V Jornada Anual del

FORO DE LA GOBERNANZA DE INTERNET EN ESPAÑA

27 a 29 de Mayo de 2015
Madrid

Organiza

Con el apoyo de

Coordinan

Colaboran

www.igfspain.com

#igfspain

Tabla de contenidos

Recursos críticos de Internet

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.

Mensajes del foro

Sobre el carácter político de algunas funciones técnicas que desarrolla ICANN.

- La relevancia de la gestión de los recursos críticos que realiza ICANN contrasta extraordinariamente con el poco conocimiento que se tiene de este organismo y de sus funciones para la inmensa mayoría de los usuarios de internet.

- La complejidad tecnológica de estas funciones, así como la complejidad relacionada con los mecanismos de trabajo, los plazos y la toma de decisiones, el hecho de que el inglés sea el idioma dominante y la elevada dedicación que requiere dificultan las posibilidades de participar en los procesos de toma de decisiones.
- Se constata que una parte importante de la actividad de ICANN tiene una dimensión política muy obvia.

La dimensión política de ICANN es también patente en las dificultades para modificar los términos de la relación privilegiada que hasta ahora ha mantenido con el gobierno estadounidense.

- La internalización de la ICANN y la retirada de la tutela estadounidense que realizaba la NTIA sobre las funciones de la IANA se realizará de acuerdo con una serie de principios, entre los que se encuentra la voluntad de que se refuerce el *multistakeholderism* y la participación.
- Este proceso es positivo tanto por su carácter simbólico como por las conquistas en términos de apertura, internacionalización y participación
- Pero hablando de *multistakeholderism*, cabe señalar las dificultades para definir lo que quiere decir la participación "multipartita", pues no todas las partes implicadas o afectadas por las decisiones de ICANN tienen las mismas posibilidades de influir o participar en los procesos de toma de decisiones.
- Algunas entidades de la sociedad civil encuentran grandes dificultades para ser representadas en el proceso de ICANN (lo que hace que no sea de todos) y se encuentran con gastos importantes que hay que afrontar para hacer valer su voz en este foro
- Se observa una voluntad del gobierno estadounidense de que este proceso de transición por el que se desvinculará de ICANN no conlleve la apropiación o un exceso de influencia por parte de otros actores, y especialmente de otros Estados. De un modo u otro, el gobierno estadounidense seguirá teniendo durante algún tiempo una ascendencia e influencia sobre ICANN, pero no de manera formalizada como hasta ahora ha tenido.
- Los borradores de esta transición que hasta ahora han circulado parecen adoptar un carácter conservador, con el que ICANN parece querer "blindarse" de influencias gubernamentales diferentes de la estadounidense.

Apoyo total del foro al proceso de transición, poniendo foco en los grandes retos que se plantean tanto para hacer que siga funcionando aquello que hasta ahora lo ha hecho razonablemente bien para una parte del mundo, como para hacer que el modelo de participación en esta gestión se haga de acuerdo con nuevos parámetros que aporten más legitimidad en cuanto a representatividad y a rendición de cuentas.

Regulación y ciberseguridad

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 ciberdelincuencia 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.

Mensajes del foro

- Totalmente a favor de la regulación en el ciberespacio. el ordenamiento jurídico debe tener una evolución acorde con la evolución de la tecnología, definiendo unos mecanismos que actúen contra la ciberdelincuencia pero no a cualquier precio, se deben mantener los derechos y valores fundamentales de los ciudadanos. Expone una serie de tipos penales ya se contemplan en la legislación actual
- Para poder realizar estrategias para asegurar la protección y seguridad es necesario tiempo, recursos financieros y tecnológicos y capital Humano. A pesar de que España tiene estrategias en contra de la ciberdelincuencia, se necesita realizar estrategias a nivel global, ya que en la ciberdelincuencia no existen fronteras. Además de tratar la ciberdelincuencia a nivel global, es muy importante que los estados tengan claras las amenazas, los riegos y las oportunidades que dicha

ciberdelincuencia plantea, para poder así desarrollar unas estratégicas bien definidas.

