechos, el régimen de compensación equitativa por copia privada y las competencias y naturaleza del regulador."

Sería importante que se realizaran dichos trabajos preliminares necesarios para acometer en la próxima legislatura la Reforma integral de la Ley. Igualmente relevante sería, aprovechando dicha reforma, la trasposición a nuestro ordenamiento jurídico de la Directiva 2014/26/UE, relativa a la gestión colectiva, que debe ser realizada antes de abril de 2016.

6 | 2 | 2 En Europa

Presentación del informe REDA (15.01.2015)

PROYECTO DE INFORME sobre la aplicación de la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.

La eurodiputada ponente Julia Reda propone reducir los derechos exclusivos, proponiendo introducir más excepciones en el marco normativo europeo, que tengan carácter obligatorio, y que en algunos casos los Estados miembros no prevean compensación por ley a favor de los titulares de derechos por el uso de sus obras en aplicación de una excepción.

El informe establece, según Adepi, un inexistente conflicto entre ciudadanos y creadores, obviando el papel de las plataformas de internet. Ha sido fuertemente criticado por todos los grupos del europarlamento, lo que ha motivado la presentación de más de 500 enmiendas.

Tratado de Libre Comercio entre la UE y Estados Unidos

Desde el 2013 la UE está negociando un acuerdo de comercio e inversión con los EEUU: el “Transatlantic Trade and Investment Partnership” (TTIP) o, en español, la “Asociación Transatlántica de Comercio e Inversión” (ATCI).

Uno de los capítulos se refiere a los contenidos y servicios culturales, por lo que puede afectar a la regulación de los derechos de propiedad intelectual.

Estrategia e Iniciativa legislativa sobre el Mercado Único Digital

El Presidente de la Comisión Europea, Jean-Claude Juncker, ha hecho de la consecución del mercado único digital uno de los grandes y urgentes objetivos de su mandato con el fin de impulsar el crecimiento económico y la creación de empleo. En su programa Juncker incluso fijaba, como fecha para que la Comisión lance la iniciativa legislativa, el primer semestre de 2015, si bien no se ha comprometido en cuanto al calendario (de hecho los servicios competentes de la Comisión ya sitúan en el mes de octubre de 2015 la aprobación de la iniciativa legislativa que se someterá al Consejo).

El 6 de mayo los Comisarios Ansip y Oettinger hicieron pública su estrategia de consecución del Mercado Único Digital (Digital Single Market), en la que se incluirá la propiedad intelectual como una materia prioritaria sobre la que adoptar medidas.

Se estima que en otoño 2015, se presente una propuesta legislativa sobre propiedad intelectual.

La modernización del régimen europeo de derecho de autor

Una de las 16 medidas clave de la 'Estrategia sobre un Mercado Único Digital para Europa', dentro del Pilar I: "Mejorar el acceso de los consumidores y las empresas a los bienes y servicios digitales en toda Europa":

> **6.** Se presentarán propuestas legislativas antes de finales de 2015 para reducir las diferencias entre los regímenes de derechos de autor nacionales y permitir un acceso más amplio a las obras en toda la UE, incluidas nuevas medidas de armonización. La finalidad es mejorar el acceso de los ciudadanos a los contenidos culturales en línea – incentivando de este modo la diversidad cultural– a la par que se ofrecen nuevas oportunidades a los creadores y a la industria de contenidos.
>
> En particular, la Comisión pretende garantizar que los consumidores que adquieren películas, música o artículos en el hogar puedan disfrutar también de ellos cuando viajen por Europa.
>
> La Comisión analizará también el papel de los intermediarios en línea en relación con las obras protegidas por derechos de autor y reforzará la aplicación de la ley contra los delitos mercantiles que vulneren los derechos de la propiedad intelectual.

Según la Comisión esta modernización permitiría la portabilidad del contenido adquirido legalmente y facilitar el acceso transfronterizo a servicios pagados legalmente. A ello habría que añadir la revisión del marco normativo civil de respeto de los derechos de propiedad intelectual (Directiva 2004/48/CE) y la posibilidad de proponer legislación que armonice los procedimientos de eliminación de contenido ilegal de las plataformas.

La concesión de licencias y el respeto de los derechos de sus miembros son dos grandes funciones que por ley se atribuyen a las entidades de gestión colectiva de derechos que asisten así a sus miembros. Esto se aplica no solo al entorno analógico sino muy en particular al entorno digital en el que la difusión de los contenidos protegidos es mucho más fácil y menos costosa debido a los avances tecnológicos.

a

Normas para facilitar el comercio electrónico transfronterizo

> **1.** Ello incluye normas armonizadas de la UE en materia de contratos y protección de los consumidores en la compraventa en línea: ya se trate de bienes físicos, como calzado o muebles, o de contenidos digitales, como libros electrónicos o aplicaciones para dispositivos móviles. Se espera que los consumidores se beneficien de una gama más amplia de derechos y ofertas, a la par que las empresas podrán vender más fácilmente a otros países de la UE. Se reforzará la confianza en la compra y venta transfronterizas.

b

La eliminación del geo-bloqueo injustificado

La Comisión considera que el bloqueo geográfico injustificado de productos (entre ellos, los contenidos) es incompatible con el Mercado Único y anuncia medidas que perseguirán eliminar la discriminación basada en la residencia del consumidor.

> **4.** El fin del bloqueo geográfico injustificado — una práctica discriminatoria utilizada por motivos comerciales, cuando los vendedores en línea deniegan a los consumidores el acceso a un sitio web en función de su ubicación o los redirigen a la tienda más próxima con precios diferentes. Este bloqueo se traduce en que, por ejemplo, los clientes del servicio de alquiler de vehículos en un determinado Estado miembro pueden acabar pagando más por el alquiler de un coche idéntico en el mismo destino."

Así la Comisión avanza como medidas la modificación de la Directiva 2000/31/CE de comercio electrónico y la clarificación del artículo 20 de la Directiva 2006/113/CE de servicios en el mercado interior.

La Asociación española Adepi ve con mucha preocupación la eliminación del geobloqueo, ya que una de las bases fundamentales de las industrias creativas europeas es la libertad comercial de gestión nacional. El sector está muy preocupado porque algunas de las opciones políticas previstas por la Comisión Europea podrían impactar negativamente y disminuir seriamente los incentivos para invertir en la producción, distribución y difusión de contenidos de las obras audiovisuales de toda Europa.

Mientras que la decisión comercial de distribuir el contenido recae en el proveedor de servicios y/o en la plataforma, no se debe olvidar que la gestión colectiva de derechos es el mecanismo utilizado por muchos autores y en algunos casos intérpretes y productores para negociar las licencias sobre sus obras con los distribuidores.

Cualquier iniciativa en este contexto podría tener un gran impacto sobre su esquema de relaciones con distribuidores y plataformas que son quienes difunden el contenido a los consumidores europeos.

c

Investigación anti-monopolio en comercio electrónico

Como medida para reforzar el impulso del comercio electrónico trasfronterizo y suprimir los geo-bloqueos injustificados (especialmente, de los contenidos digitales) la Comisión ha iniciado una investigación sobre la competencia en el sector, el mismo día de la presentación de la Estrategia del Mercado Único Digital (06.05.2015):

> **5.** La determinación de posibles problemas de competencia que afecten a los mercados del comercio electrónico europeo. Por ello, la Comisión ha iniciado hoy una investigación de la competencia antimonopolio en el sector del comercio electrónico de la Unión Europa.

d

Reducir las cargas administrativas para las empresas.

A nivel fiscal, en particular del IVA, la Comisión planea presentar un Plan de Acción para reducir las cargas administrativas para las empresas europeas y que se derivan de la aplicación de diferentes porcentajes de IVA en los Estados miembros:

> **8.** La reducción de la carga administrativa a que se enfrentan las empresas como consecuencia de diferentes regímenes del IVA: de modo que los vendedores de bienes físicos a otros países se beneficien también del registro electrónico y el pago únicos, con un umbral común del IVA para ayudar a vender en línea a las pequeñas empresas de nueva creación.

El IVA sobre los productos y servicios culturales podría así ser armonizado, aunque la versión preliminar de la Estrategia de la Comisión Europea no alude en ningún momento específicamente al mismo.

e

Convergencia de los Servicios de comunicación audiovisual

Un fenómeno muy importante, recogido en la Estrategia, es la convergencia de los servicios de comunicación audiovisual, que será tratada en el marco de la revisión de la Directiva de servicios audiovisuales:

> **10.** Revisará el marco de comunicación audiovisual con el fin de adecuarlo al siglo XXI, centrándose en las funciones de los distintos agentes del mercado en la promoción de las obras europeas (las cadenas de televisión, los proveedores de servicios audiovisuales a la carta, etc.). Se estudiará asimismo la forma de adaptar las normas vigentes (la Directiva de servicios de comunicación audiovisual) a los nuevos modelos empresariales para la distribución de contenidos

f

Análisis de las Plataformas en línea

La Comisión conducirá una investigación sobre el papel de las plataformas en línea en el mercado actual y en particular, su responsabilidad con respecto a los contenidos en internet.

> **11.** Analizará exhaustivamente el papel de las plataformas en línea (motores de búsqueda, redes sociales, tiendas de aplicaciones, etc.) en el mercado, abarcando cuestiones como la transparencia de los resultados de la búsqueda y de las políticas de fijación de precios, el uso de la información obtenida, las relaciones entre plataformas y proveedores, y la promoción de sus propios servicios en detrimento de los competidores, en la medida en que no estén ya regulados por el Derecho de la competencia. También estudiará la mejor manera de luchar contra los contenidos ilícitos en Internet

6 | 3.Conclusiones: La Propiedad Intelectual ante el Mercado Único Digital

Debe ponerse en valor el papel de los contenidos culturales en el desarrollo de la economía del conocimiento, y el carácter competitivo de Europa en la producción de estos contenidos. En este sentido, no se debe perder de vista el impacto de negocio que los bienes creativos debieran tener en un mercado digital único desarrollado, tal y como se está demostrando en otras economías desarrolladas.

La UE debe ser consciente de los nuevos modelos de negocio existentes en el marco del derecho de autor y los cambios tan rápidos que se producen en los mismos en la era digital. Así, la adopción de iniciativas para conseguir un mercado lo más adaptado posible a dichos modelos, desde el punto de vista del titular de derechos, del usuario y del consumidor deviene fundamental, de tal manera que, en el marco del mismo, sea posible por un lado incentivar la creación y por otro lado éste resulte lo suficientemente atractivo para la inversión tanto de capital comunitario como de terceros países.

En el marco del incentivo a la creación, la UE debe ser consciente del papel que juegan los diferentes actores en la cadena de valor, e intentar conseguir un equilibrio entre los mismos. No es posible obviar aspectos en la era digital como el nuevo papel del consumidor como creador o el rol que pueden desempeñar unas excepciones o limitaciones equilibradas a los derechos de autor en entornos tales como la educación o la investigación considerados claves para el correcto desarrollo de la economía del conocimiento, si bien respecto a este último aspecto es posible entender que la Directiva 2001/29/CE de Derechos de Autor permite un cierto margen de actuación a los Estados miembros.

En el terreno del mercado digital único como ámbito atractivo para una mayor inversión que redunde igualmente en una mayor creación de contenidos culturales, la UE debe seguir trabajando para implantar políticas de transparencia, evitando situaciones discriminatorias de unos agentes frente a otros, reduciendo costes y fomentando, en la medida de lo posible, sistemas de licencias accesibles, sencillas y equilibradas respecto a derechos de autor, que favorezcan tanto al titular del derecho como al usuario.

Sería conveniente promover una mayor armonización regulatoria de los principios y conceptos más relevantes en materia de derechos de propiedad intelectual y apoyar la actividad de la COM en el ámbito de la lucha contra la vulneración de los derechos de propiedad intelectual.

Una mayor armonización regulatoria debería priorizar la observancia de los derechos de propiedad intelectual en el ámbito digital, incrementar la seguridad jurídica de los titulares de derechos y de los agentes intervinientes en el sector de los contenidos digitales, incluidos tanto creadores de contenido, distribuidores y terceros intermediarios.
Se debe priorizar asimismo la reducción de los costes y la complejidad de las transacciones transfronterizas.

La citada armonización deberá tener como objetivo lograr un efecto positivo en el crecimiento de la economía de los contenidos creativos en Europa, considerando para ello los nuevos escenarios que abren las TIC en la forma de generar, distribuir y consumir contenidos digitales.
Lo anterior se deberá realizar garantizando la protección de los titulares de derechos, fomentando el dinamismo y los incentivos de la creación intelectual y promoviendo nuevas formas de comercialización de contenidos al servicio de los ciudadanos con un enfoque integrador que tenga en cuenta las fortalezas europeas.

Asimismo, debería apoyarse a nivel europeo una más eficaz lucha contra la vulneración de los derechos de propiedad intelectual. En particular, se debe avanzar en la puesta en marcha de actuaciones denominadas “follow the money” para eliminar los incentivos de las actividades vulneradoras de los derechos de propiedad intelectual.

Al mismo tiempo, es necesario matizar y dotar de garantías a la obligación de colaboración de terceros intermediarios, medios de pago y publicitarios, en la lucha contra la vulneración de derechos de propiedad intelectual en Internet. Asimismo es conveniente impulsar, en el marco de la colaboración público-privada, el desarrollo de códigos de conducta publicitaria para la protección de los derechos de propiedad intelectual en el entorno digital.

No es creíble que se quiera desarrollar un mercado único digital si no existe una mayor armonización en ciertas materias.

Problema de autores extranjeros que, en aplicación de los límites al derecho de autor que existe en sus países solicitan inscripción de obras intelectuales, pero que, conforme a la normativa española requieren autorización de los autores o titulares de las obras incorporadas.
Por ejemplo, el derecho de cita que es muy restrictivo en España, obliga a denegar inscripción de obras de otros países (ej. Francia) en los que sí son lícitas.

Urge armonizar los límites y crear uno similar al “fair use” norteamericano, que amparen los usos inocuos de contenido que no causan daño al titular de derechos.

Mayor seguridad jurídica que mejore la tutela de los derechos de propiedad intelectual y, con ello, la lucha contra la piratería, favoreciendo el negocio de los contenidos lícitos en Internet, sin cercenar de forma injustificada el desarrollo de otros negocios digitales.

Capítulo 7

Internet abierta y neutralidad de red

Coordinación: **Zoraida Frías Barroso**

Editores/Autores: **Zoraida Frías Barroso, Carlos González Valderrama, Angel León**

Grupo de Trabajo:

Maite Arcos Sánchez (Directora de Relaciones Institucionales/Orange)

Víctor Domingo (Presidente/ Asociación de Internautas)

Zoraida Frías Barroso (Investigadora/ETSI de Telecomunicación, Universidad Politécnica de Madrid)

Carlos González Valderrama (Investigador/ETSI de Telecomunicación, Universidad Politécnica de Madrid)

Ángel León (Vocal Asesor/ Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información)

Gonzalo López- Barajas (Manager Public Policy and Internet/ Telefónica)

Miguel Pérez Subías (Presidente/ Asociación de Usuarios de Internet)

7 | 1.Introducción

El año 2014 ha sido sin duda un año intenso como pocos en materia de Gobernanza de Internet. Tanto la privacidad – con las llamadas revelaciones de Snowden¬ – como la gestión de recursos críticos – con la declaración de intenciones del Departamento de Comercio de Estados Unidos de transferir la supervisión de las funciones de IANA a la comunidad internacional multistakeholder – han acaparado buena parte de la atención en la esfera internacional durante este último año.

Estas cuestiones no han eclipsado sin embargo el omnipresente debate sobre la neutralidad de la red y la Internet abierta que poco a poco va evolucionando. La naturaleza del debate en relación con la Internet abierta y la neutralidad de red resulta difícil de abordar desde un enfoque nacional, presentándose en este capítulo una revisión global.

El último año se ha caracterizado también por su intensidad legislativa a este respecto tanto en Europa como en Estados Unidos. En septiembre de 2013, la Comisión Europea presentaba una propuesta de Reglamento de Mercado Único de Telecomunicaciones, que trata cuestiones de neutralidad de red y que ha sido debatida en el Parlamento durante los primeros meses de 2014, encontrándose en mayo de 2015 en el Consejo. En Estados Unidos, el 2014 comenzaba con una resolución de la Corte de Columbia estimando parcialmente una apelación de Verizon contra la Orden de Internet Abierta adoptada por la FCC en 2010, anulando las reglas de no bloqueo y de no discriminación establecidas en dicha Orden. Así, el intenso debate durante todo el año ha desembocado en una regulación de la FCC en febrero de 2015, que reclasifica el servicio de acceso a Internet de banda ancha como servicio de telecomunicación.

Internet ha permitido la consolidación de un ecosistema con muy bajas barreras de entrada y altas dosis de innovación. La creación de una red de redes sobre la base de estándares abiertos y redes de acceso ubicuas y a precios cada vez más bajos ha propiciado el desarrollo de infinidad de aplicaciones y servicios en constante evolución. Por eso, la naturaleza abierta de la red constituye para muchos su esencia y la característica más importante que preservar.

Sin embargo, la definición de Internet abierta no resulta unánime y se interpreta de modo distinto a lo largo de toda la cadena de valor de Internet por diferentes agentes y en distintas regiones. Así, los países en vías de desarrollo reclaman la esencia abierta e integradora de Internet a través del simple acceso a la Red, mientras que en países con regímenes autoritarios el debate se centra más en la censura y la libertad de expresión, siendo para los países con marcada política exterior un importante elemento de influencia geoestratégica y económica. De otro lado, mientras los desarrolladores de contenidos y aplicaciones aspiran a garantías de libre acceso a redes con una calidad de servicio suficiente para desarrollar sus servicios, los operadores de redes reclaman la aplicación de las mismas reglas para todos los elementos de la cadena de valor, basadas en la libertad de acuerdos comerciales entre empresas que les permitan desarrollar nuevos modelos de negocio.

Por último la neutralidad de red es vista por parte de los usuarios como sinónimo de seguir disfrutando de acceso a un creciente universo de innovaciones y nuevos servicios con pleno respeto a sus derechos, pero de forma simultánea perciben nuevos cuellos de botella más allá del acceso a Internet, hasta ahora una de las principales limitaciones. Mientras tanto, los reguladores afrontan el dilema de hasta qué punto deben adoptar medidas específicas o bien perfeccionar aquellas de las que ya se dispone para las diferentes facetas de la cuestión.

Uno de los aspectos más relevantes del debate sobre la neutralidad de la red es sin duda la gestión de los diferentes tipos de tráfico, que ha evolucionado durante el último año en dos sentidos. En primer lugar, a raíz de las advertencias de los agentes inversores se está alcanzando cierto consenso sobre el hecho de que para la prestación satisfactoria de distintos servicios se necesitan distintos requisitos calidad de servicio y, consecuentemente, la gestión de tráfico para cada uno de ellos. Es decir, algunas posiciones defensoras del «igual trato a todos los bits» se han ido moderando, y este debate se ha ido desplazando en dos vertientes.

Por un lado, hacia cuestiones relacionadas con la protección del ciudadano mediante el control de spam y tráfico indeseado, así como así como la interceptación legal de las comunicaciones más allá de la mera telefonía y las llamadas de emergencia.

Por otro lado hacia temas relacionados con el derecho a la competencia, exigiendo una no discriminación por parte de los proveedores de acceso Internet ante servicios con requisitos técnicos similares en términos, por ejemplo, de latencia o capacidad. Además, el debate en torno a este principio de no discriminación se ha extendido a todos los eslabones de la cadena de valor de Internet, de manera que ninguno de ellos pueda actuar como gatekeeper o “portero”, haciendo abuso de poder al condicionar a los usuarios finales sobre qué productos finales debe utilizar o limitando de forma práctica su oferta.