- La intención de la Unión Europea de reforzar la colaboración público-privada, así como favorecer el intercambio de información de manera homogénea entre los distintos órganos competentes de cada estado miembro, elegidos por la propia Unión Europea, con la finalidad de poner fin a las fronteras entre los distintos estados miembros en lo que a ciberespacio se refiere. No se pueden aplicar las mismas leyes al mundo físico que al mundo digital y que debe haber un cambio, en el que se pase de una legislación correctiva a una legislación preventiva.
- Es necesaria una regulación, pero es complicado definir una legislación para menores o para mayores, por lo que debe realizarse una legislación para los ciudadanos y las empresas. Se debe buscar una regulación dinámica, que se adapte a los continuos cambios de la tecnología, a nivel global, no a nivel nacional. La regulación actual permite que no estemos desprotegidos, pero que desde luego existe un cambio de mentalidad que requiere un enfoque distinto al que se ha llevado hasta ahora, el cual debe ser llevado a cabo con ayuda de las empresas y de todos los ámbitos, ya que el estado por sí solo no puede con todo al tratarse de un fenómeno muy nuevo y muy grande.
- Los operadores jurídicos tienen dificultades para aplicar los distintos tipos penales debido a su baja formación tecnológica, aunque se está realizando un esfuerzo importante para que haya una formación tecnológica de dichos operadores.

Privacidad y vigilancia

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.

Mensajes del foro

La privacidad es un bien jurídico en riesgo en distintos niveles:

- La acción del Estado, como ha puesto de manifiesto el caso Snowden, y la STJUE en el caso Digital Rights Ireland, sigue constituyendo una amenaza para la privacidad. A ambos lados del Atlántico el rastreo indiscriminado y la indexación de toda la población generan una relación de desconfianza con la garantía de los derechos frente al Estado en una sociedad vigilada.
- El usuario. El segundo factor de riesgo deriva de la conducta del propio usuario. Si bien es cierto que la información legal y las políticas de privacidad no son claras, no lo es menos que el usuario ya tiene indicios suficientes para ser cuidadoso con su comportamiento en internet y en la

identificación de los lugares y servicios confiables. Sinn embargo no parece ser así.

- Problemas éticos y jurídicos. Se considera necesario que las empresas asuman compromisos éticos y jurídicos en la garantía de la privacidad.

Marco regulador

- El actual marco regulador se caracteriza por su antigüedad e inadecuación, así como por su dificultad en la aplicación. Se requiere un marco normativo futuro adaptado a los tiempos y basado en principios flexibles susceptible de ser incorporado al diseño de bienes, productos y servicios TI.

Tecnología

- Se reivindica una tecnología neutral en el que los usos resulten garantes de la privacidad y en su diseño la interacción tecnología-derecho rinda resultados positivos y respetuosos con la privacidad.

Oportunidades

- Tecnopolítica y participación democrática. Las tecnologías de la información y las comunicaciones pueden plantearse como catalizadoras de una mejora de las instituciones democráticas y en transferir capacidad, empoderar al ciudadano, mediante instrumentos de participación digital.
- Garantía de los derechos. El derecho fundamental a la protección de datos, la privacidad, puede y debe erigirse en el pilar que soporte nuestro sistema de libertades en internet.
- Desarrollo de aplicaciones. El sistema europeo de privacidad debería constituir una oportunidad de crecimiento en el mercado digital global mediante una oferta de servicios basados en una oferta de privacidad garantizada.

Identidad de niños y jóvenes

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 estos momentos, mayo 2015, 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, es un punto de partida en esa necesaria evolución.

Mensajes del foro

- Se debe dar identidad de los niños y jóvenes en la red, garantizando la protección de la infancia
- Hay que potenciar los usos positivos y maximizar los beneficios asociados. El mayor riesgo es desperdiciar el potencial que las TIC traen para el desarrollo de los niños y jóvenes
- 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.