El primer debate internacional de gobernanza de Internet de 2014 tenía lugar en Sao Paulo los días 22, 23 y 24 de abril bajo la convocatoria del ICANN y el Gobierno de Brasil en la Cumbre Mundial multipartita sobre Gobernanza de Internet NETmundial. Esta cumbre ha sido muy valorada por la comunidad internacional por su capacidad para generar un documento de principios de gobernanza de Internet y una hoja de ruta para la evolución del ecosistema de gobernanza de Internet, a pesar de no tener ningún carácter vinculante.

Sin embargo, no se halló consenso en la problemática relacionada con la neutralidad de la red, por lo que apareció en el documento como tema de debate futuro. Sí aparecieron muchos aspectos de alto nivel relacionados con la Internet abierta, como la protección de los mismos derechos online y offline, incluyendo el derecho de acceso a la información, o la promoción y uso de estándares abiertos que permitan una red interoperable, que dé acceso a todos y facilite la innovación.

Por su parte, el foro de debate europeo sobre Gobernanza de Internet, EuroDIG, que tuvo lugar en Berlín los días 12 y 13 de junio de 2014, organizó una mesa redonda sobre la Internet abierta bajo el título «Neutralidad de red a lo largo de toda la cadena de valor TIC: de las redes a las plataformas» que tenía como propósito ampliar el debate de la neutralidad a todos los agentes que operan en Internet, pero en la que la discusión se mantuvo bastante enfrascada en la parte de conectividad y acceso físico, hallándose cierto consenso en relación con la necesidad de favorecer en Europa la competencia en nuevos mercados en toda la cadena de valor, falto sin embargo de enfoque.

Durante la celebración en septiembre de 2014 del IGF en Estambul quedó patente el consenso mencionado sobre la necesidad de gestionar el tráfico para permitir la innovación con servicios novedosos que requieran prestaciones diferenciadas. Así, el propio Vinton Cerf, vicepresidente de Google, admitía que «neutralidad de red no significa que cada paquetes deba ser tratado igual». No obstante, el debate encontró posiciones muy enfrentadas. La novedad, sin embargo, es que se percibe cierto desplazamiento a las cuestiones de Internet abierta y de la necesidad o no de regular para fomentar la competencia. Así, uno de los temas estrella fueron los acuerdos de zero rating de algunas tarifas de acceso móvil de banda ancha, especialmente en países en vías de desarrollo, por los que algunos proveedores de servicios (como Facebook o Google) acuerdan patrocinar el consumo de datos de sus servicios, de manera que no se descuenten del volumen mensual contratado por el usuario, viéndose estas prácticas como una oportunidad para promover el acceso de los usuarios a los servicios de Internet pero, al mismo tiempo, como amenaza para que dichos servicios se monopolicen por los agentes que los patrocinan.

Resulta evidente que existe amplio margen de interpretación acerca de qué va y qué no va en contra de una Internet abierta. Por ello, no debemos entender el concepto de “la Internet abierta” como un dogma absoluto, sino que debemos ser conscientes de los compromisos que aparecen al profundizar en su concepto, siendo conscientes de la estructura técnica y de mercado que hay detrás del acceso a una Internet abierta. El debate da todavía mucho de sí.

7 | 2 Neutralidad de red

7 | 2 | 1 Evolución del debate en Europa

En Europa la regulación de los servicios de comunicaciones electrónicas se desarrolla a nivel nacional, si bien las actuaciones de los distintos reguladores deben regirse por la normativa comunitaria -compuesta por diferentes directivas- entre las que destacan las del llamado "paquete telecom" de 2002 y posteriormente enmendado en 2009. A pesar de que la Directiva 2009/140/CE incluye una provisión específica que hace referencia a "la capacidad de los usuarios finales para acceder y distribuir información o ejecutar las aplicaciones y los servicios de su elección", prácticamente la totalidad de la regulación existente en Europa hasta la fecha en relación con la neutralidad de la red y la Internet abierta tiene carácter expost.

Sin embargo, en septiembre de 2013 la Comisión Europea presentó una propuesta de Reglamento de Mercado Único de Telecomunicaciones[1] que recogía algunos aspectos relacionados con estas cuestiones bajo las provisiones relacionadas con la armonización de los derechos de los usuarios.

A pesar de que la propuesta de la Comisión prohibía expresamente las prácticas de bloqueo o degradación de contenidos recibió duras críticas por parte de los defensores de la neutralidad de red por permitir a su vez los acuerdos comerciales entre los agentes de servicios de acceso a Internet.

[1]http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013PC0627&from=EN

> **Artículo 23** – Libertad para suministrar y hacer uso del acceso a una Internet abierta, y gestión razonable del tráfico […]
>
> **2.** Los usuarios finales también serán libres de celebrar acuerdos relativos a la prestación de servicios especializados con una mejor calidad de servicio con proveedores de comunicaciones electrónicas al público o con proveedores de servicios, aplicaciones y contenidos.
>
> Con el fin de hacer posible la prestación de servicios especializados a los usuarios finales, los proveedores de contenidos, aplicaciones y servicios y los proveedores de comunicaciones electrónicas al público tendrán libertad para celebrar acuerdos entre sí a fin de transmitir los correspondientes volúmenes de datos o tráfico como servicios especializados con una calidad de servicio definida o una capacidad dedicada. La prestación de servicios especializados no menoscabará de forma recurrente o continuada la calidad general de los servicios de acceso a Internet. […]
>
> **5.** Dentro de los límites de los volúmenes de datos o las velocidades de los servicios de acceso a Internet acordados contractualmente, los proveedores de servicios de acceso a Internet no restringirán las libertades previstas en el apartado 1 mediante el bloqueo, la ralentización, la degradación o la discriminación de contenidos, aplicaciones o servicios específicos ni de clases específicas de estos, excepto en los casos en los que sea necesario aplicar medidas razonables de gestión del tráfico. Las medidas razonables de gestión del tráfico deberán ser transparentes, no discriminatorias, proporcionadas […].

Los más críticos esgrimen que la priorización positiva resulta equivalente a una discriminación de tráfico por proveedor de contenido, lo que altera la competencia y va en contra de los principios que se asocian a la neutralidad de la red.

En marzo de 2014, la Comisión de Industria, Investigación y Energía (ITRE) del Parlamento Europeo presentaba un informe al Parlamento con una propuesta[2] de modificaciones a la propuesta de la Comisión, que cubría cuestiones de la neutralidad de red con la intención de reforzar las garantías en diferentes aspectos.

Este informe de la Comisión de Industria, Investigación y Energía añade en los considerandos (cuyo valor es interpretativo) respecto al texto de la Comisión Europea una definición de neutralidad de red[3], y pone mayor énfasis a través de modificaciones en el articulado en la exigencia de que la prestación de los servicios especializados no debe degradar la calidad general de la prestación de los servicios de acceso a Internet, y para que no se emplee la gestión de tráfico para discriminar a los servicios que compitan con los ofrecidos por el proveedor de acceso a Internet, reforzando por otra parte los poderes de supervisión y control de cumplimiento de las Autoridades Nacionales de Reglamentación, a través de un artículo específico. Así, la Comisión ITRE modificaba el primer punto del artículo 23 sobre la "libertad para suministrar y hacer uso del acceso a una Internet abierta y gestión del tráfico".

> "**Artículo 23.1**. Los usuarios finales tendrán derecho a acceder a la información y contenidos, así como a distribuirlos, ejecutar y suministrar aplicaciones y servicios y utilizar terminales de su elección, con independencia de la localización del usuario final o del proveedor o de la localización, origen o destino del servicio, información o contenido, a través de su servicio de acceso a Internet."

[2] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0190+0+DOC+PDF+V0//ES

[3]Considerando (45) Internet se ha desarrollado en las últimas décadas como una plataforma abierta de innovación […]. El principio de «neutralidad de la red» en la Internet abierta significa que todo el tráfico de Internet debe recibir el mismo trato, sin discriminación, restricción o interferencia, independientemente de su emisor, receptor, tipo, contenido, dispositivo, servicio o aplicación.

En relación con la existencia de servicios especializados, el texto de la Comisión ITRE explicitaba la prohibición de que fueran usados para discriminar entre servicios en competencia.

> Considerando (49) […] Cuando se celebre este tipo de acuerdos con el proveedor de acceso a Internet, el proveedor debe garantizar que la mayor calidad de servicio no supone un detrimento sustancial de la calidad general del acceso a Internet. Asimismo, no deben aplicarse medidas de gestión del tráfico de manera que se discrimine entre servicios competidores.
>
> **Artículo 23.2.** Los proveedores de acceso a Internet, los proveedores de comunicaciones electrónicas al público y los proveedores de servicios, aplicaciones y contenidos serán libres de ofrecer servicios especializados a los usuarios. Esos servicios únicamente se ofrecerán si la capacidad de la red es suficiente para prestarlos además de los servicios de acceso a Internet y si no suponen un detrimento sustancial de la disponibilidad o la calidad de los servicios de acceso a Internet. Los proveedores de servicios de Internet a los usuarios no discriminarán entre los servicios.

A pesar de estas propuestas, los defensores más acérrimos de la neutralidad de red en el Parlamento reclamaban que profundizara en las enmiendas sobre la propuesta de la Comisión en las siguientes líneas:

- Mayor refuerzo de los principios de no discriminación
- Mayores garantías para que las prácticas de gestión de tráfico en las redes no interfieran en la calidad de los servicios de acceso a Internet.
- Limitación a la capacidad de celebración de acuerdos entre operadores de acceso a Internet y prestadores de servicios especializados.

El texto finalmente aprobado en primera lectura por el Parlamento Europeo el día 3 de abril de 2014[4] recogió cambios en este sentido, y ha sido percibido por muchos como un gran avance en materia de neutralidad de red. Así, el artículo 2.2 recogía la definición de neutralidad de red tal y como había sido introducida en los considerandos por la Comisión ITRE, que debía aplicar a la de servicio de acceso a Internet. Las mayores diferencias radican quizá en la exigencia para que los servicio especializados se ofrezcan sobre capacidades diferenciadas de la utilizada para la prestación del servicio de acceso a Internet de manera que no menoscaben su calidad[5]y la eliminación de los artículos de las referencias a la posibilidad de que operadores de acceso y prestadores de contenidos celebren acuerdos.

Tras la votación del Parlamento Europeo, el texto pasó al Consejo donde está siendo debatido por los Estados miembros, cuyo enfoque se basa en enumerar una serie de principios cuya aplicación, dando cierto margen a las autoridades nacionales, garantizaría a los usuarios la neutralidad de red y no discriminación

Las principales diferencias con el Parlamento son que la propuesta del Consejo[6], para tener un alcance más general, no incluye definiciones de “neutralidad de red” ni de “servicio especializado”, y no exige que éstos se ofrezcan sobre capacidades diferenciadas del acceso a Internet, permitiendo además mayor flexibilidad a la gestión de tráfico, en particular autorizando trato diferenciado a servicios con requisitos de calidad diferentes.

[4]http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0281+0+DOC+XML+V0//EN

[5]Ver definición de “servicio especializado” en el punto (1.5) del artículo 2.

[6]http://data.consilium.europa.eu/doc/document/ST-6482-2015-INIT/en/pdf

7 | 2 | 2 Evolución del debate en Estados Unidos

En Estados Unidos, la idea de la Neutralidad de Red en un texto regulador aparece con las Computer Inquiries, serie de documentos de la Comisión Federal de Comunicaciones (FCC) que pretenden promover la libre prestación de servicios de transmisión de datos sobre las redes de telecomunicaciones tradicionales en un entorno de competencia en este último mercado aún emergente.
La Telecommunications Act de 1996[7], que modifica la Communications Act de 1934, cuyo objetivo es impulsar la competencia en la prestación de todo tipo de servicios de comunicaciones, recoge por otra parte los principios de las Computer Inquiries establece dos categorías de servicios:

- **Servicios de telecomunicaciones:** referido a la oferta de servicios de telecomunicaciones directamente al público, o a aquellas clases de usuarios que puedan hacer efectiva la puesta en disposición al público, con independencia de las infraestructuras usadas.

- **Servicios de información:** referido a la oferta de capacidad para la generación, adquisición, almacenamiento, transformación, procesado, recuperación, uso o puesta en disposición de la información a través de las telecomunicaciones incluyendo la publicidad electrónica, pero sin incluir el uso ni la capacidad para la gestión, control u operación de cualquier servicio de telecomunicaciones.

[7]http://transition.fcc.gov/telecom.html

Desde el punto de vista conceptual la principal diferencia entre ambos tipos de servicios radica en la exigencia de algún tipo de procesado de la información para que un servicio pueda calificarse como "de información", mientras desde el punto de vista normativo se ejerce mayor intensidad reguladora sobre los servicios de telecomunicaciones. Así, mientras que para ellos la ley recoge disposiciones para el establecimiento de medidas y control por parte de las administraciones locales y la federal junto con la FCC, y exige que su prestación se realice en condiciones transparentes e iguales para todos sus usuarios, y con tarifas definidas[8], mientras que los servicios de información no se encuentran sujetos a estas exigencias de la regulación.

Al encontrarse en aquel momento el principal cuello de botella para la competencia en las redes de acceso telefónicas, la Telecommunications Act obliga a los operadores de estas redes a ofrecer acceso a sus centrales locales a sus competidores, para que puedan ofrecer cualquier tipo de servicio de telecomunicación. En este momento se considera a los servicios de acceso a Internet como servicios de telecomunicaciones, impulsando de modo su competencia a la par que la de los servicios telefónicos, ya que los operadores alternativos pueden incorporar en sus ofertas servicios de ADSL.

Sin embargo, vistas las dificultades en la aplicación práctica de estas obligaciones de acceso y el éxito de las redes de cable para competir con los operadores telefónicos tradicionales, desde 2002 y hasta el año 2006 la FCC realizó un cambio de paradigma sobre el funcionamiento de los mercados de comunicaciones, decidiendo que se basaría en una fuerte competencia en infraestructuras que fomentase el despliegue de nuevas redes con mayores capacidades. De esta forma, durante estos años la FCC desplegó un proceso de desregulación que dio lugar a la reclasificación de los servicios de provisión de acceso a Internet de banda ancha como servicios de información. Este proceso comenzó inicialmente en las redes de cable[9] para extenderse posteriormente a las redes telefónicas tradicionales[10] con la eliminación de la obligación de permitir que terceros ofrezcan ADSL sobre las redes de acceso de los operadores telefónicos, consiguiendo un equilibrio en las condiciones de competencia entre ambos tipos de infraestructuras.

[8]Este conjunto de obligaciones subyacen bajo el concepto de "common carrier", que se refiere a las personas físicas o jurídicas que transportan personas o bienes de los que son responsables y que ofrecen servicios al público en general bajo licencia o autorización de un órgano regulador y que, según la definición de la Ley de Comunicaciones, es inherente a cualquier prestador al público de servicios de telecomunicación.

[9]http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-220835A1.pdf

[10]http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-150A1.pdf

Lo anterior derivó en menor competencia en la prestación de servicios de banda ancha, surgiendo el temor de que desde su posición reforzada los operadores de acceso limitaran el acceso a Internet. Al no poder imponer condiciones directamente sobre estos operadores por estar considerado un servicio de información, la FCC publicó en 2005 el Internet Policy Statement estableciendo los "cuatro derechos"[11] de los usuarios en relación con los servicios de acceso a Internet, que guiarían su actuación en las disputas que se plantearan entre los operadores de acceso y los proveedores de contenidos sobre Internet.

La validez de este enfoque fue recurrida en el caso Comcast[12], determinando en 2010 el Tribunal[13] que la FCC carecía de autoridad para imponer obligaciones a los proveedores de servicios de acceso a Internet mediante decisiones individuales como la citada. Por ello, en diciembre de 2010, la FCC adopta la Open Internet Order[14] codificando los principios recogidos en el Internet Policy Statement en nuevas reglas, que se aplican de forma diferente a los segmentos fijo y móvil, dada la baja maduración del mercado móvil en el momento que se toma la decisión y se sintetizan en las siguientes:

1. Regla de transparencia
2. Regla de no bloqueo en redes fijas, referida a cualquier tipo de servicio o aplicación.
3. Regla de no bloqueo en redes móviles, que sólo prohíbe el bloqueo de servicios que compitan con los servicios de voz o videotelefonía ofrecidos por el operador móvil
4. Regla de no discriminación, aplicable únicamente a las redes fijas
5. Regla de gestión razonable de la red, que se aplica con mayor flexibilidad a las redes móviles.

Tras varias idas y venidas, en julio de 2012, Verizon apeló[15] las normas relativas a la Open Internet[16] ante un tribunal federal. La Corte de Columbia emitió su resolución en enero de 2014[17], estimando parcialmente la apelación de Verizon quedando en consecuencia derogados los principios de no bloqueo y de no discriminación contemplados por la orden de la FCC. En efecto, el argumento principal esgrimido por el tribunal radica de nuevo en la falta de competencia de la Comisión para regular de este modo la provisión de servicios de acceso a Internet pues, tal como estaban formuladas estas reglas, equivalen a la imposición de obligaciones de "common carrier" que no pueden ser aplicadas a estos servicios mientras que estén considerados como servicios de información y no como servicios de telecomunicación.

[11]Derecho a acceder a cualquier contenido legal, a usar cualquier aplicación o servicio legal, a conectar cualquier dispositivo legal que no dañe la red, y a beneficiarse de la competencia entre proveedores de red, de aplicaciones y servicios y de contenidos

[12]https://apps.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf

[13]https://www.eff.org/files/Comcast%20v%20FCC%20(DC%20Cir%202010).pdf

[14]http://www.law.cornell.edu/cfr/text/47/part-8

[15]https://www.cdt.org/files/pdfs/VZBriefs/Verizon_Metro_PCS_brief_Verizon_v_FCC.PDF

[16]http://www.fcc.gov/openinternet

[17]http://www.cadc.uscourts.gov/internet/opinions.nsf/3AF8B4D938CDEEA685257C6000532062/$file/11-1355-1474943.pdf

De forma paralela a esta decisión, Netflix, una empresa de contenido audiovisual en Internet estaba empezando a sufrir problemas en la transmisión de su contenido a través de los principales operadores estadounidenses. Estos operadores a su vez argumentaban que sus redes se encontraban congestionadas debido al espectacular aumento en el tráfico que debían transmitir, siendo Netflix el origen de más del 30% de este, y que sufrían todos sus usuario. De esta forma exigían a Netflix una compensación económica en caso de querer disponer de mejores conexiones con sus clientes finales.

Ante esta situación en mayo de 2014 la FCC abre un periodo de consulta pública sobre una propuesta de legislación para la regulación del acceso a Internet[18], que se extiende hasta septiembre, proponiendo como salida a las objeciones planteadas por el tribunal una formulación más relajada de las reglas de no bloqueo y no discriminación. Concretamente, esto permitiría que operadores de acceso y prestadores de servicios sobre Internet negociaran las condiciones dentro de los límites de no discriminación que establecen las "prácticas comercialmente razonables". Por este motivo, la propuesta resultó fuertemente criticada y fue vista por muchos como un paso atrás en materia de neutralidad de red al entenderse como la consagración del enfoque de "Internet de dos velocidades".

En este debate el gobierno de Obama se ha posicionado abiertamente y en diferentes ocasiones del año en favor de la neutralidad de red[19,20], pidiendo adoptar reglas más fuertes para su protección mediante la clasificación de los servicios de acceso a Internet bajo el enfoque de los "common carrier" implícita a la regulación de los servicios de telecomunicaciones bajo el Título II de la Communications Act.