- 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.
- Se debe 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.
- Es imprescindible un nuevo marco de competencias digitales.
- El ámbito sanitario se ha mostrado como un canal de acceso para la prevención, estudio y acompañamiento de los niños y jóvenes.
- La tecnología avanza muy rápido y ha provocado que las conclusiones de las distintas jornadas hayan ido quedando obsoletas año tras año.
- No estamos preparados para acompañar a los niños y jóvenes en su crecimiento entre tecnología. 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 cercanos se están sumando los profesionales de la salud, y esta es una gran noticia pues son el canal de prevención natural

Políticas de Propiedad Intelectual

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.

Principales mensajes del foro

El principal mensaje del foro es una apuesta por el valor del Derecho de Autor y de la Propiedad Intelectual en el entorno digital, protegiendo la libertad del autor de hacer lo que él quiera con sus obras: difundirlas gratuitamente o explotarlas económicamente.
También se ha estado de acuerdo en que el "mercado único digital" no es sólo europeo, es global y debería tenderse a unas "reglas de juego" iguales para todos, porque los problemas y retos globales tienen que tener soluciones globales, para poder competir en igualdad de condiciones.
En tercer lugar, se ha constatado que las TIC han supuesto una revolución que todavía no se percibe en su verdadera dimensión y obliga a repensar los derechos intelectuales y los modelos de negocio y gestión, siendo posible la coexistencia de una gestión individual junto a la colectiva.

Otros mensajes:

1. Los sectores de contenidos y de internet están obligados a entenderse
2. Los contenidos digitales son (y serán aún más) uno de los principales motores de crecimiento de la economía europea.
3. Es esencial la cooperación entre los distintos Ministerios, Administraciones españolas y Gobiernos de la UE.
4. Es esencial la colaboración público-privada y la autorregulación sectorial; porque internet no se puede regular y controlar por Gobiernos
5. Con la Estrategia del "Mercado Único Digital" España y Europa se están jugando el papel que van a desempeñar en un futuro en el entorno global.
6. Es necesario un marco armonizado para que surjan empresas europeas competitivas.
7. Planteamientos en exceso garantistas pueden dificultar competir con multinacionales.
8. Las medidas contra el geo-bloqueo puedan perjudicar la cadena de valor de los contenidos.
9. Hay que potenciar los nuevos modelos de negocio, pero la Propiedad Intelectual seguirá siendo la piedra angular, si queremos fomentar industria que da trabajo a miles de personas.
10. Hay que vigilar cómo afectan los Términos y Condiciones de Uso de plataformas digitales multinacionales a los derechos de propiedad intelectual.

Internet abierta y neutralidad de red

El pasado día 26 de febrero de 2015, la FCC redefinía el servicio de acceso de banda ancha a Internet como servicio de telecomunicación, quedando al amparo del título II de la Ley de Telecomunicaciones. La nueva regulación, ampliamente defendida por la Administración Obama, pretende salvaguardar la esencia abierta de la Red y situar a la FCC en mejor posición legar para garantizarla tras las dificultades de los últimos años, en los que los tribunales han considerado que la regulación del servicio de acceso de banda ancha a Internet caía fuera de su ámbito competencial.
La regulación establece las reglas de no bloqueo, no ralentización, no priorización pagada y transparencia mejorada de la gestión del tráfico en el servicio de acceso a Internet, con la novedad de que se aplica tanto al segmento fijo como al móvil.
Mientras tanto, en Europa se está gestando un Reglamento de mercado único de telecomunicaciones que ha sido ya enmendado en el Parlamento Europeo y pasado a ser debatido en el Consejo. El texto, que trata diversas cuestiones relacionadas con la Internet abierta y la neutralidad de la red, incluye provisiones para los servicios especializados.