«No hay peajes en las autovías de Internet» ha sido uno de sus mensajes en alusión a su defensa de la priorización pagada de contenidos, junto con la que ha defendido la necesidad de reglas de transparencia, no bloqueo y no discriminación, que ha considerado que no entran en conflicto con la necesidad de una gestión razonable de la red, ni con la existencia de servicios especializados, como por ejemplo, los de hospitales. No obstante, Obama ha insistido en que la decisión última estaba en mando de la FCC, una agencia independiente.

[18] FCC, In the Matter of Protecting and Promoting the Open Internet http://www.fcc.gov/document/protecting-and-promoting-open-internet-nprm

[19] https://petitions.whitehouse.gov/petition/restore-net-neutrality-directing-fcc-classify-internet-providers-common-carriers

[20] https://www.whitehouse.gov/net-neutrality

La inclusión del servicio de banda ancha de acceso a Internet bajo el Título II supone, para los proveedores de servicios de acceso a Internet el sometimiento de Internet a una regulación de principios del siglo XX, que terminaría dañando la esencia abierta de Internet, la competencia y la innovación. Así, los ISP han venido intentando terceras vías durante 2014 con estrategias de regulación que permitieran la no discriminación de tráfico, pero que no supusieran la aplicación del Título II a sus servicios. Para otros, sin embargo, que el servicio de acceso a Internet sea considerado servicio de telecomunicación y quede al amparo del Título II de la Ley de Comunicaciones proporcionaría un entorno legal más estable para la FCC para hacer cumplir su legislación, dados los precedentes.

La regulación se aprueba finalmente con la orientación propuesta por la Administración Obama en votación el 26 de febrero de 2015, con los votos a favor de tres comisarios frente a dos en contra.

Esta regulación de la FCC define el servicio de acceso de banda ancha a Internet (BIAS, Broadband Internet Access Service) como:

> “Un servicio minorista orientado a un mercado de masas[21] que mediante tecnologías alámbricas o inalámbricas proporciona la capacidad para transmitir y recibir datos hacia y desde todos los puntos de Internet, incluyendo las capacidades inherentes y que permiten la operación del servicio de telecomunicaciones, excluyendo los servicios dial-up.”

[21]Comercializado y vendido para clientes domésticos, pequeños negocios y otros clientes como colegios y bibliotecas. Se excluyen los servicios prestados a grandes empresas

Estos accesos no incluyen redes privadas virtuales (VPN), redes de distribución de contenidos (CDN), alojamiento o almacenamiento de datos, o servicios de backbone de Internet. También se excluyen aquellas redes WiFi personales no intencionadas para la prestación de estos servicios a otros usuarios. Sin embargo, la definición se estos servicios sí incluye el intercambio de tráfico de Internet de un edge provider o intermediario con la red del operador.

Otra de las mayores novedades es la introducción del mismo tratamiento a las redes fijas como para las móviles, cuyo mercado consideran ya suficientemente maduro.

Por otro lado, la FCC considera que todos los servicios que no estén dentro de la definición anterior, pero se presten sobre el mismo medio físico, pueden ser catalogados como Non-BIAS, algo equivalente a los servicios especializados o gestionados de Europa.

Las reglas de la FCC que aplican al nuevo servicio de acceso a internet de banda ancha (BIAS) disponen:

- **No bloqueo.** Los usuarios que pagan por una conexión de acceso a Internet deben tener acceso a todos los destinos legales de Internet. Por tanto:

> “En la provisión de servicios de acceso a Internet, no podrán bloquearse contenidos, aplicaciones ni servicios legales, ni dispositivos que no perjudiquen el funcionamiento de la red, sujeto a prácticas razonables de gestión de red.”

- **No ralentización.** La regla de 2010 contra el bloqueo contenía una prohibición subordinada contra la degradación de contenidos, aplicaciones, servicios o dispositivos legales, que equivaldría al bloqueo. En este caso, se ha creado un principio separado:

> “En la provisión de servicios de acceso a Internet, no se podrán menoscabar o degradar contenidos, aplicaciones ni servicios legales, ni dispositivos que no perjudiquen el funcionamiento de la red, sujeto a prácticas razonables de gestión de red.”

- **No priorización pagada.** La priorización pagada hace alusión a la gestión del tráfico de la red de manera que se beneficia a un contenido particular aceptando el proveedor de servicios de acceso a internet un pago (monetario o de cualquier otra forma) como contrapartida. Para evitar las llamadas “vías rápidas” la FCC dispone:

> “La provisión de servicios de acceso a Internet no podrá involucrar priorización pagada, refiriéndose a la gestión de la red de un proveedor de banda ancha para directa o indirectamente favorecer algún tráfico sobre otro, incluyendo las técnicas de redistribución, priorización, reserva de recursos u otras formas de gestión de tráfico preferente, bien (a) como contrapartida de una retribución (monetaria u otra) de una tercera parte o (b) para favorecer a una organización asociada.”

No obstante, la FCC señala que podría permitir esta práctica en casos excepcionales si el solicitante consigue demostrar que dicha práctica beneficia al interés público y no daña la naturaleza abierta de Internet.

Por otro lado, el texto señala dos cuestiones adicionales con fin de limitar la capacidad de los operadores en actuar sobre las elecciones de los usuarios y para la mejorar la transparencia e información al consumidor.

- **No interferencia injustificada:** Los operadores no podrán interferir contra la capacidad de los consumidores y de los edge providers para seleccionar, acceder y utilizar la banda ancha para comunicarse. Un caso de especial relevancia es el patrocinio en el uso de datos (zero rating) mediante el cual el tráfico de un determinado servicio no se descuenta del volumen mensual contratado. Debido a los argumentos a favor de estas prácticas como los peligros de distorsión de competencia que pueden generar se ha decidido no legislar sobre estas prácticas sino analizarlas caso por caso bajo los criterios de no realizar una interferencia injustificada.

- **Transparencia mejorada:** La Regulación de la FCC reafirma la importancia de la transparencia acerca del acceso a Internet que están contratando, de forma que los proveedores de servicios de la Información[22] sepan si sus servicios funcionarán como se anuncian.

> “En la provisión de servicios de acceso a Internet se deberá revelar información precisa sobre las prácticas de gestión de red no se podrán menoscabar o degradar contenidos, aplicaciones ni servicios legales, ni dispositivos que no perjudiquen el funcionamiento de la red, sujeto a prácticas razonables de gestión de red, su rendimiento y los términos comerciales de los servicios de acceso a Internet de manera que los usuarios puedan tomar decisiones informadas en relación con el uso de ese servicio y para que los proveedores de contenidos, aplicaciones, servicios y dispositivos puedan desarrollar, anunciar y mantener sus ofertas en Internet.”

Estas reglas no resultan conceptualmente muy diferentes de las anteriores salvo por la no distinción entre servicios fijos y móviles. La diferencia radica en que la posición legal de la FCC es ahora más fuerte. Sin embargo, no conviene descartar nuevos desafíos en la regulación del acceso a Internet, pero no sólo del acceso, si no de Internet en su conjunto tras la aprobación de estas nuevas reglas.

[22]Edge providers

Posiciones de los distintos agentes

Así, se han sucedido las reacciones de distintos agentes, habiendo gracias discrepancias entre las valoraciones de unos y otros, como es natural.

Los operadores han criticado fuertemente la regulación alegando que ha resultado una intromisión del gobierno en un sector caracterizado por su libertad e innovación. Son comunes las alusiones a la creación de los grandes servicios de Internet remarcando la total libertad que existía en Internet en el momento de su creación.

Otros han alzado la voz en relación con las implicaciones que podría tener la reclasificación del servicio en lo referente a la privacidad de las comunicaciones. La Communications Assistance for Law Enforcement Act (CALEA)[23] exige que toda red de comunicaciones, hardware, software y equipamiento sea diseñado para que pueda ser intervenido por las fuerzas de seguridad a nivel local, estatal y federal.

En el momento de su aprobación esta ley aplicaba solo a las redes de telefonía pública pero en 2004 tras una solicitud del departamento de Justicia, la FCC añadió las redes de banda ancha y VoIP. En dicha ampliación se estableció explícitamente que CALEA solo se podía imponer sobre los operadores de telecomunicaciones y que excluiría a los servicios de información.

De esta manera, la decisión de la FCC podría fomentar los argumentos ya expuestos por el FBI para que los servicios prestados a través del servicio de acceso a Internet (email, redes sociales, P2P) estén sujetos a CALEA.

[23]http://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act

En lo referente al impacto que esta normativa tiene en los modelos de negocio de los operadores observamos que las reacciones son muy distintas en función de si el operador es fijo o móvil. En un primer momento podríamos pensar que dicha decisión condiciona en mayor medida a los operadores móviles, que hasta la fecha gozaban de una regulación más ligera, pero las mayores quejas están proviniendo de los operadores fijos.

Los operadores en el mercado fijo estadounidense son los más damnificados de la regulación aprobada ya que puede llegar a comprometer la viabilidad de algunas inversiones, mayores que la de los operadores móviles, por la obra civil que involucran. La priorización pagada había sido vista por los operadores como una posible nueva fuente de ingresos. Ante esta medida, los mayores operadores, liderados por AT&T, Comcast y Verizon, han realizado declaraciones en las cuales afirman que esta decisión puede provocar una menor inversión para el despliegue de las redes de nueva generación, ya que afecta a la rentabilidad de las mismas.

Por otro lado destaca el posicionamiento de T-Mobile y Sprint, ambos operadores móviles puros, que han hecho público que no están especialmente preocupados por el documento de la FCC, aunque todavía tienen que realizar un análisis detallado del mismo. En la misma línea, ambos operadores han confirmado que dicha normativa no afecta de forma sustancial a su negocio y que, por tanto, no se ven comprometidas sus inversiones en el sector. Finalmente, T-Mobile ha expresado su confianza en que las tarifas zero-rating, como el programa "Music Freedom[24]", serán permitidas tras su estudio individualizado como indica la normativa.

[24]Programa por el cual los clientes pueden consumir música en streaming procedente de una docena de proveedores sin que dicho tráfico se contabilice dentro del volumen de descarga mensual.

Posibles desarrollos del debate

La aprobación de la FCC de la reclasificación bajo el Titulo II ha sido una decisión muy controvertida, existiendo grandes discrepancias a nivel político, por lo que se prevé que sus detractores exploten todas las vías disponibles para la derogación de la norma.

Por un lado, a pesar de que la FCC sea una agencia independiente, existe una gran discusión sobre la posible influencia de la Casa Blanca sobre la FCC para la toma de dicha decisión. Obama instó públicamente a la FCC[25] a que tomase esta decisión por lo que se está realizando una investigación sobre la posible influencia del gobierno en la agencia[26].

El partido republicano, a su vez, ha mostrado su total oposición a la aprobación de estas medidas habiendo expresado esta opinión públicamente. Además, los Republicanos tienen el control de las dos cámaras legislativas, por lo que podrían proponer una legislación que anule la norma de la FCC aunque muy probablemente Obama ejercerá su derecho veto impidiendo la actuación por esta vía.
De todas formas, aun cuando los Republicanos no pudieran sacar a delante dicha legislación, los proveedores de banda ancha pueden demandar la decisión de la FCC ante los tribunales[27]. El recurso ante los tribunales de una decisión de la FCC sigue la línea de la decisión de Verizon en 2010 de cuestionar la autoridad de la FCC en imponer normas relacionadas con la neutralidad de red, y se espera que pueda extenderse durante un año alcanzando el Tribunal Supremo estadounidense.

Finalmente, al haber sido una decisión tan ajustada, 3 votos frente a 2, no descartan que dicha decisión pueda cambiarse en un futuro próximo por la propia FCC.

[25]http://www.fiercetelecom.com/story/president-obama-throws-support-behind-fccs-title-ii-broadband-reclassificat/2014-11-10

[26]http://www.fiercetelecom.com/story/report-wheelers-net-neutrality-rules-come-under-fcc-inspector-general-inves/2015-03-18?utm_medium=nl&utm_source=internal

[27]http://www.reuters.com/article/2015/03/19/us-usa-internet-neutrality-idUSKBN0MF01V20150319

7 | 3 Internet abierta

Merece la pena recordar que el debate sobre la neutralidad de la red no es sino parte del debate sobre la naturaleza abierta de la Red. El propio Presidente Obama, en su carta de 10 de noviembre de 2014 en apoyo a la propuesta de la FCC habla del éxito de los servicios de telefonía en la creación de un espacio neutral, aludiendo a las reglas de interoperabilidad y no discriminación, que él mismo asegura que debería aplicar a la transmisión de información.

> "For almost a century, our law has recognized that companies who connect you to the world have special obligations not to exploit the monopoly they enjoy over access in and out of your home or business. That is why a phone call from a customer of one phone-company can reliably reach a customer of a different one, and why you will not be penalized solely for calling someone who is using another provider. It is common sense that the same philosophy should guide any service that is based on the transmission of information — whether a phone call, or a packet of data."

La esencia del debate sobre la Internet abierta se apoya en el espíritu abierto, colaborativo, transparente e interoperable con el que nace Internet y que dio lugar a la creación de una red de redes que permitía interconectar sistemas de información muy diferentes, sobre la base de protocolos abiertos que se iban convirtiendo progresivamente en estándares de facto.
En los últimos años, con el advenimiento de redes sociales, sistemas operativos móviles y aplicaciones, los principios sobre los que se desarrolla Internet están siendo puestos en entredicho.

De esta manera, los conceptos de neutralidad se están extendiéndose progresivamente de las redes a los servicios. El debate de la Internet abierta que considerando todos los eslabones de la cadena de valor está tomando relevancia a uno y otro lado del Atlántico, si bien en Europa ha adquirido especial intensidad durante el último año.

Del debate en Europa pueden distinguirse dos planos bien diferenciados en las líneas de discusión. Por un lado, los operadores europeos de telecomunicación reclaman un "terreno de juego equilibrado" (a level playing field) para competir con los servicios de los OTT, muchos de los cuales son sustitutivos de los tradicionales de los operadores de telecomunicación, pero no están sin embargo sujetos a la misma regulación. No obstante, esta cuestión, aunque puede contextualizarse dentro del debate sobre la Internet abierta, se refiere a aspectos más específicos de la situación de la regulación de las comunicaciones electrónicas en el marco europeo, por lo que no se ha tratado en este informe.

Por otro lado, existe una creciente demanda de que los principios de neutralidad de red – transparencia, no bloqueo y no discriminación - se apliquen también a las distintas plataformas que se han consolidado en Internet y a través de las cuales se accede en gran medida y cada vez más frecuentemente a la información y los contenidos.

En este informe se aborda la problemática de la Internet abierta en dos de sus aspectos más esenciales: la competencia en los diferentes eslabones de la cadena de valor de Internet, bajo el marco de los derechos del consumidor, y el respeto a los derechos humanos en la Red.

7 | 3 | 1 Competencia en diferentes eslabones de la cadena de valor

Las externalidades de red que presentan muchos de los servicios que se han desarrollado sobre Internet, en su mayoría no interoperables, han provocado altas cuotas de mercado que algunos agentes han denunciado como regímenes de cuasi-monopolio, debido a la escasa competencia que existe en algunos eslabones de la cadena de valor de Internet por diferentes motivos.

Muchos de los servicios online están controlados por grandes agentes presentes en diversos eslabones, por lo que está surgiendo una nueva integración extremo a extremo (desde los contenidos hasta el hardware con el que el usuario accede a Internet), que algunos consideran que crea “islas” de información y comunicación sobre una red que nació precisamente para solventar este problema.

De esta forma, las redes sociales se han constituido como espacios gratuitos de libre acceso a los que se accedía principalmente a través de la web[28], pero que han conformado un ecosistema propio, con sus propias interfaces que deben utilizar aquellas aplicaciones (APIs) que quieran integrarse en él.

El desarrollo de Internet en movilidad y los avances en los dispositivos electrónicos han propiciado diferentes sistemas operativos móviles que a su vez han conseguido desarrollar nuevos servicios, aportando mejores y más eficientes soluciones que las ofrecidas a través de la navegación web, consiguiendo además que los usuarios paguen por ellas, algo en lo que la web ha fracasado de forma rotunda y continuada. Sin embargo, estos sistemas operativos móviles han acelerado la proliferación de estas denominadas “islas” en Internet, o en cualquier caso de la integración extremo a extremo.

[28]Aunque con el desarrollo de Internet en movilidad y los sistemas operativos móviles, cada vez es más frecuente el acceso a través de aplicaciones

No obstante, la web clásica, sigue siendo la instancia más evidente de la naturaleza abierta de la red, pero cada vez concentra más tráfico en menos actores: los 10 sitios más populares de Internet concentraban el 26% del tráfico de Internet en 2001, en 2006 ya concentraban el 40% y en 2010 ya superaban el 75% de todo el tráfico de Internet.

De hecho, la Comisión Europea y en concreto sus comisarios de Competencia[29] han declarado en diversas ocasiones durante el 2014 que estaban vigilantes acerca de la prácticas de Google por posibles comportamientos anticompetitivos[30], cuestión que Europa viene arrastrando desde varios años atrás en 2011, cuando comenzaron las investigaciones en relación con posibles comportamientos anticompetitivos relacionados con su motor de búsquedas[31,32].

La Comisión remitió a Google el pasado mes de abril de 2015 un pliego de cargos por violar las prácticas de competencia de la Unión Europea al considerar que su buscador sesga los resultados que ofrece en relación con su servicio de comparación de precios en favor de sus propios productos y en detrimento de los productos de la competencia. Google se enfrenta a una multa de hasta el 10% de su facturación.

De forma paralela a la acusación formal de la Comisión, ésta ha iniciado también un procedimiento formal de investigación sobre el sistema operativo Android, que pretende determinar si Google ha dificultado el acceso al mercado de sistemas, aplicaciones y servicios rivales en el mercado móvil.

En cualquier caso, Google se ha enfrentado ya a las mismas acusaciones en Estados Unidos, donde la FTC abrió una investigación en 2011, que se resolvió de forma favorable a Google en 2013[33], quien cedía en cambiar algunas prácticas en relación con las patentes de los dispositivos, su plataforma publicitaria y los resultados de las búsqueda online.

[29]Primero Joaquín Almunia, luego Margrethe Vestager

[30]http://www.abc.es/tecnologia/redes/20140520/abci-google-europa-almunia-201405201543.html
http://www.abc.es/tecnologia/redes/20140630/abci-google-posicion-dominante-youtube-201406301749.html

[31]http://www.abc.es/medios-redes/20130111/abci-bruselas-google-cambie-busquedas-201301102245.html
http://europa.eu/rapid/press-release_IP-10-1624_en.htm

[32]http://europa.eu/rapid/press-release_IP-10-1624_en.htm

[33]https://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc

En relación con las patentes, Google aceptó conceder uso de sus patentes (adquiridas a través de la compra de Motorola Mobility) relacionadas con tecnologías clave para los dispositivos de forma "justa, razonable y no discriminatoria". En relación con la plataforma publicitaria, Google aceptó eliminar restricciones que pudieran evitar la gestión de las campañas publicitarias a través de plataformas competidoras; y finalmente, en relación con el sesgo de las "webs verticales" la Comisión Federal de Comercio consideró que la introducción de la opción de "búsqueda universal", así como otros cambios realizados sobre los algoritmos de Google podían estar justificados como innovaciones que mejoran sus productos y la experiencia de los usuarios, por lo que cerró la investigación a este respecto.

Por otro lado, a pesar de que el Reglamento de Mercado Único de Telecomunicaciones no recoge expresamente cuestiones relacionadas con la Internet abierta más allá de los aspectos relacionados con la neutralidad de la red, las enmiendas del Parlamento Europeo a la propuesta de la Comisión reflejaban la necesidad de abordarlas de manera progresiva en una amplia evaluación y revisión del marco regulador europeo de las comunicaciones electrónicas. En este sentido la enmienda del Parlamento incluye entre los objetivos de la revisión:

- Asegurar que los usuarios de servicios digitales sean capaces de controlar su vida y datos digitales eliminando obstáculos al cambio de sistemas operativos sin por ello perder sus aplicaciones y datos
- Reforzar la promoción de una competencia eficaz y sostenible

[34]Enmienda 229 (Artículo 39, párrafo 1)

[35]https://www.etno.eu/datas/positions-papers/2014/14-28%2007-15-2014%20European%20Telecommunications%20Network%20Operators'%20Association%20ETNO%207521394442.pdf

Algunas posiciones

En cuestiones de competencia, mientras los operadores de telecomunicación reclaman la aplicación de los principios de neutralidad a todos los eslabones de la cadena de valor, los OTT niegan realizar prácticas de abuso de poder.

Así, la asociación europea de operadores de telecomunicación, ETNO, publicó en julio de 2014 y a raíz de la consulta de la FCC un documento[35] con un doble objetivo: establecer los principios que en su opinión debería seguir cualquier política que desee preservar la naturaleza abierta de la Red; y responder a la petición de la FCC de clarificar su análisis sobre el marco legal europeo para la Internet abierta.

Por este motivo, la argumentación de ETNO se refiere en mayor medida a lo que atañe a la neutralidad de la red. En este sentido, considera necesaria la gestión del tráfico para garantizar que los usuarios disfruten de un servicio adecuado y creen que las reglas para la Internet abierta deberían tener en cuenta la necesidad de inversiones.

Aunque el documento está más centrado en la parte de neutralidad de red, ETNO señala que la consecución de los objetivos de transparencia y apertura debería ser una cuestión que concerniera a todos los agentes en todos los niveles de la cadena de valor de Internet, y no solo a aquellos en la parte de conectividad. En cualquier caso, ETNO insta a las autoridades reguladoras a que las medidas que adopten estén orientadas a largo plazo para conseguir que el ecosistema Internet sigue creciendo.

Por otro lado, las plataformas niegan que utilicen su posición de dominio en un eslabón de la cadena para favorecer los servicios que prestan en algún otro. Así, tras la acusación formal de la Comisión Europea de abril de 2015 a Google, la compañía argumenta en su blog oficial[36] que su participación en los diferentes sectores, en relación con las llamadas “webs verticales”, que se centran en categorías específicas de los negocios, como webs de viajes o compras online¸ no ha modificado su posición histórica en los diferentes mercados y de hecho sus servicios de Google Shopping o Google Travel continúan con una cuota de mercado despreciable frente a la de los agentes que lideran cada mercado.

[36]http://googleblog.blogspot.be/2015/04/the-search-for-harm.html

7 | 3 | 2 Derechos humanos e Internet

En relación con los derechos humanos en Internet, la naturaleza abierta de la Red ha permitido potenciar algunos, como la libertad de expresión o la libertad de asociación, pero pone en riesgo otros como el derecho a la privacidad, que en Europa ha sido concebido tradicionalmente como un derecho fundamental.

El ecosistema Internet ha supuesto sin duda un cambio en cómo se ejercen y cómo se protegen los derechos en Internet. Uno de los mayores problemas a los que se han venido enfrentando los Estados con el desarrollo de la Internet comercial ha sido la dificultad de hacer cumplir las legislaciones nacionales que protegen los derechos, dado el carácter global de la Red.

Aunque se está avanzando en este aspecto, sigue siendo uno de los mayores retos a abordar en el futuro y cuya responsabilidad –como ha venido sucediendo a lo largo de la historia de Internet- está siendo compartida por múltiples partes interesadas[37]. Durante el último año, han surgido distintas iniciativas que reclaman la misma protección de los derechos online y offline[38,39].

[37]En gobernanza de Internet se entienden habitualmente cinco partes interesadas: gobiernos, sociedad civil, comunidad técnica, academia y sector privado

[38]De hecho, la máxima es que no exista una diferenciación entre los derechos online y offline

[39]Véase por ejemplo http://www.derechoseninternet.org/

En el contexto de la Unión Europea, Francia está siendo de los países más activos en abordar la problemática y el papel de todos los agentes de la cadena de valor de Internet en el ejercicio de los derechos humanos. Así, el Conseil National du Numérique francés publicó en mayo de 2014 un informe[40] titulado «Platform Neutrality. Building an open and sustainable digital environment» en el que reconoce que las plataformas en Internet juegan un papel crucial en la sociedad digital y la garantía de la neutralidad de la Red, dado su poder de mercado. Así, en él detalla una serie de recomendaciones que considera que deberían ser adoptadas por la nueva Comisión Europea y que constituyen la posición de Francia en el Consejo europeo. Entre ellas, cabe destacar:

- Conseguir garantías de transparencia de las plataformas y de la sostenibilidad de sus modelos de negocio, aumentando la comprensión de su comportamiento como mercados multilaterales.

- Algunas recomendaciones en relación con el uso de datos personales por parte de las plataformas, como por ejemplo, la concesión del control de sus datos al usuario o la limitación de su uso para los fines para los que fueron recogidos.

- Impulsar modelos de desarrollo digital abiertos y construir una sociedad digital basada en los valores europeos, donde mencionan explícitamente la necesidad de revisar el tema impositivo.

El Consejo de Estado francés utilizó esta opinión para la elaboración de su informe[41] de septiembre de 2014 y en él reconoce que “los operadores de comunicaciones electrónicas no son los únicos actores que representan un papel determinante en el ejercicio de las libertades sobre Internet: la situación de las llamadas plataformas debe ser considerada igualmente” y a ese respecto propone la creación de una nueva categoría jurídica, la de plataformas, basada en el hecho de que ofrecen servicios de clasificación de contenido, bienes o servicios de terceros. El Consejo reconoce que «Las plataformas no pueden someterse a las mismas obligaciones de neutralidad que un operador de comunicaciones electrónicas, ya que su papel es organizar, priorizar o personalizar contenidos […] Por el contrario, las plataformas deben estar sujetas a la obligación de lealtad a sus usuarios, tanto a los no profesionales en el marco de los derechos del consumidor, como a los profesionales en el marco del derecho de competencia. »

[40] http://www.cnnumerique.fr/wp-content/uploads/2014/06/PlatformNeutrality_VA.pdf

[41] http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf

Capítulo 8

La economía de Internet. Innovación y emprendimiento

Coordinación: **Juan M. Zafra**

Editores/Autores: **Juan M. Zafra** (Epígrafe 1), **Benigno Lacort Peña** (Epígrafe 2), **Ignacio Muro** (Epígrafe 3), **Luis Llairó** (Epígrafe 4), **Esteban Egea Sánchez** (Epígrafe 5), **Antonio Fumero, César Ullastres y Luis Galindo** (Epígrafe 6), **Maite Arcos Sánchez** (Epígrafe 7)

Grupo de Trabajo:

Maite Arcos Sánchez (Directora de Relaciones Institucionales/ Orange)

Esteban Egea Sánchez (Vpte. Relaciones Institucionales Poli-TIC, Ex Director de Relaciones Institucionales de IBM, Ex Secretario General de AMETIC)

Antonio Fumero (Head of Marketing/ Beachlanding, Ltd.)

Luis Galindo (Head of Innovation 2.0/Telefónica)

Benigno Lacort Peña (Director General/AMETIC)

Luis Llairó (Vicepresidente Adigital/ Asociación Española de la Economía Digital)

Ignacio Muro Benayas (Presidente de Poli-TIC /ASINYCO Asociación Información y Conocimiento)

César Ullastres (Profesional Independiente. Experto Asesor en Biotecnología e Innovación)

Juan M. Zafra (Profesor/Universidad Carlos III de Madrid)

8 | 1 El reto de la Economía en Internet: crear empleo en un entorno de competencia global

Es necesario establecer un nuevo marco económico y social para extraer el enorme potencial de crecimiento de la productividad que puede suponer la implementación de las tecnologías de la información y la comunicación (TIC) en la economía. Según un estudio de McKinsey Global en los países más maduros en el uso de Internet, el 21% del crecimiento del PIB en los últimos cinco años se ha debido al uso de TIC. Internet crea empleos en unos sectores y los destruye en otros, pero el balance final en las economías que han sabido incorporar las TIC en su modelo productivo es, según este estudio, de 2,6 empleos creados por cada puesto de trabajo estruido. El reto está en encontrar la fórmula que permita incrementar la productividad al tiempo que se crean puestos de trabajo asociados al uso de las TIC, rediseñar los procesos, transformar la cultura corporativa, identificar las nuevas habilidades y promover la capacitación profesional, redefinir la regulación de los mercados y la legislación para fomentar la innovación y el emprendimiento y las relaciones laborales, entre otros factores. Esa hoja de ruta requiere un esfuerzo multidisciplinar, repensar el país para adecuarlo al nuevo contexto digital.

El principal problema en Europa, con especial incidencia en España, y otras regiones desarrolladas y menos desarrolladas del planeta sigue siendo la falta de expectativas para sus jóvenes. Con una tasa de paro del 22%, la UE tiene el enorme reto de crear puestos de trabajo y mantener su competitividad en el entorno de competencia global.

Una de las claves para que Europa retome su posición en el mundo está en las competencias digitales, determinantes para que las economías de los países miembros recobren el pulso, inicien una senda de crecimiento sostenible y generen puestos de trabajo.

Pero, ¿cómo es posible crear empleo en un contexto digital en el que la aplicación de las TIC y la innovación tecnológica no parecen ir acompañadas de tasas de crecimiento como las conocidas hasta ahora y mejoras en la productividad de los sectores?

El progreso técnico y la innovación han sido tradicionalmente la base del aumento de la productividad -aportación al PIB por hora trabajada-. Sin embargo, la tercera revolución industrial, marcada por la generalización de las tecnologías de la información y la comunicación, no parece tener incidencia en la creación de empleo. Antes bien, según un estudio de la Universidad de Oxford, el 47% de la población activa en EEUU tiene un alto riesgo de pérdida de trabajo. Podría decirse que la innovación está teniendo un elevado coste social y también está generando desigualdades.
El esfuerzo debe centrarse en la capacitación, la formación y la enseñanza. El problema atañe no sólo a las nuevas generaciones, los llamados nativos digitales, sino también, y especialmente, a los decisores. “No sólo necesitamos profesionales de las tecnologías de la información y la comunicación (TIC), sino también dirigentes, administradores y empresarios competentes en el ámbito digital en todas las profesiones y sectores”, afirmaba el vicepresidente de la Comisión Europea responsable de Industria e Iniciativa Empresarial, Antonio Tajani.

Sus palabras suponen reconocer que el problema de crecimiento, creación de empleo y competitividad tiene que ver con la falta de visión de los decisores sobre lo que significa la digitalización de la sociedad -abierta, global, interconectada, interdependiente-. La capacidad de las empresas europeas para competir en ese nuevo contexto, y de las españolas en particular, depende cada vez más del uso estratégico de las tecnologías de la información y la comunicación –considerando desde las telecomunicaciones, Internet, el software, los nuevos materiales….-; de la capacidad de que se implementen en todos los sectores y de que los procesos de producción y la organización del trabajo se adecúen a las oportunidades que representan las nuevas herramientas.

La UE asume que la inversión en TIC es una de las que mayor retorno genera en crecimiento y productividad -lo que denomina “Dividendo TIC”-.

Subraya que para la generación de ese dividendo son imprescindibles las inversiones en infraestructuras de banda ancha y acceso, que deben complementarse con otras en capital intangible como:

- La reestructuración organizativa de las empresas, facilitar el acceso y la compartición de la información en las compañías, inveritr en una nueva cultura digital corporativa…
- La rotación y formación continua de los empleados, la aplicación de mecanismos que ligan los salarios a la productividad, las nuevas formas de contratación y de establecimiento de relaciones laborales…
- El marco regulatorio.
- Las políticas públicas de ámbito local.

Señala que los países que más han invertido con esa mentalidad en TIC son los escandinavos y el Reino Unido, con incrementos de productividad del trabajo medios en los últimos 15 años del 1,1% y del 2%, respectivamente. Los que menos han sido Italia y España, con un crecimiento medio de la productividad del trabajo del 0,3% y del 0,8%.

Nuevos perfiles profesionales.

Necesitamos profesionales que sepan utilizar las TIC de forma eficaz, pero es aún más urgente que quienes han de implementarlas en las organizaciones sean conscientes de que sin ellas, la pérdida de competitividad será dramática a medio y largo plazo; el crecimiento y la creación de empleo serán un deseo inalcanzable.

Desarrollar y compartir un modelo orientado hacia la Sociedad en Red, de la Información y el Conocimiento no significa únicamente introducir nuevas tecnologías en los procesos productivos, conectarse a Internet o implementar herramientas que mejoren la eficiencia y la eficacia. Supone que, sin pérdida de tiempo, se deben revisar los modelos de relaciones laborales, con clientes, proveedores y competidores; las categorías y perfiles profesionales; la contratación de nuevos trabajadores con capacidades nuevas y/o adaptadas a la revolución digital; la formación continua; los derechos de los consumidores...

“Es preciso replantear y construir muchas de las organizaciones e instituciones que han cumplido su función durante décadas, pero que han llegado al final de sus ciclos vitales”, señala el Manifiesto de las Competencias Digitales, coordinado por Don Tapscott por encargo de la Comisión Europea.

Para explotar el potencial de la revolución digital que vivimos -todavía en sus albores, aunque resulte difícil de creer- y mantener su posición en el mundo, Europa tiene que capacitar a su población activa en habilidades digitales -desde las plantillas de base a sus más altos ejecutivos-, a las nuevas generaciones -ahora en las fases de educación primaria, secundaria y universitaria- y a sus dirigentes políticos.

Es obvio a estas alturas que Internet no es una amenaza, sino una oportunidad única para reducir los costes, generar riqueza, potenciar la innovación sobre la base de la cooperación en red y desarrollar nuevos modelos de negocio. La Sociedad en Red es un entorno de innovación abierta, conocimiento compartido e inteligencia colectiva que debe potenciar el talento y generar nuevas oportunidades en los mercados globales.

“Es esencial para Europa poder permanecer a la vanguardia de las destrezas en TIC más valoradas en esta competición global y generar mano de obra”, escribe Dan Tapscott, “incluyendo a emprendedores y gerentes que dispongan de un conocimiento profundo de la tecnología y de la cultura de la revolución digital en su propio ADN”.

Se hace, por ello, imprescindible abordar medidas en los ámbitos de:

- Alfabetización digital de la población en riesgo de exclusión. Entrarían en ese grupo las personas mayores, un colectivo cada vez más numeroso para el que el uso de las TIC debe convertirse en rutinario en su relación diaria con la sanidad, la administración y/o su entorno familiar; las personas con discapacidad o aquellas que se encuentran en regiones con menos desarrollo y despliegue de redes.

- Reciclaje profesional en sectores amenazados por la deslocalización, la globalización y el progreso tecnológico.

- Formación continua de los trabajadores para la asunción de nuevas capacidades en un entorno caracterizado por la innovación continua en segmentos como la informática (software, hardware), la robótica, la nanotecnología… La adopción de medidas para garantizar que los profesionales de la UE tengan las altas capacidades necesarias contribuirá a retener y atraer inversiones y a impedir la pérdida de empleos y la deslocalización del talento a otras regiones que se muestran más dinámicas en la adecuación al nuevo contexto digital.

- Revisión de los programas de estudios para incorporar nuevas disciplinas; fortalecimiento de las relaciones de la universidad con las empresas para introducir la empresa en las aulas y para que los jóvenes se hagan una idea del empleo aumentando el aprendizaje en el puesto de trabajo.

- Dotar de un mayor protagonismo a la docencia en todos los niveles educativos – especialmente en la Universidad-.

Según un reciente estudio de Freelancer, uno de los mayores contratadores online en el mundo, se están creando miles de empleos en la Red.
Los perfiles más demandados son los de desarrolladores de aplicaciones (apps), diseñadores, expertos en marketing online y en tecnología 3D. Si la gestión de grandes volúmenes de datos (big data) ha supuesto meses atrás la contratación de un elevado número de matemáticos y expertos en estadística, la disrupción que supone en el proceso de producción la aparición de las impresoras 3D va suponer una revolución en el mercado de trabajo y habrá que estar preparada para ella. Por ello debemos intensificar la formación en ciencia, matemáticas y física.

No significa que no haya lugar para otras disciplinas, más próximas a las letras, las artes, la ética o la filosofía. Es necesario mantener un equilibrio más perfecto entre ciencias y humanidades y, lo que es más importante, es imprescindible abordar la revolución digital con un nuevo espíritu que atañe a todas las disciplinas y no deja ajeno a nadie.

También a la docencia, que debe asumir los nuevos retos y sus profesionales adecuarse a los nuevos requerimientos para aprender y enseñar mejor.

Ahora que se prepara el próximo curso y nos hacemos la lista de los buenos propósitos para la recta final ejercicio en las empresas cuando es importante destacar la importancia de la formación continua, el reciclaje profesional permanente en empresas y organizaciones. Lo que podemos haber aprendido hoy, puede estar obsoleto mañana; la titulación no garantiza un empleo y ni siquiera las capacidades adquiridas podrán sacarnos de un apuro pasados unos meses.

La competencia es mundial, la Red determina un nuevo espacio global y unas nuevas referencias temporales; la competencia se mueve hoy en tiempo real y cada minuto requiere adaptarse a una situación nueva y más compleja que la anterior.

“Lo que más importa es la capacidad de formación continua, de investigación, de documentación, de análisis, de síntesis, de contextualización, de evaluación crítica, de aplicación de lo investigado a la resolución de problemas, de colaboración y de comunicación”, advierte el Manifiesto de las Competencias Digitales.

Androulla Vassiliou, Comisaria de Educación, Cultura, Multilingüismo y Juventud señalaba en el momento más difícil de la crisis, con medidas de austeridad generalizadas y recortes en los presupuestos de educación que “Replantear la educación no es solo cuestión de dinero: si bien es cierto que debemos invertir más en educación y formación, es evidente que los sistemas educativos también deben modernizarse y funcionar de forma más flexible para responder a las necesidades reales de la sociedad actual. Europa solo podrá volver a tener un crecimiento sostenido formando a personas muy cualificadas y versátiles que puedan contribuir a la innovación y el emprendimiento.
Una inversión eficiente y bien orientada es fundamental para ello, pero no alcanzaremos nuestros objetivos reduciendo los presupuestos educativos”.

8 | 2 El poder transformador de las TIC como motor de crecimiento

El desarrollo tecnológico siempre ha jugado un papel fundamental en la historia de la humanidad. No obstante, en los últimos cincuenta años, el cambio tecnológico se ha acelerado de manera espectacular principalmente debido al desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC), que han actuado como driver fundamental para favorecer la consolidación de la Sociedad de la Información. La aparición de los ordenadores personales, el uso masivo de Internet y la evolución de las infraestructuras de banda ancha constituyen hitos fundamentales en la expansión de la digitalización.

Así pues, las Tecnologías de la Información y las Comunicaciones (TIC) han cambiado por completo el paradigma socio-económico a nivel mundial acelerando el proceso de globalización hasta cotas impensables, provocando cambios radicales en nuestra civilización y, consecuentemente, generando nuevos retos de gobernanza.