Mensajes del foro

Los mensajes que nos gustaría trasladar a los foros supranacionales, especialmente EuroDIG, que tiene lugar los días 4 y 5 de junio de 2015 en Sofía son:

- El concepto de Internet abierta es subjetivo e interpretable, pero debe cubrir todos los aspectos de la cadena de valor de Internet: desde los terminales, a las redes, las plataformas y la información en la Red.
- La protección de la Internet abierta debe preservar la libertad de elección de los usuarios, respetar los derechos humanos (libertad de expresión, privacidad) y fomentar la innovación en sentido amplio.
- En lo que respecta a las redes de acceso, el caso de EEUU es muy diferente del de Europa, ya que en Europa hay una mayor competencia entre operadores lo que implica un mayor poder de elección para el usuario a la hora de contratar un servicio de banda ancha de acceso a Internet, especialmente en altas velocidades.
- En el caso de Europa, las fórmulas de competencia + transparencia – bien ejecutadas- pueden ser suficiente en la mayoría de los casos para no necesitar regulación *exante* en materia de neutralidad de red.
- En Europa las tarifas *zero rating* representan una fórmula comercial mediante la cual los operadores no reciben contraprestación económica alguna por el tráfico de datos –incluido en esta fórmula comercial– cursado por los clientes. En este sentido, el caso de Europa y el de los países en vías de desarrollo es también muy diferente: por ejemplo, en India el uso de estos esquemas está generando un intenso debate por el efecto que puede tener en la liberta de expresión.
- Ni la regulación estadounidense ni la europea están siendo capaces de abordar correctamente los paralelismos existentes entre las redes de

servicios de comunicaciones electrónicas, gestionadas por los operadores,, y las redes de distribución de contenido (CDN, *Content Delivery Networks*), que utilizan otros agentes económicos que intervienen en toda la cadena de Internet, lo que está dando lugar a asimetrías.

- Europa necesita abordar el problema de la Internet abierta en toda su dimensión, con una revisión del marco regulador sectorial para estudiar qué aspectos deben seguir protegiéndose sectorialmente y cuáles deberían cubrirse con un enfoque horizontal.
- La innovación que ha permitido Internet hasta ahora debe tenerse en cuenta en la toma de decisiones de cara a la revisión del marco regulador europeo, dada la dificultad de Europa hasta el momento para generar *startups* en comparación con otras regiones, como EEUU.

La economía de Internet. Innovación y emprendimiento

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, o, en la línea de economía colaborativa la 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 se atreven a embarcarse en una nueva aventura cada día. Confiamos en que en 2015 cada día sean muchos más.

Mensajes del foro

- Hay múltiples oportunidades para generar empleo en las TIC, especialmente en sectores como los videojuegos, desarrollo de aplicaciones móviles y servicios de valor añadido para los dispositivos móviles o análisis de datos.
- Hay varias externalidades positivas para el empleo de Internet que podrían ser mejoradas por el Mercado Único Digital
- Máquinas están absorbiendo los trabajos que requieren un conjunto de habilidades inferior. Nuevo, más creativo, se necesitan perfiles de cambiar a una economía basada en el conocimiento. Fortalecimiento del perfil profesional independiente, que requiere más participación en proyectos

empresariales sin perder su independencia y la capacidad para hacer frente a otras iniciativas.

- Existe una gran diferencia entre la regulación de empresas de telecomunicaciones y servicios de Internet.
- El Internet no es un sector económico y esto debe ser tenido en cuenta en la medición de su impacto.
- Crecimiento importante de financiación alternativa con diferentes modos y funciones que son capaces de adaptarse tanto a la hormiga inversor del empresario.
- La política de innovación no puede limitarse a un solo departamento dentro de la empresa. La sociedad debe convertirse en el principal agente de innovación.
- El autoempleo no es emprendimiento. No podemos, por tanto, asumir como base de apoyo a la actividad emprendedora los conjuntos de medidas políticas adoptadas al calor de una coyuntura sociopolítica adversa en la que se cotizan al alza las políticas destinadas a maquillar las cifras de desempleo.
- El escenario al que se enfrenta el emprendedor, ante la dicotomía de "innovar para emprender" o "emprender para innovar", la innovación se convierte en una actividad ecosistémica, a la que le obliga la propia naturaleza competitiva de su hábitat. Por tanto, el emprendedor seguirá siendo innovador a pesar de la atención privilegiada que ha suscitado el auto-empleo como actividad pseudo-emprendedora.