Desde finales del siglo XX es indiscutible la evolución de la sociedad hacia una sociedad en red[1] basada en el conocimiento y su intercambio. No obstante, para encontrar su origen es preciso retroceder a los años 70, donde se encuentran primeras reflexiones estructuradas[2] en relación a la transición de las economías y las propias sociedades hacia un nuevo paradigma en el que la información debería ser el principal activo.

En efecto, al final de la década de los 70, Estados Unidos y Japón empezaron a considerar que las tecnologías de la información podrían ser la respuesta óptima a los problemas de política pública a los que tenían que enfrentarse en ese momento, principalmente en lo relativo a la crisis energética de Japón y el estancamiento de la productividad en Estados Unidos.

Posteriormente, el resto de países desarrollados comenzaron a diseñar estrategias sectoriales que tomaron el mismo camino, si bien estas políticas no empezaron a ocupar un papel central en el discurso público hasta la década de los 90, sobre todo a partir de la aprobación en Estados Unidos de la agenda para la construcción de una Infraestructura Global de Información, que implicó una decidida apuesta por la sociedad de la información para generar crecimiento económico y bienestar social y que constituyó el hito que marca una nueva era en la concepción de la influencia de la digitalización en la Economía por parte de los poderes públicos .

[1]Castells, M. (2000). The information age: economy, society and culture. Volume I - the rise of the network society. Blackwell.

[2]Crawford, S. (1983). The origin and development of a concept: the Information Society. Bulletin of the Medical Library Association, 71(4), 380–385.

¿Qué son las TIC?

A pesar de la dificultad que supone acotar el concepto, que por su propia naturaleza está en constante evolución, para entender el alcance y el impacto de las TIC es imprescindible definir formalmente a qué nos referimos cuando hablamos de las Tecnologías de la Información y las Comunicaciones.

Las TIC surgen de la convergencia tecnológica de la electrónica, el software y las infraestructuras de telecomunicaciones, cuya interrelación permite nuevos usos de la información. En cuanto a su finalidad, las TIC son el conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento y análisis y presentación de información en cualquier formato y que se distribuyen a través de señales de naturaleza acústica, óptica o electromagnética.

Actualmente, el hipersector TIC deriva de la evolución tecnológica, organizativa y de mercado de sectores que en su momento podían estudiarse de forma aislada pero que con el paso del tiempo se han ido relacionando cada vez más intensamente en un proceso que surgió en los años 90 bajo el nombre de convergencia.

Por tanto, las TIC deben tratarse como un todo, ya que en su evolución se combinan elementos de los sectores de telecomunicaciones, electrónica, informática y audiovisual y la interacción entre estos sectores es continua, en algunas ocasiones para colaborar y otras para competir, desarrollando nuevos productos, ampliando los mercados existentes y abriendo nuevos horizontes y paradigmas.

Según el World Economic Forum[6], un aumento de un 10% en el índice de digitalización de un país genera un incremento de un 0,75% en el PIB per cápita y un descenso del 1,02% en la tasa de paro y en los países en vías de desarrollo, la digitalización podría contribuir a sacar de la pobreza a más de 500 millones de personas en la próxima década. Por su parte, el Banco Mundial[7] concluyó en que un incremento de un 10% en la penetración de banda ancha en los países desarrollados supondría un incremento de un 1,21% en el PIB per cápita, siendo aún mayor su efecto en los países en vías en desarrollo.

Prueba de su potencialidad es que la Economía Digital no ha dejado de crecer a pesar de la coyuntura y el pronóstico[8] es que la tendencia continúe en los próximos años, con un crecimiento medio anual del 5% en los países del G-20 y de un 18% en los países en vías de desarrollo.

Es evidente que las TIC aumentan la eficiencia de las economías mejorando los procesos de producción, creando nuevos productos y servicios, posibilitando nuevas maneras de organización y, sobre todo, eliminando en muchos casos la intermediación entre los consumidores y los productores de bienes y servicios. Su poder transformador es transversal y se manifiesta no sólo favoreciendo el crecimiento económico, sino también en términos de eficiencia, suponiendo un importante aumento de la productividad, impactando positivamente en la sostenibilidad y el medio ambiente y provocando un salto cualitativo en la calidad de vida de quienes las adoptan.

Para aprovechar las ventajas que ofrece la adopción de las TIC, es imprescindible contar con un marco estructural e institucional adecuado, de manera que se potencie la inversión en capital humano e infraestructuras, se favorezca la trasferencia tecnológica, se fomente una cultura emprendedora y se impulse la innovación desde el punto de vista organizativo, de manera que se genere un entorno incentivador que permita maximizar su potencialidad.

[6]WEF, The Global Technology Information Report. Growth and Jobs in a hyperconnected World (2013)

[7]Banco Mundial - Information and Communications for Development: Extending reach and increasing impact (2009)

[8]BCG, The Trillion opportunity – The Internet Economy in the G20 (2012)

8 | 3 Una problemática acuciante. Empleo en la economía de Internet

Cualquier persona que quiera evaluar la contribución de Internet en el bienestar económico general requiere responder a las siguientes preguntas: ¿Por qué el aumento de la productividad de tanto cambio tecnológico radical no ha elevado el nivel de vida de la mayoría de la gente? ¿Y por qué existen dudas razonables sobre si los efectos de la nueva oleada de automatización provoque esta vez una destrucción neta de puestos de trabajo?

Las implicaciones y preocupaciones de este nuevo orden han dejado de ser preocupaciones exclusivas de los tecnólogos para pasar a preocupar a los economistas que empiezan a dudar si el optimista principio de la “destrucción creativa de empleos” se cumplirá esta vez. Las dudas afectan no solo a la cantidad del empleo neto creado sino también a su calidad y se resumen en dos cuestiones fundamentales: si la pérdida de empleos provocada por la digitalización encontrará contrapartida con la creación de otros que equilibrarían la balanza. Y si la tecnología digital será, a pesar de los incrementos de productividad que provoca, una fuente añadida de desigualdad social.

8 | 3 | 1 Tendencias estructurales claramente detectables

Los diversos estudios que analizan la influencia tecnológica en el mercado de trabajo norteamericano suelen utilizar el año 2000 como referente de la consolidación de la nueva ola tecnológica. Esos estudios han ocupado no solo a grandes expertos sino a instituciones de prestigio como el MIT (2012) o el Pew Research (2014). Este último, ha impulsado una encuesta cualitativa entre casi 2000 grandes expertos que debían responder sobre la incidencia estimada del cambio de la automatización de los procesos en el empleo neto en el horizonte 2025.

El periodo que estamos abarcando, sumando experiencias consolidadas desde el 2000 y análisis prospectivo hasta el 2025, se extiende por tanto a 25 años, un horizonte que trasciende lo meramente coyuntural y que señala tendencias de un ciclo largo tecnológico con una cierta consistencia estructural. A pesar de la profundidad de esa mirada el resultado tiene necesariamente componentes parciales, ente otras cosas porque el campo de trabajo utilizado se vuelca principalmente en el mercado de EEUU, líder indiscutido en tecnologías digitales.
Las consecuencias de los mismos fenómenos para los países de la UE y, en mayor medida, para los que como España ocupan posiciones intermedias en la cadena de valor, pueden ser claramente diferentes, empeorando las previsiones al mitigarse los efectos positivos asociados a la creación de empleo y acentuarse los destructivos.

Aunque este trabajo pretende limitarse a exponer los efectos sobre el empleo y el mercado de trabajo, no puede abstraerse de mencionar algunos rasgos esenciales de la revolución en los procesos que incorpora la economía de internet.

8 | 3 | 2 Rasgos esenciales de la economía de Internet

De alguna forma, nos encontramos ante algo parecido a un nuevo taylorismo. Las tareas más complejas, como la programación de una computadora o la redacción de un escrito legal, se pueden ya descomponer en partes y subcontratar a especialistas de todo el mundo, del mismo modo que el taylorismo descompuso, a comienzos del siglo XX, las operaciones mecánicas de la economía industrial.

Si entonces la sistematización de las tareas en secuencias y procesos permitió optimizar la relación entre el obrero y las máquinas, ahora las nuevas tecnologías permiten extender esas experiencias a los procesos intangibles, descomponiendo tareas complejas asociadas al conocimiento en rutinas parciales. Con una diferencia: si la organización científica del trabajo, que así se llamaba el taylorismo, concentraba en grandes fábricas máquinas y trabajadores, hoy las nuevas rutinas asumibles por aplicaciones digitales son ejecutadas por personas aisladas pero conectadas desde fuera de los perímetros organizativos de las empresas, ubicadas en cualquier lugar, próximo o lejano.

El efecto combinado de esos fenómenos (automatización, externalización, deslocalización) aumenta la productividad del trabajo en los servicios mientras trastoca profundamente los perfiles del trabajador y los rasgos del mercado de trabajo. Frank Levy y Richard Murnane planteaban, en su libro (2005) La nueva división del trabajo, cómo las computadoras modifican el mercado laboral que automatización y deslocalización van de la mano; que los call centers se desplazaban de Illinois a India porque el trabajo se puede describir en guiones en la pantalla; que los trabajos de manufactura se mudaban a China porque el trabajo es previsible y requiere poco conocimiento experto.

Cualquier trabajo que tenga rutinas o esté bien sistematizado está abierto a la automatización total o parcial. En esas operaciones el ser humano tiene cada vez menos ventajas. Un ejemplo recurrente se refiere a los mercados de valores, donde los robots de trading automatizado, que trabajan con algoritmos muy complejos con infinidad de parámetros, representan casi tres cuartas partes del volumen de la negociación de acciones de Estados Unidos.

Aunque los cambios revolucionan los subsectores de servicios, una nueva generación de robots de propósito general están además preparados para revitalizar la manufactura. Pero estas nuevas máquinas no están concebidas para unos determinados puestos de trabajo de unas determinadas industrias; son adaptables a diversos tipos de negocios, afectan a tareas comunes a muchos sectores. Es lo que W. Brian Arthur, investigador en el Xerox Palo Alto Research Center y ex profesor de Stanford, llama “economía autónoma”. El cambio es mucho más sutil que la idea de robots haciendo trabajos humanos: engloba “procesos digitales relacionados con otros procesos digitales y creando nuevos procesos”, permitiendo hacer muchas más cosas con menos gente.

8 | 3 | 3 ¿Desempleo masivo o solo cambios en la división del trabajo?

Una mirada al centro tecnológico global, que es EEUU, nos muestra un conjunto extraordinario de empresas tecnológicas lideres: son estadounidenses las diez mayores del mundo por capitalización bursátil (Apple, Google, Amazon, Microsoft, IBM, Intel, Oracle, Qualcomm, Facebook y Cisco), pero también lo son otras “más pequeñas” que lideran sus segmentos de mercado respectivos como eBay, Paypal, Linkedin, Skype, Twiter y Youtube.

Esas grandes compañías generan un ecosistema de pequeñas y medianas empresas en el sector de las aplicaciones, los servicios y los contenidos digitales que está creciendo por encima del 10% anual que tiene una gran influencia en la creación del nuevo empleo. Así, de los 466.000 empleos creados en Estados Unidos durante el periodo 2007-2011, el 40% se ha generado alrededor de la economía digital, que tiene un importante efecto multiplicador, un sector que agrupa aplicaciones móviles, cloud computing, servicios de seguridad, microprocesadores o la venta de accesorios y electrónica de consumo.

Por otro lado la Oficina de Estadísticas Laborales de EEUU proporciona otras pistas sobre los perfiles de los nuevos puestos. Entre las diez nuevas categorías de más rápido crecimiento de empleos entre 2009 y 2011, siete tienen la palabra ciber, digital o software en ellos, de acuerdo con un análisis realizado por Matt Beane, un estudiante de doctorado del MIT. Sin embargo, eso no significa que se refieran a empleos de alta cualificación ni, tampoco, que incorporen planteamientos de una mínima estabilidad, tal como en seguida abordamos.

Resumiendo: si nos referimos solo a EEUU, no es la capacidad de crear empleo lo que está en cuestión, sino los efectos indirectos que la automatización tiene sobre la destrucción de empleo en otros sectores y, especialmente, los perfiles y la calidad y estabilidad del empleo creado. Así, el 52% de los casi 2000 expertos preguntados por Pew Research mostraba opiniones dominantemente pesimistas ya que muchos de los trabajos actuales (especialmente en los campos de asistencia sanitaria, transporte, logística o atención al cliente) serán reemplazados por máquinas.

8 | 3 | 4 El "ahuecamiento" del mercado de trabajo

El economista del MIT David Autor señalaba en 2010 que el mercado laboral se está "ahuecando." Con ese término, al que se han añadido Frank Levy y Richard Murnane y otros expertos, se quiere escenificar la redefinición de los roles funcionales y la polarización del empleo en las economías de la OCDE. Lo que resalta es que las oportunidades de empleo se concentran cada vez más en unos pocos de alta calificación y salarios muy altos dedicados a tareas abstractas y una mayoría de baja calificación, principalmente puestos de trabajo de la industria de servicios en el escalón peor remunerado (preparadores de alimentos, ayudantes de cuidados en el hogar y otros asociados a las diferentes formas de venta).

La misma tendencia señala el MIT en un extenso informe sobre el futuro del mercado de trabajo publicado en julio de 2012. Son los puestos de trabajo intermedios los que están desapareciendo y, con ello, no se apunta solo a profesionales de perfil medio-bajo como asesores fiscales o agentes de viaje, sino también a empleos más cualificados y, en particular, a licenciados que hasta ahora representaban a las profesiones liberales independientes, como médicos o abogados o profesores. Ellos, y otros como ellos, se verán afectados en la medida que realizan trabajos en los que se pueden segregar funciones rutinarias o en los que nuevas aplicaciones puedan asumir tareas del tipo de analizar imágenes o comprender el lenguaje en contextos complejos.

La misma tendencia aparece en el informe del Pew Research ya citado que recoge algunas claves preocupantes en los que existe consenso entre los expertos encuestados: que la próxima ola de innovación no afectará tanto al empleo de obreros como a los trabajadores cualificados "de cuello blanco". Y vuelve a resaltar la polarización en los extremos y el ahuecamiento de los perfiles intermedios: "Ciertos perfiles de trabajadores altamente cualificados tendrán un éxito evidente en este nuevo entorno pero muchos más pueden ser desplazados, en el mejor de los casos, a los escalones más bajos de la industria de servicios o, en el peor, al desempleo permanente".

Existe también consenso de que lo que hoy empieza a ser evidente se acentuará en el futuro con dos consecuencias: por un lado, seguirá ensanchándose el abanico salarial entre los diferentes tipos de trabajadores; por otro, muchos de los empleos perdidos en los últimos años no van a volver.

8 | 3 | 5 Los freelancers, nuevo prototipo de trabajador

Si esa nueva forma de producir acarrea profundas implicaciones en la organización del trabajo también lo tendrá en la naturaleza del contrato social, aunque nada asegura que vaya en una dirección u otra. Lo que empieza a estar claro es la lectura que los think tank y otros centros de pensamiento estratégico empiezan a hacer sobre la evolución del futuro previsible a partir de ciertos datos actuales.

En ellos se destaca que un tercio de la población estadounidense ya está realizando algún tipo de trabajo freelance. Utilizan como fuentes estudios realizados por plataformas conectadas con esos colectivos y, por tanto, interesadas en exagerar tendencias o presentar como positivos los cambios pero, no por ello, rechazables. El trabajo es una colaboración entre Freelancers Unión, una asociación sindical de nuevo tipo, y Elance, la mayor plataforma para contratar autónomos on-line, con más de 3 millones de currículos. Otra fuente, Work Market, también del mismo perfil, vaticina que más de la mitad de los estadounidenses se podrá encuadrar en alguna de las definiciones de freelancer antes de 2020. Con "retraso" esa tendencia hacia el trabajo autónomo también se detecta en España, donde representa ya el 19%, con datos de junio de 2014, pero con clara tendencia a aumentar.

Lo previsible se mezcla en cualquier caso con los deseos hasta construir, sutilmente, "lo recomendable" y, en consecuencia, se empieza a reforzar la idea del freelance como modelo y ejemplo de la libertad del "nuevo trabajador" y, por tanto, la más adecuada a los nuevos tiempos. Desde esa lógica la estabilidad en los ingresos familiares futuros requerirá a los miembros activos asumir "en plena libertad" diferentes trabajos "a tiempo parcial", con horarios dispersos y retribuciones variables que harán más fácil la conciliación de la vida familiar y laboral.

Obviamente no es la única perspectiva. Otra, relacionaría el freelance con el término adecuado para recoger todas las variantes del empleo precario en expansión por todo el mundo.

Incluye, el denominado trabajo a la pieza, un conjunto de servicios que se ofrecen día a día en un régimen de trabajo asociado a la inmediatez, pero incluye también, en su acepción más amplia, a autónomos independientes, pluriempleados y ciertas formas de trabajo a tiempo parcial.

Ambas perspectivas se complementan en la descripción de las tendencias "previsibles" y/o "recomendadas" para las relaciones laborales del futuro en las que se detectan claramente, por un lado, una mayor atomización del trabajo y, por otro, la "necesidad de una mayor desregulación". Una y otra, enlazan, quizás sin saberlo, con el origen del término free-lancer (lanceros libres), al parecer acuñado por primera vez en 1819 por el escocés Sir Walter Scott, que la incluyó en las páginas de Ivanhoe para retratar a caballeros mercenarios de la Europa feudal que no tenían rey ni señor y se vendían al mejor postor a cambio de ciertas libertades.

8 | 3 | 6 ¿Es la tecnología la fuente decisiva de desigualdad salarial?

En este contexto, buena parte de la academia se decanta por considerar a las nuevas tecnologías como el factor decisivo que provoca ya, y va a acentuar en el futuro, los fenómenos de desigualdad salarial. Viene a decir que la brecha creciente que se está produciendo entre diferentes grupos de trabajadores está en función del rol que tienen sus puestos y sus actividades en relación con el cambio tecnológico.

Si la polarización del empleo está homogeneizando los salarios en la parte baja de la tabla de distribución es porque los empleos rutinarios que realizan no pueden ser identificados por sus calificaciones y habilidades específicas ni retribuidos por ellas, sino solo de forma genérica con un sueldo base. Como cada vez más funciones se caracterizan por las operaciones rutinarias de las que no se puede extraer un valor diferenciado, la distribución de sueldos en la parte baja se hace menos dispersa, más homogénea, aplastándose hacia dicho sueldo base. De esta forma, se va generando una igualdad a la baja entre trabajadores diferentes pero homogeneizados por las nuevas rutinas tecnológicas.

Del mismo modo, cuando unos perfiles determinados se escapan de las rutinas impuestas por las nuevas aplicaciones y robots y emigran hacia trabajos analíticos, entran en la élite de los trabajadores muy bien pagados. Esos trabajos están marcados por la capacidad para identificar y resolver problemas o detectar nuevas necesidades que aportan valor a los productos y servicios. En este grupo, las diferentes habilidades individuales son reconocibles y pueden ser remunerados por su productividad marginal, remuneración que el mismo cambio tecnológico se encarga de reconocer y elevar de forma desigual.

Obviamente, tratar la desigualdad salarial descolgada de la creciente desigualdad social provocada por la distribución de las rentas entre el capital y el trabajo, denunciada por Piketty, no deja de ser poner el foco en lo pequeño olvidando lo grande. Se trata de fenómenos convergentes que abordan partes complementarias de una realidad social que no tiene un recorrido trazado de antemano y que ofrece espacios a la esperanza. La esperanza de que, como ha ocurrido en otros momentos históricos, la sociedad encuentre el camino para que se repartan adecuadamente entre capital y trabajo los incrementos de productividad generados por el cambio tecnológico, para que se retribuya adecuadamente cada tipo de trabajo y para que se mejoren los niveles de bienestar heredados.

Ambos fenómenos, consolidan un abanico salarial disperso, con una minoría de trabajadores muy bien remunerados con sueldos más y más desiguales entre ellos mismos y, al tiempo, cada vez más alejados respecto a los trabajadores “aplanados” por las rutinas. En la parte alta, se acentúa la desigualdad entre trabajadores similares desde la perspectiva de su ubicación ante el cambio tecnológico mientras la posición de ese grupo acentúa la desigualdad con “el resto”.

8 | 4 Las capacitaciones en la nueva era digital

¿Cuáles deben ser las capacitaciones para las que hay que prepararse como sociedad y como individuos para no perder el tren de la revolución más intensa que jamás se haya producido en el mundo del trabajo y de la empresa desde la revolución industrial?

Los fenómenos de este cambio ocurren a tal velocidad que no nos da tiempo a percibir su trascendencia. Asistimos a la obsolescencia del conocimiento profesional con una resignación impotente y no identificamos los nuevos vectores de transformación hasta que es demasiado tarde para reaccionar.

Todo se pone en cuestión: los procesos, los comportamientos, las organizaciones, la estructuración de la sociedad, la distribución del poder, la asignación de valor. En pleno proceso de transición de una sociedad industrial a una sociedad del conocimiento y de la información conviven esquemas de funcionamiento de las dos lógicas. La sustitución acelerada de la una por la otra es progresiva e imparable, hay una relación directa entre el cambio tecnológico y el cambio social. Identificar las habilidades de la nueva era digital, formar a los ciudadanos en ellas es el único medio para disponer de mejores empleos. Sólo así se podrán ofrecer perspectivas de una mejor calidad de vida a la sociedad.

Estas habilidades deben corresponderse con las necesidades reales del mercado de trabajo que se transforma a gran velocidad. La sociedad debe poder ofrecer oportunidades a los jóvenes para que hagan uso de todas sus capacidades. Se espera que la educación en capacitaciones en la era digital favorezca que se creen empleos de alta cualificación y alto valor añadido para competir con mayor eficiencia en la economía global, promoviendo el espíritu emprendedor y la innovación.

8 | 4 | 1 Los agentes en la acción formativa de nuevas habilidades

Todos los actores deben implicarse en esta ingente tarea, los propios individuos, las instituciones educativas, las empresas y los gobiernos. Todos son agentes indispensables.

Como ciudadanos debemos anticipar con nuestra actitud personal este cambio de escenario en las formas de organización y en las capacidades que se requieren. Debemos reevaluar en permanencia las habilidades que nos pide la realidad social y poner los recursos adecuados para desarrollarlas y actualizarlas. El impacto en el entorno universitario de los MOOC (Massive Open Online Courses), al alcance de grandes grupos de población, ofrece opciones antes inaccesibles. Es una muestra de cómo será la formación en el futuro: más híbrida, menos reglada. Con una interacción profesor alumno menos presencial, y más electrónica, menos local y más global. Los trabajadores deberemos ser adaptativos y estudiantes a lo largo de toda la vida laboral.

Es tarea inaplazable de las instituciones educativas proponer una respuesta rápida a estas necesidades. El enorme déficit formativo en España no se encuentra entre los titulados universitarios, un 30%, equivalente al de nuestro entorno europeo, sino en la formación secundaria que con sólo un 22%, es la mitad de la media de la OCDE. Es la evidencia de las secuelas lamentables producidas por la devastadora burbuja inmobiliaria. Ahí está el peor fracaso de nuestras “élites”, miopes y egoístas. Y detrás, el fracaso de toda una sociedad que tardará decenios en mitigarse sin un esfuerzo enorme de reciclaje formativo. El inventario de pasados déficits y nuevas habilidades debe ser incorporado sin demora a las soluciones formativas que ofrezcan las instituciones educativas.

Las empresas, conscientes de este cambio de entorno deberían rediseñar su visión a largo plazo del negocio. Romper con cualquier tendencia asociada al negocio fácil, al pelotazo, planificar y desarrollar estrategias que aseguren que están en línea con los requerimientos de la cutura digital, repensar los procesos, crear un clima laboral que permita detectar y desarrollar el talento de sus empleados. Si las empresas se desentendieran de esta responsabilidad, colocarían a sus trabajadores ante el riesgo de obsolescencia de sus habilidades que acabarían penalizando a la generación de negocio y la sostenibilidad de los objetivos empresariales. Para estimular la responsabilidad formativa de las empresas, en algunos países se establecen cuotas mínimas del 1,2% de la masa salarial para presupuesto formativo utilizable en programas concretos para el personal de la compañía, pero que revierten a un fondo colectivo en caso de no ser usados para tal fin.

Es esencial que los profesionales de recursos humanos consigan implicar a las universidades en los nuevos aprendizajes requeridos a lo largo de toda la vida laboral. En nuestro país instituciones universitarias privadas como ISDI, disponen de propuestas formativas para el desarrollo del talento y la adaptación de la organización a los desafíos de la transformación digital. (Ver el modelo KATA de Competencia Digital de Isdi).

Para responder a este cambio de panorama es indispensable que los gobiernos a través sus políticas tomen la iniciativa y el liderazgo haciendo de la educación su prioridad absoluta. Si la educación no es priorizada, cómo ha ocurrido en nuestro país en las dos pasadas décadas, se compromete gravemente la capacidad de preparar a las personas para un futuro sostenible y con oportunidades de desarrollo. La sociedad debe preparar a los ciudadanos en el amplio abanico de nuevas capacidades que se requieren, dando una mayor importancia al aprendizaje continuo y a la constante revisión de las capacitaciones.
El sistema escolar francés tiene ya bien identificadas las competencias para preparar a sus ciudadanos para la era “du numérique” (“digital” en francés) en las etapas equivalentes a nuestros ESO y Bachillerato. La Secretaria de Estado para la economía digital, Axelle Lemaire, reconocía en una entrevista de mayo de 2014 la necesidad de enseñar a programar a los alumnos ya desde la escuela primaria, a los seis años.
Para acelerar la implantación de ese proyecto, aceptaba incluso que se iniciara en periescolar con la participación de asociaciones y empresas, sin esperar a reformular los programas oficiales.

8 | 4 | 2 El trabajador de la era digital

Para responder a las exigencias de la era digital 3.0, el profesor John Moravec en su libro “El Aprendizaje Invisible”, describe la adaptación que han experimentado los que llama “knowmads”: los nuevos nómadas, personas que pueden trabajar a cualquier hora, en cualquier lugar, intensivos en conocimiento y en capacidad de innovación. Saben dónde identificar y resolver problemas, aprovechan las tecnologías para solucionar nuevos desafíos.
Son capaces de trabajar sin barreras geográficas, aprenden permanentemente y desaprenden rápidamente. Y no tienen miedo al fracaso, que ven como una oportunidad de aprendizaje.

Ese perfil del trabajador convivirá con otros más analógicos, forzados a una transición rápida a los nuevos tiempos, también obligados a desaprender sus viejas certezas, a romper sus viejas rutinas. Unos y otros convivirán enfrentados a unas relaciones sociales complejas, sometidas a un caos auto-organizado que sustituye al orden estructurado del pasado. Este nuevo paradigma se caracteriza también por unas relaciones de sinergia por oposición a las viejas relaciones jerárquicas. Nuevos y viejos trabajadores estarán comprometidos con pautas menos colectivas a la manera tradicional, para pasar a otras más mercantiles e individualistas, a la vez que también más colaborativas e interdependientes. El día a día no tiene ya la continuidad del pasado, no hay evolución, hay ruptura, con las consecuentes tensiones desgarradoras en lo personal, social y económico: es la sustitución implacable del viejo modelo. A todos esos cambios disruptivos (neologismo que define esta transición), de destrucción creativa acelerada, y por saltos, responde este nuevo “ser” en el que los nuevos profesionales del mundo digital se presentan como una vanguardia de comportamiento profesional.

Pero unos y otros, los nativos digitales y los aclimatados, están obligados a evolucionar juntos y compartir, de una forma u otra, los cambios que debe soportar el mundo del trabajo y de la empresa en el futuro.

8 | 4 | 3 Los grandes vectores de cambio y en qué modo condicionarán las habilidades profesionales

El IFTF (Institute for the Future) de la Universidad de Phoenix, ha sistematizado los vectores de cambio de las próximas décadas y, sobre ellas, ha identificado lo que considera el "ecosistema formativo" y el desarrollo de las nuevas habilidades que debe acompañar al ciudadano a lo largo de su vida. En lugar de repetir sus conclusiones voy a comentar aquellos elementos que más interés suscitan desde un entorno como el de nuestro país. Entre los seis vectores de cambio que destaca el IFTF el "aumento extremo en la longevidad", en la esperanza de vida, será sin duda un factor distorsionador de primer nivel en nuestro entorno europeo, ya que nos coloca ante el reto de asumir los costes de una creciente población inactiva desaprovechada, y el consiguiente peso creciente del elemento "salud" en la sociedad y en la economía o, como alternativa, encontrar los modos de seguir aportando valor económico en cualesquiera de sus formas. Desarrollar actitudes y habilidades que convivan con esa realidad se convierte en esencial lo que requiere personas con mucha curiosidad, mucha capacidad de aprendizaje, en toda su vida laboral.

El segundo vector que destacaría entre los propuestos por el IFTF sería la evidencia de "un mundo globalmente conectado" en el que la innovación ya no es patrimonio exclusivo de los países desarrollados. De esa evidencia se desprende la necesidad de un pensamiento original y adaptativo ya que, una vez destruidos los puestos de trabajo rutinarios y deslocalizados a otros países los de cualificación media, las oportunidades laborales surgen en los extremos. Tanto en los de alta cualificación en tareas de "abstracción", como en los de tareas manuales, si aportan soluciones originales adaptativas. Encontrar la especialización productiva más adecuada se convierte en esencial.

Ese entorno abierto requiere también nuevas competencias interculturales. No se trata sólo de hablar idiomas, especialmente inglés, sino de ser capaz de colaborar en entornos culturales diversos. Los trabajadores deben disponer de esta competencia perceptiva y de comunicación intercultural para hacer la organización más inteligente.

Un tercer vector a destacar, también resaltado por IFTF, es la prevista “automatización creciente de los procesos”, que tiene dos componentes, por un lado, el “aumento de las máquinas inteligentes y de los sistemas complejos”, y por otro, el “desarrollo del mundo computacional”. Uno y otro nos coloca ante el reto de nuevas adaptaciones, asumir que para ser más eficientes debemos ser más diversos, más complementarios. Aceptar ser reemplazados en muchas tareas por las máquinas, aprender a colaborar con ellas asumiendo las nuevas dependencias mutuas.

Las máquinas inteligentes tienen más memoria y capacidad de proceso que los humanos: el valor humano seguirá siendo el de añadir capacidad de interpretar, dar sentido, significado, reflexión y criterio a lo que las máquinas nos entreguen. De alguna forma supone seguir desarrollando inteligencia social para suplir a las máquinas, a los robots.

Por otro lado, ser capaces de tomar decisiones en base a datos y en ausencia de ellos, desarrollar la capacidad de comprender los conceptos que se explican a partir de los datos, de utilizar simulaciones para entender las respuestas de los modelos de creciente complejidad, se convierte en una habilidad decisiva.

Otro vector que reclama y condiciona nuevas habilidades es lo que el IFTF denomina las “organizaciones superestructura”. El mundo en red cambia las formas de colaboración e impacta el orden clásico de las organizaciones, de modo que su jerarquía estricta es ahora un obstáculo para aportar soluciones a problemas complejos. Las redes sociales permiten una comunicación abierta, el conocimiento está distribuido.

En ese contexto, la transdisciplinariedad se convierte en una necesidad. Es imprescindible ser un buen profesional con conocimientos profundos al menos en una disciplina pero, sobre todo, ser capaz de dialogar y comprender el lenguaje de cuantas más materias mejor para colaborar con expertos en ellas construyendo en equipo soluciones por la suma de conocimientos transversales. Por otro lado, la colaboración virtual exige nuevas formas de socialización en la distancia para ser productivos ya que las habilidades para trabajar en equipos que se relacionan a distancia son específicas y requieren mayor precisión en la identificación de los objetivos comunes o individuales.

El último eje del cambio es la “ecología de los nuevos media”. Vivimos en el mundo de la comunicación, de los contenidos, de las imágenes, que ahora pueden ser producidos desde nuestros propios dispositivos. Los nuevos trabajadores deben estar “alfabetizados” en herramientas como el video, edición de imágenes, presentaciones, para transmitir sus mensajes con capacidad de convencer a sus interlocutores individuales o colectivos. Discriminar la información del ruido, requiere adquirir nuevas habilidades para poder participar en el relato visual de los nuevos “marcos mentales” en los que se construyen nuestras identidades y las actividades empresariales.

Algunos países han comprendido, más que otros, los desafíos formativos de la era digital y preparan a sus trabajadores de hoy y mañana para liderar la reconversión digital.
Han comprendido que las habilidades serán la auténtica “moneda” del siglo XXI, cuyo valor se deprecia o aprecia determinando el bienestar global de las sociedades basadas en el conocimiento. Otros no ven venir la intensidad de la amenaza, retrasan las decisiones y comprometen el futuro colectivo de las nuevas generaciones.

8 | 5 Economía Colaborativa: ¿Sociedades más duales o más integradoras?

La evolución económica del ser humano desde sus inicios de inteligencia hasta hoy se basa en lo que el economista Shumpeter ha llamado “Destrucción Creativa” En efecto, el avance económico y social de la humanidad, se ha basado en las mejoras que la capacidad del ser humano ha introducido sustituyendo -destruyendo- lo viejo para dar pasos adelante creando lo nuevo, en un progreso general en la evolución económica a pesar de los costes que la destrucción de lo viejo siempre conlleva.

Las sociedades que se obstinaron en proteger lo viejo quedaron ancladas en el atraso y la miseria.
Las sociedades que han creado mejores oportunidades y mayor calidad de vida son aquellas que más rápidamente destruyeron “empleo” nómada en beneficio del sedentario (imperios antiguos), quienes aceptaron destruir empleos agrarios en beneficio de los industriales (Inglaterra) y quienes aceptaron sustituir los empleos industriales de menor valor, por empleos de servicios de mucho mayor valor (Estados Unidos). Las sociedades que no quisieron o no supieron sustituir lo viejo creando lo nuevo se condenaron al atraso, la dependencia, el desempleo y la baja calidad de vida.

Hoy, sectores completos de la economía están siendo, de nuevo, “destruidos” y sustituidos por la creatividad de Internet y las nuevas aplicaciones en movilidad.
El comercio, el ocio, el transporte, el alquiler, el cuidado personal y de los dependientes, la salud...todo cambia de forma más productiva a velocidad de vértigo a través de millones de aplicaciones y nuevos modelos de negocio.

Gran parte de la “destrucción creativa” se produce hoy en la rápida y global desintermediación - o más eficiente intermediación - de los servicios y la creación de la llamada “economía colaborativa” que los medios de Internet, la movilidad y su Economía en Red facilitan.

8 | 5 | 1 Definición de EC

Estamos asistiendo a un mutación profunda con respecto al papel tradicional del capital, la propiedad, el trabajo, el consumo y de las relaciones sociales que está cristalizando en una nuevo modelo llamado economía colaborativa (EC) donde la tecnología permite nuevas maneras de conectar, crear y compartir valor, más allá de la tradicional medición de desarrollo económico capturada por el PIB. Como sugiere Albert Cañigueral en su libro “Vivir mejor con menos”, la EC representa un cambio hacia una economía híbrida, “en parte capitalista y en parte colaborativa donde los dos sistemas económicos a menudo trabajan juntos y a veces compiten”.

La economía colaborativa se compone de diferentes aspectos, el consumo colaborativo (compartir uso de coche u oficinas, alojarse con particulares, bancos de tiempo…) es la parte de la economía colaborativa que está creciendo más rápido y facilita la figura del ciudadano productor donde los ciudadanos colaboran, explotan y comparten servicios, bienes, tiempo o conocimiento, por medio del intercambio o trueque, o bien facilitando planteamientos de emprendeduría y desarrollo personal, convirtiéndose en autónomos o pequeños empresarios que prestan servicios o sacan un rendimiento de sus activos infrautilizados alquilándolos o intercambiando tiempo o conocimiento. La ideóloga del movimiento, la británica Rachel Botsman, llega a plantear que “el consumo colaborativo puede tener un impacto similar a la Revolución Industrial”. Igualmente, el economista estadounidense Jeremy Rifkin define y adopta la EC como el nuevo paradigma económico con su idea de la figura del prosumidor, es decir, el ciudadano productor y consumidor.

En efecto, la EC propone nuevos modelos de producción y de organización que difuminan la línea divisoria entre el productor y el consumidor, donde son determinantes la idea de oferta basada en el acceso o uso y compartición del bien improductivo en contraposición a su adquisición. Combinación que unas veces puede basarse en una relación entre iguales, esto es “peer-to-peer”, o bien que una empresa ponga a disposición del usuario el acceso a un bien bajo demanda cuando le resulte más conveniente, “business-to-consumer”. Además del consumo colaborativo, esta economía comprende también aspectos como la Co-innovación, la Ciudadanía Colaborativa (para dialogar con los gobiernos u obtener beneficios individuales o colectivos), el ”crowfunding” o financiación entre particulares, la educación y el conocimiento en abierto y la cultura de los ‘makers’ redefiniendo así la banca, la educación y la producción de bienes.

La EC está cobrando relevancia para un sector creciente de la población. La eficiencia y escalabilidad de estas plataformas, centradas en la comunidad y en la confianza, están creando nuevos mercados que responden mejor a las expectativas y necesidades de ciudadanos y consumidores con un menor nivel de las desigualdades que caracterizan al hiperconsumismo. Parece evidente el elevado potencial transformador de este modelo para asegurar la sostenibilidad de nuestras sociedades desde el triple punto de vista social, económico y medioambiental, pero también el importante impacto sobre las formas de vida de los ciudadanos y los derechos de trabajadores y consumidores.

8 | 5 | 2 Ventajas de la EC

La EC puede incidir en la reducción de las desigualdades y el impacto negativo en el medio ambiente que el modelo económico existente y determinados modos de vida producen, racionaliza los patrones de consumo de bienes y servicios y genera confianza e interacción entre los ciudadanos.

A nivel europeo, Neelie Kroes, anterior Comisaria europea responsable de la Agenda Digital, y otros miembros de la Comisión Europea, han manifestado la necesidad de no limitar estas actividades de la EC por la mejora que representan, en términos de eficiencia, para la sociedad de la información y los beneficios para los consumidores, aspecto este último que ha sido analizado en detalle en un Dictamen del Comité Económico y Social Europeo.

La Comisión Nacional de Mercados y Competencia (CNMC) dice en un reciente informe que la EC genera efectos favorables para la competencia, dando la oportunidad para la desregulación de sectores hiper-regulados y avanzar en marcos normativos racionales y eficientes que sean igualmente garantistas, asignación más eficiente de los recursos infrautilizados, menores costes de transacción y reducción de los problemas de información asimétrica que obligan a los proveedores tradicionales a innovar y a reducir sus márgenes y precios generando mejor y mayor oferta para el consumidor y unos efectos medioambientales positivos al crear una economía basada en el acceso a los servicios y no en la propiedad de los bienes.

8 | 5 | 3 Riesgos de la EC

Desde la perspectiva de la gobernanza, la EC plantea la necesidad de profundas reformas del sistema que van mucho más allá de los espacios de Internet que permiten su desarrollo. Son muchas las cuestiones que debemos resolver a corto plazo. ¿Cuáles son los derechos laborales en una EC?, ¿el ciudadano productor, que tipología laboral tiene?, ¿está a expensas de unas plataformas que en modo alguno se definen como empleadores pero que si pueden determinar el acceso a más, menos o ningún tiempo de trabajo?

La EC es un paso más en los procesos de destrucción creativa que genera evolución económica y social.
Como en todos los casos, la destrucción inicial supone unos perdedores, al menos transitorios (taxistas o conductores de bus, empleos en hoteles, etc...) ¿Qué hacemos para reducir la dualidad ganadores - perdedores que se está produciendo?. ¿Qué nuevas garantías debemos diseñar para los consumidores? o ¿cómo evitar prácticas monopolísticas?

El impacto de la EC y las acciones a tomar por las administraciones públicas en relación a la misma, está ya siendo considerado en todos los países desarrollados.

En este sentido, el Comité sobre la pequeña empresa del Congreso de Estados Unidos reconoció recientemente el impacto de la cultura “peer-to-peer” en la sociedad, el Gobierno británico anunciaba el pasado septiembre un estudio para poder incorporar la EC como prioridad en el modelo económico de Reino Unido y la Unión Europea, a través de la Comisión y del Comité Económico Social, han subrayado su importancia y necesidad. En un entorno donde es tan necesario como difícil cambiar el modelo productivo, España también debe hacer lo necesario para maximizar las oportunidades que el desarrollo de la EC comporta.

Para ello es necesario generar un debate transversal en el que el gobierno, en colaboración con todos los actores implicados, encuentren la forma en la que la sociedad pueda maximizar las ventajas y transformar los riesgos de la EC en oportunidades, poniendo en marcha un plan de acción para la evolución hacia la EC que incluya los cambios regulatorios y presupuestarios adecuados. Los párrafos siguientes desarrollan algunas reflexiones y propuestas para dicho debate.

La rapidez e inevitabilidad del cambio hacia la EC y la consiguiente "destrucción" de la antiguas fórmulas económicas, no significa que el mismo sea instantáneo, ni tampoco que la transición de lo antiguo a lo nuevo a través de la desintermediación o intermediación más eficiente y global de los servicios, sea o no a través de experiencias de la EC, no pueda ser incluso acelerada ayudando a limitar o incluso a transformar los riesgos de la destrucción de lo antiguo que la EC, como toda innovación económica comporta, en nuevas oportunidades.

Si deseamos que la EC nos ayude a construir sociedades más integradoras en vez de más duales, debemos crear un marco para la EC en el que se avance en la igualdad de oportunidades del siglo XXI, con derechos laborales asegurados, con apoyo en la transición a nuevos empleos, con mayores garantías y servicios a los consumidores en un entorno en competencia y fiscalmente más justo, que se desarrolle en un marco jurídico globalmente adecuado para la EC y donde se puedan aprovechar las lecciones aprendidas de lo "viejo" para construir "lo nuevo" y donde "lo viejo" sea capaz de transformarse a si mismo en "lo nuevo".

Un cambio hacia la EC con víctimas, con conectados y aislados, con ganadores y perdedores, una sociedad de nuevos ricos y clases medias empobrecidas, de integrados y marginados que quedan en la cuneta de la vida, no solo es injusto e inaceptable para nuestras sociedades es, también, ineficiente ya que esa sociedad dividida, se convierte en una rémora para el avance del progreso económico y social.

Por eso, nuestras sociedades, sus gobiernos y sus empresas, deben aprovechar la EC para ayudar a crear una sociedad con derechos sociales garantizados, especialmente para los actores de la EC con un nuevo acuerdo social que lleve a normas facilitadoras de la transición que llega, donde los afectados por la rápida evolución hacia la EC sean rápidamente reintegrados a nuevas oportunidades con todos sus derechos sociales garantizados.

8 | 5 | 4 UBER como posible ejemplo de transición

Aunque se suscitan dudas razonables de que UBER pueda ser considerado como un servicio típico de la economía compartida, deseamos utilizarlo aquí como ejemplo de conflicto social reciente que la transición a nuevos modelos de servicio a través de Internet pueden generar, así como de sus posibles soluciones.

El sector del taxi se ve sorprendido por la aparición de UBER, una empresa que a través de una aplicación en Internet permite compartir o utilizar el automóvil privado propiedad de un ciudadano, reduciendo, por una parte, los costes para el usuario y reduciendo drásticamente el mercado de los taxis, en parte por su mayor eficiencia tecnológica y, en parte, por los menores costes regulatorios y los menores derechos y garantias que implica.

El transporte urbano a través del taxi es un claro ejemplo de servicio público estrictamente regulado para garantizar el beneficio de usuarios, taxistas y administraciones públicas pero que, a cambio, genera un mayor coste tanto para todos ellos así como para el tráfico, y la contaminación en la ciudad (circulación en vacio y no compartido…), además, también permite la aparición “de profesionales de UBER” que prestan los servicios de un taxi de forma más eficiente – al menos más barata para el usuario y eficiente para la ciudad- si bien a costa de las ventajas (fiscales, etc) de la administración, de los derechos de los usuarios y de los profesionales del taxi.

Ante ello, la alternativa de la administración pública ha de ser la búsqueda del interés general. Por un lado, so riesgo de quedar anclados en el pasado, no debe impedir que la nueva y más eficiente forma de prestar el servicio sustituya a la vieja regulación del sector del taxi, pero, por otro lado, tampoco puede permitir la aparición de una economía sumergida que reduzca las garantías de seguridad para el usuario y de competencia equilibrada tanto regulatoria como fiscal ni, finalmente, dejar a merced de la destrucción los miles de empleos y de inversiones del sector del taxi.

¿Es posible una solución que, tras la siempre compleja transición, asegure un nuevo equilibrio l? Para ello es necesario conciliar lo mejor de lo nuevo y de lo experimentado aprovechando la ocasión para modernizar el servicio.

8 | 6 Apuntes para la reformulación de una I+D+i industrial en un ecosistema emprendedor

> "La innovación tecnológica, si no es innovación social plena, puede quedarse en pura, estéril y hasta peligrosa maquinaria."
>
> (Fernando Sáez Vacas, en "La Memoria del Futuro", 2001)[9]

Desde que el propio J. Schumpeter acuñara la metáfora de la "destrucción creativa" el rol del empresario, del emprendedor, ha sido la innovación. Se trata de un papel que implica cierta "responsabilidad" social; la cual escapa a la actual popularización de la actividad emprendedora de base tecnológica en general y específicamente la que saca partido de la Internet que conocemos y los fenómenos que marcan tendencia en el ecosistema creado a su alrededor.

Más allá de los titulares, hoy nos interesa destacar dos elementos básicos de la actividad emprendedora en Internet y que caracterizan, en su íntima relación, el impacto socioeconómico de la misma: la tecnología, su capacidad transformadora; y las personas, los innovadores que permiten convertir su potencialidad en verdadera innovación social desde la actividad económica de sus organizaciones empresariales o institucionales.

Hablaremos en este trabajo de un 'ecosistema emprendedor' desde una aproximación "ecológica" que considera la existencia de diversos elementos (individuos, organizaciones, instituciones, etc.) que interaccionan en red sobre la base de relaciones complejas, como por ejemplo la simbiosis. Esa interacción está en la base de la sostenibilidad de las iniciativas que generalmente asociamos al esfuerzo individual de un emprendedor particular. Esta aproximación, que adoptara también en su momento Daniel Isenberg en su popular artículo "How to start an entrepreneurial revolution"[10], será la base de nuestra contribución.

[9]http://oa.upm.es/23475/

[10]Este artículo fue publicado en 2010 por la prestigiosa Harvard Business Review (HBR) y está accesible en la siguiente dirección, https://hbr.org/2010/06/the-big-idea-how-to-start-an-entrepreneurial-revolution/ar/1

El objetivo genérico de esta breve reflexión en clave de ensayo es el de establecer un marco conceptual de partida sobre el que podamos desarrollar, en sucesivas ediciones de este informe, los casos de estudio que vengan a marcar la evolución de la Gobernanza de Internet a lo largo de los ejes de la innovación y el emprendimiento (i+e)[11].

Esta nueva fórmula (i+e) parte de la consideración –propia de autores como Schumpeter o Drucker-, de que la innovación es la actividad propia del rol social del emprendedor. Esto convierte al emprendimiento como una vía especialmente dotada para la transferencia de la innovación y a las startups (o empresas de base tecnológica) en su instrumento dentro de un nuevo sistema de innovación.

Esos dos ejes se encuentran necesariamente en el punto en el que se da esa "conexión creadora" o transformadora entre Tecnología y Personas; algo que en gran parte ocurre debido a que la Tecnología es el logro más humano de nuestra especie[12]. Es precisamente lo que nos convierte en humanos; siendo esta la componente determinante de la innovación y el emprendimiento que, en nuestro marco conceptual, se convierten en procesos de innovación social desencadenados por diferentes roles, como son los del innovador o el emprendedor.

Se trata, en definitiva, de reformular la I+D+i clásica; pretendemos reescribir esa fórmula para poder hablar de una i+e que incorpore los elementos fundamentales de sostenibilidad, complejidad y sistémica que están en la base del proceso de Gobernanza de Internet, que debe entenderse necesariamente como un proceso de innovación social.

Evidentemente, para entrar en materia, nos pondremos en contexto con algunas cifras que aportan fuentes como el INE o Eurostat y que sintetizan los informes de Cotec[13] y el GEM (Global Entrepreneurship Monitor).

[11]Hablaremos consistentemente en este trabajo de innovación y emprendimiento (i+e) destacando la relación simbiótica de ambas actividades; y nos referiremos a esta relación con esta fórmula manteniendo ambas iniciales en minúscula, de la misma manera que se hacía al introducir la 'i' en la tradicional fórmula de la I+D.

[12]Esta afirmación, que no es aventurada, hace referencia a la aproximación del propio Ortega y Gasset a la filosofía de la tecnología en "Meditación de la Técnica" (1939), una obra en la que el autor considera al ser humano un ser técnico en la medida en que "la técnica es lo contrario de la adaptación del sujeto al medio, puesto que es la adaptación del medio al sujeto".

[13]http://www.cotec.es/index.php/pagina/sala-de-prensa/notas-de-prensa/show/id/1033/titulo/cotec-presenta-su-informe-2014-sobre-tecnologia-e-innovacion-en-espana

Según los datos de Eurostat[14], en 2012 solo el 23,2% de las empresas españolas de 10 o más trabajadores introdujeron o desarrollaron alguna innovación tecnológica, casi 13 puntos porcentuales por debajo de la media comunitaria. Tampoco en el apartado de innovación no tecnológica los datos son positivos. Solo el 23,4% de las empresas presentaban novedades en el ámbito de la organización o el marketing, frente al 37,1% de media en la UE.

Los datos del INE muestran igualmente esta carencia por parte de las compañías españolas. Entre 2011 y 2013, solo el 26% de las empresas de 10 o más empleados se consideraban innovadoras. En 2013, dedicaron únicamente el 1,8% de su cifra de negocio a innovación tecnológica, y entre 2012 y 2013 el gasto en este ámbito se redujo un 1,3%.

Hay pocos marcos más rigurosos que el Global Entrepreneurship Monitor (GEM) para medir la actividad emprendedora. Una de sus ratios más significativas es la Tasa de Actividad Emprendedora (Total Entrepreneurial Activity, TEA) que mide las iniciativas de entre 0 y 3,5 años en el mercado sobre la población de entre 18 y 64 años.

Según los datos del GEM 2013, este índice ha experimentado en España un leve descenso, pasando de 6% a 5,2%. Esto ha mantenido al país por debajo de la media europea. Desagregando esta ratio y comparándola con la obtenida en 2012, podemos afirmar que en cuanto al emprendimiento por oportunidad no se observan variaciones, manteniéndose en un 33% (también por debajo de la media europea, que se sitúa en un valor del 47%). En el caso del emprendimiento por necesidad se observa un ligero incremento (del 26% al 29%), lo que indica que se incrementa el número de emprendedores que han tomado la decisión de iniciar un negocio obligados por la situación económica. En este caso, la cifra ara nuestro país se sitúa 7 puntos porcentuales por encima de la media europea.

Así las cosas –y desde un punto de vista siempre pragmático de la modelización-, nuestra aportación a este primer informe quiere abordar la naturaleza sustancial de la innovación y del emprendimiento, destacando los elementos que nos permitan mostrar los casos de estudio que sustentan de manera coherente y consistente esa reformulación de la tradicional e industrial I+D+i en una i+e compleja y sistémica.

[1]http://www.elmundo.es/economia/2015/03/03/54f4b00de2704e181b8b456c.html

8 | 6 | 1 Innovación

A finales de 2008, Bruce Nussbaum, a la sazón, editor de Business Week y actualmente dedicado a la enseñanza en temas de creatividad, además de ser un activo asesor en el Foro de Davos, aseguraba que la innovación había muerto asesinada por el uso excesivo del término, la obsesión por medir la incertidumbre y el fracaso en su evolución.

Definir la innovación no es fácil y hacerlo la limita. La manera de abordar el concepto es conocer de dónde viene y cómo funciona. La innovación no es un término técnico, sino económico y social. Su criterio no es la ciencia o la tecnología, sino un cambio en el ámbito económico y social, un cambio en la conducta de las personas como consumidores o productores, como ciudadanos.

Hasta hace poco, finales del XX, hablábamos de tecnología e innovación como si fueran una misma cosa. Ahora, en pocas ocasiones discriminamos lo uno de lo otro, y entendemos la tecnología como el resultado de la aplicación del conocimiento científico a entender, mejorar o crear procedimientos que sirven a un fin práctico, nuevas técnicas y a la innovación como la puesta en valor de la tecnología.

A mayor abundamiento, en nuestro país, hemos convenido la fórmula I+D+i que si bien incorpora el hecho de que la innovación forma parte de un sistema en la que los tres elementos están interrelacionados, analizar los tres elementos en conjunto lleva a confundir la innovación con la investigación y desarrollo.

Es en sus personas donde reside en primera instancia el conocimiento de la empresa y es precisamente la materialización de ese conocimiento su esencia. Todas las personas tenemos creatividad y capacidad de resolver problemas. En mayor o menor medida todos tenemos habilidades y manejamos ciertas tecnologías. La empresa tiene que potenciar la creatividad de sus personas, transferir y potenciar la capacidad de resolución de problemas de cada una de ellas para materializar lo que saben en forma de productos, modelos de negocio y conocimiento nuevo que son los elementos en los que se basa su existencia en el mercado.

La innovación aglutina el esfuerzo que hacen todos en la empresa efectuar un cambio en su potencial, o para sobrevivir a la competencia. Para sobrevivir hay que tener, a la vez, productos que vender y desarrollos de I+D.

A las empresas les interesa la innovación que genera valor y el valor máximo es el que se produce cuando se ahorra más porque se reducen o eliminan los costes no necesarios para producir y cuando se produce algo diferente que mejora el nivel de lo existente, cuando se consigue un producto o servicio con el que se consigue multiplicar el volumen de facturación.

La búsqueda simultánea de diferenciación y bajos costes exige trabajar en dos planos el primero, la innovación radical o disruptiva que se basa en los descubrimientos y el segundo, la innovación incremental se basa en mejorar lo que actualmente se hace.

Como afirman Tony Dávila y Marc J. Epstein[15], a falta de revoluciones industriales son el desempeño y la capacidad de gestionar la innovación incremental las que determinan vencedores y perdedores. La innovación incremental puede ser una estrategia sostenible durante periodos de tiempo que pueden llegar a ser largos si la estructura del sector permanece estable. Se trata de observar los factores que en el sector están establecidos y, sin embargo, pueden eliminarse y aquellos factores que se deben infra ponderar respecto al estándar del resto de las industrias del sector. La innovación incremental suele responder a estrategias defensivas y las empresas consolidadas es algo que hacen muy bien.

La innovación disruptiva requiere un modelo que fomente los hallazgos y la visión, pone el énfasis en explorar entornos diversos y en fomentar la experimentación tanto con la tecnología como con los modelos de negocio. Se trata de focalizarse en los factores que se pueden sobre ponderar respecto al estándar del sector y en aquellos que nunca se han considerado y deben crearse.

[15]The Innovation Paradox: Why Good Businesses Kill Breakthroughs and How They Can Change, Berrett-Koehler, 2014.

Para que una organización sea verdaderamente próspera a largo plazo deberá ser capaz de apalancar y capitalizar las innovaciones disruptivas en el momento que se produzcan pero sin olvidar innovar de forma incremental construyendo ventajas competitivas día a día.

Descubrir algo que revolucione un sector de forma que se traduzca en un producto o servicio con capacidad de desbancar los existentes que permita a la empresa que lo hace diferenciarse de las del resto de su sector y hacer que todas se fijen en ella cuando comprueban que sus clientes que consideraban cautivos dejan de elegirles a ellos es algo que en los tiempos que vivimos ha dejado de ser excepcional.

La innovación radical es por definición arriesgada y se fracasa a menudo pero lleva intrínseca un gran potencial de crecimiento, se basa en la disciplina, en circunscribirse a un campo pequeño y muy focalizado, en cuestionar nuestros valores y creencias, en la forma en la que creemos como se trabaja en cada sector eliminando nuestras ideas preconcebidas.

Esto implica tener afán por descubrir para lo que hay que generar una permanente conversación hacia abajo que involucre a todas las personas de la empresa, su inteligencia interna, y a las redes externas que se dispongan. Para que haya innovación tiene que haber talento.

José Antonio Marina en su libro seminal “Teoría de la Inteligencia Creadora” afirma, cargado de argumentos, que la realidad adquiere nuevas posibilidades al integrarse en un proyecto inteligente. Tener un proyecto es lo que permite una mirada inteligente que anticipe y prevenga que utilice la información conocida, la reconozca y la interprete. Del mismo modo, para que una empresa sea innovadora, la innovación debe de formar parte de su proyecto empresarial.

8 | 6 | 2 Innovación en sentido amplio

En el cuaderno número catorce del Think Tank de la Fundación de la Innovación Bankinter, “El Arte de Innovar y Emprender. Cuando las Ideas se convierten en riqueza”[16], con un enfoque absolutamente pragmático, dan por buena la definición de innovación de la OCDE incluida en el “Manual de Oslo” de 2005. La OCDE define el concepto de innovación como «la introducción de un producto (bien o servicio) o de un proceso, nuevo o significativamente mejorado, o la introducción de un método de comercialización o de organización nuevo, aplicado a las prácticas de negocio, a la organización del trabajo o a las relaciones externas». Esta definición se ha convertido en el estándar aceptado por los países miembros de esta organización y distingue cuatro tipos de innovación:

- **Innovación de producto**, definida como la introducción de un bien o servicio nuevo o significativamente mejorado en sus características o usos.
- **Innovación de proceso**, definida como la implementación de un método de producción o distribución nuevo, o significativamente mejorado.
- **Innovación de marketing**, definida como la implementación de un nuevo método de marketing que conlleve cambios significativos en el diseño del producto o el packaging, la colocación, las promociones o el precio.
- **Innovación organizativa**, definida como la implementación de un nuevo método organizativo en las prácticas de negocio de la empresa, en la organización del área de trabajo o en las relaciones externas.

[16]Disponible en formato PDF en la siguiente dirección, http://www.fundacionbankinter. org/es/publications/the-art-of-innovation-and-entrepreneurship

Cotec, por su parte, nos propone una definición de "Innovación en Sentido Amplio"[17] en su informe homónimo: "de forma sucinta se puede decir que la innovación es todo cambio que está basado en conocimiento y que genera valor. Esto expresa que la innovación tiene al valor como su meta, al cambio como su vía y al conocimiento como su base".

Sobre esta definición ambiciosa, Cotec, junto con el Club de la Excelencia Empresarial, propone su propio modelo de innovación: el modelo que se propone consta de tres «subarmazones» que se refieren a otros tantos ámbitos de la empresa; cada uno de ellos está formado por elementos cuya existencia formal o informal se requiere para que se dé la innovación. Su nivel de formalidad, los recursos implicados y el grado de compromiso que con ellos asuma la empresa serán un indicador de su capacidad innovadora.

En la práctica, la innovación pasa por sustentarse en un sistema de I+D basado en la organización industrial y que ha querido legitimar la tradicional fórmula de la I+D+i.

En ese sistema, son los investigadores son los que, en última instancia, poseen el conocimiento que dará como fruto la innovación. Las empresas que necesitan de la innovación para cubrir los huecos que satisfagan mejor las necesidades de sus clientes hablan en términos de valor económico. Las universidades, los centros públicos de investigación y los centros tecnológicos están en el medio, facilitando el proceso y, a su vez, bregando para sacar partido a sus siempre escasos fondos.

También tienen interés en todo este proceso lleno de conversaciones, intercambio de información y transferencias los agentes inversores siempre ávidos de colocar su dinero en proyectos con valor añadido y en las nuevas oportunidades del mercado. Por último, el Estado tiene un claro interés en favorecer la innovación, entre otras cosas porque al hacerlo consigue un resultado inmediato. ¡Lo primero que genera la innovación es IVA!

[17]Disponible para descarga previo registro en la siguiente dirección, http://www.cotec.es/index.php/publicaciones/show/id/1946/titulo/innovacion-en-sentido-amplio--un-modelo-empresarial--analisis-conceptual-y-empirico--2010

8 | 6 | 3 Emprendimiento

No hace mucho, escribíamos en un ámbito sectorial específico alejado de Internet que la iniciativa emprendedora es, sobre todo, una forma de pensar o una mentalidad. Incluye la motivación y la capacidad del individuo, bien sea de forma independiente o dentro de una organización, para identificar una oportunidad y luchar por ella y así producir nuevo valor y, en consecuencia, resultados económicos positivos.

La motivación es el resultado de sumar: el deseo, los incentivos para realizarlo y los elementos facilitadores para hacerlo. Para aumentar la motivación es necesario actuar sobre los tres factores. La creación de empresas, tanto como disciplina de estudio e investigación, como tema de actualidad social, económica y política, ha visto incrementado su interés.

El emprendimiento (su estudio teórico) está aún en proceso de definición y la interpretación del mismo aún sigue fragmentada por diferentes puntos de vista de investigación. Basta una breve revisión de la literatura, como la que sintetizamos aquí a partir del trabajo de Rosa Mayoral Castro (Análisis de la creación de empresas españolas basadas en Internet, 2013), para ilustrar la dimensión de este fenómeno.

La revisión de la literatura que se incluye en ese trabajo de investigación nos deja una muestra de la naturaleza multidimensional de este concepto de emprendimiento (entrepreneurship), así como de la variedad de aproximaciones que se han adoptado para su estudio: Kuratko & Hodgetts1 lo definen como “un proceso de innovación y creación con cuatro dimensiones o aspectos relevantes –el individual, el de tipo organizacional, el que define el entorno y el definido por los procesos”. Ma & Tan2 hablan de “una particular forma de pensamiento, una única forma de mirar el mundo, una forma creativa de aventura y el último instrumento hacia la autorrealización y el cumplimiento de la misma”. Shane & Ventakataraman3 lo estudian bajo la óptica de lo que se denomina la función empresarial: que implica el descubrimiento, evaluación y explotación de oportunidades, es decir, nuevos productos, servicios y procesos productivos; nuevas estrategias y formas de organización, nuevos mercados de productos en inputs que no existían con anterioridad.

[18]Enterpreneurship: Theory, Process and Practice. South Western Publishers, 2004.

[19] Key components and implications of entrepreneurship: A 4-P framework. Journal of Business Venturing, 2006.

[20] The promise of entrepreneurship as a field or research, Academy of Management Review, 2000.

Hay aproximaciones “clásicas” que hablan del emprendedor innovador (Schumpeter, J., “The theory of economical development”, Harvard University Press, 1934). En “The Discipline of Innovation”, publicado por la HBR en 1985, P. Drucker intenta establecer la base sistemática y disciplinada que hay bajo la capacidad emprendedora (entrepreneurship). Para este gurú, la característica común que hay detrás de los emprendedores, no es cierto tipo de personalidad, ni una capacidad innata de liderazgo, sino un compromiso personal con la práctica sistemática de la innovación.

Según el autor, la innovación es la función específica del emprendedor; el “emprendimiento” es un tipo de actividad cuyo núcleo está constituido por un proceso sistemático de innovación; que a su vez se define como “el esfuerzo para crear un cambio intencionado en la economía o el potencial social de una empresa”.

La creación de empresas basadas en el conocimiento es el mecanismo más eficaz para pasar de la idea al mercado. Es en este tipo de empresas donde se ejemplifica mejor el hecho de que la empresa es simplemente un medio de la economía para descubrir lo que funciona y lo que no.

El concepto de empresa es una admisión expresa del hecho de que los fracasos son importantes para la economía y que los costes de oportunidad de no intentarlo pueden detener su crecimiento. La empresa el medio más eficaz y, posiblemente, el más económico de demostrar si las ideas tienen verdaderamente valor, en tanto que son de utilidad para el mercado.

8 | 6 | 4 Apuntes para el debate

Cuando hablamos de innovación o de emprendimiento estamos abordando una situación de complejidad en la que, evidentemente, debemos tener en cuenta, como mínimo, elementos organizativos, tecnológicos, individuales (sociales) y de proceso que intervendrán en la propia dinámica de esos procesos de orden intrínsecamente social y estrechamente relacionados con la iniciativa empresarial.

Nuestro análisis aquí -si bien convenientemente argumentado-, ha sido intencionadamente sesgado e interesado. El tipo de experiencias prácticas de las que hagamos acopio deben caber en un marco conceptual basado en el pensamiento sistémico y en la ciencia de la complejidad, además de aportar argumentos para un debate tan necesario como abierto; y del que nos haremos eco en sucesivas ediciones de este informe, así como en los grupos de trabajo organizados por IGF Spain. El objetivo de tal esfuerzo no será otro que el de consolidar una metodología y una dotación instrumental propias que nos permitan analizar el impacto de los procesos de innovación y la actividad emprendedora en la Gobernanza de Internet.

La evolución terminológica, hasta cierto punto retórica en el estudio de la innovación, nos ha llevado a la popularización, desde diferentes foros, de distintos "atributos" de la misma. Se habla, en ese sentido, de innovación abierta (vs. cerrada) o de innovación social (vs. innovación tecnológica). Chesbrough popularizó, por ejemplo, la innovación abierta como término paradigmático con su libro homónimo de 2003[21]: «open innovation is a paradigm that assumes that firms can and should use external ideas as well as internal ideas, and internal and external paths to market, as the firms look to advance their technology».

Nuestra aproximación sistémica es necesariamente sociotécnica; y se puede sintetizar en una afirmación debida a Fernando Sáez Vacas, reconocido pensador e investigador con una dilatada trayectoria en ese ámbito: "la innovación tecnológica, si no es innovación social plena, puede quedarse en pura, estéril y hasta peligrosa maquinaria".

Esta aproximación deja fuera del debate este tipo de atributos y nos lleva a reafirmarnos en nuestra particular formulación de una i+e que solo tiene sentido dentro de un ecosistema emprendedor en red y una situación de complejidad que considera innovación y emprendimiento dos procesos simbióticos que conforman un rol social clave, el del emprendedor.

[21]H. Chesbrough, "Open Innovation: The New Imperative for Creating and Profiting from Technology", Harvard Business School Press, 2003.

8 | 7. La importancia de la regulación en el desarrollo de la economía de Internet

Vivimos una época en la que las telecomunicaciones están revolucionando el entorno social. El teléfono tardó 75 años en ser usado por 100 millones de personas. Internet llegó a la misma cima en tan sólo 7 años. Instagram tardó 2 años. Hace únicamente dos décadas los servicios de empresas que hoy usamos, no sólo a diario, sino constantemente, no existían. Es difícil abstraer y adelantar las consecuencias que tendrán cambios que se suceden a velocidad de vértigo. Y esto probablemente nos lleve en ocasiones a diagnósticos erróneos y desajustes entre las políticas más adecuadas en cada momento. Pero hace ya más de 20 años que nació Internet y este tiempo nos permite distancia suficiente para realizar un cierto análisis.

Viendo las últimas décadas, podemos afirmar que estos enormes cambios han sido posibles gracias a la generalización de unas redes de banda ancha de capacidad creciente. El resultado de la combinación del binomio: decisiones millonarias de inversión de operadores de telecomunicaciones (sólo en España los operadores han invertido 88.000 millones de euros desde 1998[22]), y el modelo regulatorio (para nosotros el europeo, con sus luces y sus sombras) ha permitido que hoy disfrutemos de unas infraestructuras imposibles de imaginar hace tan sólo dos décadas. Se trata de unas redes de banda ancha capilares y que han batido records en su capacidad (En España, el tráfico de Internet fijo crecerá 2,1 veces desde 2013 hasta 2018, una tasa de crecimiento anual compuesto del 16%, y en móvil hasta 9 veces con una tasa de crecimiento anual compuesto del 54%) sin parar de bajar el precio del servicio. Ningún otro servicio de red, y menos aún de inversión privada, ha mejorado tanto la experiencia de sus usuarios.

Estas mejoras se han hecho tan cotidianas y las usamos tan intensivamente, que a veces olvidamos que son la base de todo el ecosistema digital. Esas redes lo han hecho posible.

Nos hemos acostumbrado tanto a tener siempre, hasta en los lugares más insospechados, una conexión que ya no somos conscientes de la cantidad de actividades cotidianas que podemos realizar gracias a que existen unas infraestructuras de banda ancha ubicua y permanentemente a nuestra disposición, para darnos un servicio silente cada instante que le exigimos conexión. Pero esas redes son el corazón del ecosistema digital.

[22]Según datos CNMC 1998-2013

Por supuesto, como cualquier ecosistema, el ecosistema digital sólo es posible en su conjunto. Es decir, los servicios digitales sobre Internet sólo son posibles gracias a que existen una red de banda ancha siempre dispuesta a soportarlos, y simbióticamente, las redes de banda ancha son buscadas con ahínco por los usuarios únicamente porque son el mecanismo por el que les hacemos llegar unos servicios digitales de creciente valor e interés para ellos.

Pero hace tiempo que se avistan negros nubarrones en el horizonte de esta crónica. La facilidad y suavidad con la que los usuarios ven evolucionar los servicios, no tiene reflejo en el backstage. Los inversores en redes de banda ancha compiten encarnizadamente entre sí por seguir garantizando que el corazón de la Economía de Internet siga latiendo con fuerza. Pero esa aportación no es juzgada como suficiente por el resto de agentes de Internet o, incluso, por los propios reguladores. Todos exigen más por menos.

El marco regulatorio nació con la liberalización del sector. En contra de lo que muchos llamaron “desregulación”, lo cierto es que la ruptura de monopolios públicos de telefonía fija trajo consigo un tsunami regulatorio. Y en aquel momento la regulación estaba teñida de tecnología por doquier. La regulación de la telefonía fija era distinta a la de la tecnología satélite, y esta a su vez no estaba relacionada con las obligaciones regulatorias de las comunicaciones de datos o las de la televisión.

El mercado, como siempre, fue por delante de la evolución. Los usuarios son “agnósticos” tecnológicos. Demandan (exigen) conectividad de banda ancha y ubicua, sin importarles qué tecnología hay detrás. Ellos usan servicios, no siglas de tecnología.

Los operadores han respondido.

Los operadores han ido haciendo los cambios de escenario necesarios sin ruido y sin molestias para los espectadores, pero con gran esfuerzo de los tramoyistas. Sin grandes planes de ayudas públicas, ni fechas para "apagados analógicos", ni campañas de comunicación institucionales, los usuarios han ido pasando del modem de 256kbps a la FTTH y de aquellos móviles analógicos en forma de maletín a la telefonía 4G. Todo ello casi sin enterarse. La mayor diferencia que han percibido es que ahora hacen muchas más cosas, utilizan muchos más servicios, gracias a que los precios han caído drásticamente (-71% desde 1998 y un -25% en 2013 respecto a 2012[23])

Y a pesar de ese historial, el desarrollo regulatorio marca con fiereza los servicios de telecomunicaciones.
La telefonía sigue regulada, incluso a veces con métodos sorprendentemente arcaicos (i.e regulación de precios de roaming). Por el contrario, otros servicios digitales no son considerados por los reguladores, simplemente porque no caen dentro de la definición que se hizo hace más de 10 años de las comunicaciones electrónicas. Es más en algunos casos como el citado roaming la voracidad regulatoria llega al extremo de plantearse no reconocer los costes que dichos servicios suponen en realidad para los operadores, llegándose a proponer forzar los mismos precios para dicho servicio que para las comunicaciones domésticas.

Mientras tanto, la realidad se encarga de poner en solfa estas definiciones: el ejemplo más reciente es la oferta del más famoso servicio de mensajería instantánea para hacer llamadas gratuitas. ¿Hasta cuándo la regulación va a poder soportar esta esquizofrenia? ¿y el desarrollo del mercado digital?

Cada vez es mayor el clamor para generar un marco regulatorio realmente orientado al desarrollo de la Economía de Internet, no sólo las telecomunicaciones. La erupción del volcán ya no está en los servicios tradicionales de telecomunicaciones. Los usuarios digitales demandan servicios finales, en cuya prestación intervienen diversos agentes, colaborando en una cadena de valor cada vez más compleja y global. En ese contexto las telecomunicaciones, las comunicaciones electrónicas en nomenclatura europea, ya sólo son una pieza del engranaje. Fundamental, pero solo una parte.

[23]Datos Informe anual CNMC – Ingreso medio de telefonía móvil por minuto aire y por tipo de tráfico

¿Cómo van a proteger los reguladores a los usuarios digitales en ese entorno ampliado, en esa realidad aumentada? ¿Cómo les van a garantizar esos derechos, que se han ido asentando en el mundo de las telecomunicaciones y a los que los ciudadanos ya no van a renunciar? Hagamos un breve repaso de algunas para concretar la idea.

- **Interoperabilidad.** Los usuarios de telecomunicaciones tienen derecho a comunicar con cualquier usuario, no importa cuál sea su país, o su proveedor de servicio. No existen walled gardens, cuando una persona descuelga el teléfono, sabe que puede comunicar con quien quiera con sólo saber su número. No importa si el destinatario está registrado en su misma compañía de telecomunicaciones o no.

- **Portabilidad.** Los usuarios de telecomunicaciones tienen derecho a conservar los datos que le identifican. Si un usuario tuviese que cambiar los datos que le identifican frente a otros miembros de la red (i.e. su número de teléfono) probablemente sería más conservador, no querría cambiar de proveedor. Evitaría pasar por el calvario de comunicar a todos sus contactos que ha cambiado de número.
En ese caso las empresas podrían obtener ventaja de esa posición de fuerza excesiva sobre el abonado y probablemente aprovecharían para presionarle para firmar unas condiciones de servicio en las que se incluyese, por ejemplo obligación de aceptar publicidad. Para evitar este abuso los reguladores obligan a los operadores de telecomunicaciones a poner en marcha los mecanismos necesarios para que el usuario sea el “propietario” de su identidad. Aunque ese derecho está limitado al número de teléfono, no se protege la apropiación del resto de elementos de su identidad digital.

- **Secreto de las comunicaciones.** Los Estados democráticos garantizan que el contenido de las comunicación e inviolable. Tanto que únicamente un juez, en ciertas circunstancias (i.e, investigación policial de delitos) puede violar ese secreto.
Pero en el planeta Internet, de escala global, no hay una autoridad legitimada democráticamente similar. Mientras no lo haya, no decide la sociedad, sino las grandes empresas de Internet, que tienen que suplir ese papel decidiendo en cada caso, según su propio criterio.

- **Seguridad en las comunicaciones.** El actual marco regulatorio garantiza la capacidad de interceptar las comunicaciones y poder conocer el contenido de las ya efectuadas a los órganos de fuerza y seguridad del estado así como a los jueces y tribunales.
En el mundo sin regular de Internet este control es totalmente imposible, no siendo posible conocer el contenido de una comunicación establecida entre un servicio de mensajería sobre la Web, y tampoco es posible garantizar la identidad de los usuarios que las generan. Esto resulta especialmente relevante en el caso, por ejemplo, de los menores que se encuentran completamente desprotegidos frente a las múltiples amenazas que pueden encontrar en la red.

- **Asequibilidad y contribución a objetivos sociales.** En muchos países, desde luego España es un ejemplo evidente, se considera que los operadores de telecomunicaciones deben contribuir a financiar los objetivos sociales, no sólo mediante el pago de los habituales impuestos, sino también mediante instrumentos excepcionales. Entre ellos destacarían dos: el llamado servicio universal y la financiación de la televisión pública nacional.

Se considera que si una persona no pudiera costearse una conexión telefónica, podría correr riesgo de exclusión social. Para evitarlo se exige a los operadores que financien un fondo extraordinario cuyo único fin es garantizar que, por muy deficitario que sea el servicio, todos los ciudadanos tienen, si así lo desean, derecho a un "pack básico" de telecomunicaciones, financiado por el reducido universo de las principales empresas de telecomunicaciones. Algo similar ocurre desde hace unos años en España con la televisión pública. El legislador consideró que las principales empresas de telecomunicaciones deberían financiar RTVE. Tampoco en este caso se considera la publicidad en Internet.

La mayoría de estas medidas nacieron y crecieron en un mundo en el que las telecomunicaciones se desarrollaban en un entorno separado de la televisión y en el que no existía Internet. Pero en la Economía de Internet que nos rodea, en la que existe un enriquecedor mestizaje de servicios y proveedores de servicios, y una involucración de Internet en todos los ámbitos y actividades económicas, es necesario reconsiderar el foco del marco regulatorio y adaptarlo al mundo en el que viven los usuarios digitales: el ecosistema digital, donde se cubran todos los servicios digitales, no solo los servicios de telecomunicaciones.

Los reguladores deberían revisar los niveles de protección de los usuarios digitales y equiparar las que ya disfrutan en los servicios de telecomunicaciones a las de otros servicios, porque en la Economía de Internet los usuarios son digitales, realicen la actividad que realicen, tanto en su ocio como en su trabajo. No son sólo usuarios de telecomunicaciones.

Asimismo es necesario equilibrar las obligaciones impuestas a los diferentes proveedores de servicios, porque si prestan los mismos servicios pero tienen obligaciones distintas el regulador está provocando un entorno de competencia desleal, dañando las posibilidades de las empresas sobre las que haga recaer más obligaciones de forma injusta y desequilibrada. Las protestas de los taxistas frente a lo que se ha considerado competencia desleal de Uber es sólo un ejemplo de lo que los políticos deben afrontar. Es necesario establecer el level playing field en la Economía de Internet.

Con el apoyo de: