Comparecencia de Eugenio Fontán Oñate, Decano-Presidente del Colegio Oficial de Ingenieros de Telecomunicación (COIT) ante la Ponencia conjunta de estudio sobre los riesgos derivados del uso de la Red por parte de los menores

30 ENERO

Buenos días. Agradezco en mi nombre y en el del Colegio Oficial de Ingenieros de Telecomunicación la invitación a comparecer ante sus señorías para trasladarles nuestra visión sobre este tema que consideramos fundamental para conseguir un correcto desarrollo de los servicios de la Sociedad de la Información: dotar a los mismos de las garantías suficientes de uso por parte de los usuarios, especialmente los menores, los llamados nativos digitales.

Como ustedes saben, las redes sociales, de las que los jóvenes son usuarios intensivos, son servicios basados en plataformas que operan sobre internet y que, resumidamente, constituyen una nueva forma de comunicación, todavía en expansión. Los ingenieros de telecomunicación, aplicando nuestro conocimiento científico y técnico, hemos contribuido a diseñar y construir las redes de telecomunicaciones necesarias para el desarrollo de este y otros paradigmas tecnológicos que están convirtiendo a Internet en la herramienta de la pancomunicación.

Lo que inicialmente se llamó “web 2.0” a mediados de la década pasada (o lo que es lo mismo, las primeras experiencias de interactividad entre los emisores de información y los receptores de la misma) ha derivado hacia un nuevo escenario donde prácticamente todos los usuarios somos creadores de contenido y lo compartimos a través de herramientas como estas que hoy nos ocupan. Desde cualquier punto del planeta y desde cualquiera que sea el terminal (fijo, móvil, televisión, ...) podemos conseguir una repercusión a nuestros mensajes impensable hace una década, proceso que viene acentuándose con la democratización del acceso a las redes de telecomunicación, que en el caso concreto de

nuestro país llega a índices muy elevados de penetración. Según el informe anual presentado este mismo mes por la Fundación Telefónica, en la franja de 16 a 24 años, un 86% de los usuarios de Internet son intensivos, esto es, viven conectados y consultan el móvil unas 150 veces al día.

Hoy en día cada dos minutos se publican en Facebook tantas fotos como se hicieron en todo el siglo XIX. En 48 horas se genera la misma información que la humanidad había creado desde el inicio de los tiempos hasta el año 2003 *(Eric Schmidt)*. 48 horas de video se suben cada minuto a Youtube. 200 millones de tuits se lanzan diariamente en Twitter… y todo esto es posible porque las telecomunicaciones siguen avanzando a un ritmo imparable. La evolución de la banda ancha y la fibra hasta el hogar y la evolución de las redes móviles que han incrementado la capacidad de datos con UMTS y LTE (3ª y 4ª generación respectivamente), unido a la irrupción de nuevos dispositivos (fundamentalmente tablets y smartphones) ha permitido ubicuidad del acceso a las redes sociales, y otros servicios de internet, por parte de un amplio espectro de la población.

El siguiente estadio, llamado "Internet de las cosas", permitirá conectar los objetos a Internet, y a los mismos, recopilar información sobre las costumbres y pautas de comportamiento de los usuarios y consumidores. Se calcula que en 2020 habrá 50.000 millones de dispositivos conectados a la red. Éstos captarán cantidades ingentes de información que, almacenada y procesada, estará disponible para la toma de decisiones en todos los ámbitos. Lo que hemos dado en llamar la era del Big Data es uno de los campos de estudio más pujantes actualmente de la ingeniería. Las principales empresas se están posicionando en materia de análisis y procesamiento de esta inmensa cantidad de información que vamos a manejar. Este nuevo entorno de los macrodatos, ya en puertas, nos va a plantear retos apasionantes a los ingenieros y sociólogos, pero también a las autoridades que deben anticipar los riesgos derivados y ofrecer garantías al ciudadano sobre la custodia de sus datos.

Es por ello que, dado que otros expertos más cualificados que yo desgranarán ante ustedes las prácticas abiertamente delictivas que se producen en la Red y que afectan a los menores, y también desde otras ramas se les expondrá la necesidad de formar a nuestros jóvenes para el correcto uso de estas herramientas, me van a permitir centrarme en este aspecto concreto que trato de introducir: estos avances revolucionarios que he mencionado, que sin duda facilitarán la vida de las personas, tienen implicaciones muy importantes en cuanto al manejo de lo que denominamos "identidad digital" y también sobre el propio concepto de privacidad y su protección. Existe y existirá cada vez más y más información nuestra en el mundo virtual, las herramientas para procesar esa información e inferir conclusiones sobre nuestras pautas de comportamiento o de consumo se están perfeccionando y debemos adelantarnos a estos cambios para que se produzcan con todas las garantías.

Sin embargo, se da la paradoja de que este nuevo medio de comunicación, Internet, el más poderoso de los inventados hasta la fecha, está sometido a instrumentos regulatorios tradicionales, que en muchos casos no están adaptados a esta realidad totalmente nueva. Las telecomunicaciones se regulan internacionalmente a través de organismos como la Unión Internacional de Telecomunicaciones (dependiente de la ONU) lo que, entre otras cosas, garantiza que podamos realizar una llamada a otro país, o usar el mismo terminal móvil cuando vamos al extranjero, por ejemplo. Aspectos como estos son coordinados internacionalmente.

Es cierto además que en el entorno de Internet existen organismos internacionales como la Internet Engineering Task Force (IETF) que coordina los nuevos protocolos de comunicación entre servidores de internet o ICANN (Internet Corporation for Assigned Names and Numbers) que coordina la administración de los elementos técnicos del DNS para garantizar la resolución unívoca de los nombres, una organización que, por cierto, fue creada por mandato del gobierno estadounidense y responde únicamente al mismo, aunque regule la asignación de dominios en

Internet en todo el mundo, pero esta coordinación internacional en el ámbito de Internet es principalmente técnica. De hecho, ICANN, integrado por expertos representantes de instituciones y empresas, es el organismo que más se aproxima a encarnar hoy por hoy la gobernanza en Internet. Sobre esto existe un debate muy interesante, poco conocido por el gran público, que demuestra que estamos ante una disyuntiva que marcará el destino de la red: ¿debe ser regulada a través de los mecanismos convencionales regulatorios que se aplican a los asuntos supranacionales o vamos hacia un modelo de autorregulación acordada por los agentes implicados, cercanos a las continuas novedades tecnológicas y de negocio?

Es notorio que la práctica totalidad de las redes sociales de mayor éxito son estadounidenses, por lo que al usuario de a pie español o europeo, nadie le informa ni le garantiza si se están cumpliendo o no los derechos que tiene en su respectivo país respecto a sus datos o si, permítanme el comentario, en su actividad en la red pesa más la primera enmieda[1] de la Constitución americana. ¿Dónde se almacenan nuestros datos?¿qué se hace con ellos?¿Se manejan con las debidas garantías de seguridad? El usuario de a pie no tiene respuesta a estas preguntas.

A mediados de diciembre pasado los grandes gigantes de Internet (Google, Microsoft, Yahoo, Facebook, Twitter, Netflix, LinkedIn, Comcast, AT&T) se reunían con el presidente Obama para reclamar transparencia sobre las operaciones de las agencias de inteligencia estadounidense sobre los datos de la Red. Es curioso que muchas de estas empresas soliciten transparencia y apertura tanto al gobierno como a los ciudadanos y a su vez oculten los modelos predictivos que han desarrollado sobre los datos de sus usuarios.

[1] Primera Enmienda: *El Congreso no hará ley alguna con respecto a la adopción de una religión o prohibiendo el libre ejercicio de dichas actividades; o que coarte la libertad de expresión o de la prensa, o el derecho del pueblo para reunirse pacíficamente, y para solicitar al gobierno la reparación de agravios.*

El debate sobre la privacidad ha puesto en el otro brazo de la balanza la seguridad (siendo supuestamente la primera de más peso para los europeos y la segunda para los estadounidenses). Jaron Lanier, uno de los gurús más influyentes del mundo de Internet, afirmaba recientemente en un artículo publicado por "Investigación y Ciencia" que *"Cuando se habla del gran compromiso entre privacidad y seguridad, o entre privacidad y servicios, se da a entender que éste resulta inevitable. Es como si hubiéramos olvidado lo más esencial de los ordenadores: que son programables*" Los programas son los que deben garantizarnos qué se puede y qué no se puede hacer.

Europa debe pugnar por proteger nuestro derecho a poseer los datos que nos conciernen. Alex Pentland, Profesor del MIT y asesor del World Economic Forum en esta materia afirma que "*para lograr una sociedad justa en la era de los datos, debemos alcanzar un Nuevo Acuerdo sobre Datos, cuya clave es tratar los datos personales como un activo, sobre el que los individuos tienen derecho de propiedad"* Propone Pentland tres puntos irrenunciables:

- *Usted tiene derecho a poseer los datos que le conciernen, sea cual sea la entidad que recoge los datos, le pertenecen y puede acceder a ellos en cualquier momento*. Los entes que recopilan datos cumplen una función parecida a la de un banco que gestiona el patrimonio de sus clientes.
- *Usted tiene derecho al pleno control sobre el uso de sus datos.* Las condiciones de uso deben ser autorizadas y estar claramente explicadas en lenguaje llano. Si no está satisfecho sobre el uso de esos datos puede retirar la custodia de los mismos en cualquier momento (igual que procedería a cerrar una cuenta bancaria).
- *Usted tiene derecho a disponer de sus datos y a distribuirlos*. Está facultado para destruir o redistribuir los datos que le conciernen en cualquier momento.

Debe propiciarse un debate internacional de calado que tenga esta consideración sobre los datos. Solo así se conseguirá una correcta

protección de los derechos de los ciudadanos, de los internautas y por supuesto, de los menores. La huella digital de los que hoy tienen 30 años, o lo que es lo mismo, su historial completo en la web, según AVG se remonta ya a 10 o 15 años atrás. La mayoría de los bebés están en internet antes de los dos años. Cuando cumplan 30 llevarán más de dos décadas de vida digital.

La oportunidad que le brinda a Europa la puesta en marcha de manera coordinada de su Agenda Digital, no debe dejar al margen asuntos tan prioritarios para la ciudadanía como estos. Pensemos que una de las líneas estratégicas de la Agenda Digital es la protección de los menores en la Red.

La propia Comisión Europea, realizó en 2011 un informe basado en 25.000 encuestas a jóvenes de Europa, del que se extraían conclusiones para la reflexión. El 77% de los menores de edad, con edades comprendidas entre los 13 y los 16 años utilizaba entonces las redes sociales (ahora serán más) y también un 38% de los menores con edades comprendidas entre los 9 y los 12 años. De las redes sociales evaluadas entonces, solo dos (Bebo y MySpace) tenían establecida una configuración por defecto que garantizaba que la información de los menores solo era vista por sus contactos aprobados. Esto es, las redes sociales más utilizadas dejaban por defecto accesibles los perfiles de los menores a cualquiera que quisiera consultarlos en la red. La seguridad de los menores en la red, que están indisolublemente concernidos al ser éstos usuarios intensivos de las redes sociales debe ser promovida entre todos y, por supuesto, desde la Administración, y las medidas que se adopten deben acompasarse con la necesaria “alfabetización digital” que no debe restringirse al uso de las propias herramientas, sino a la correcta gestión por parte del usuario (máxime si hablamos de menores) de su información personal en la red.

En España el 39% de los adolescentes pasan más de dos horas al día en las redes sociales y lo hacen al margen de que se encuentren en el colegio o en otras actividades (la media europea es del 23%). Tuenti es la red social más empleada por los adolescentes (de entre 10 y 16 años) Casi el 60%

están presentes en este servicio, mientras que el 56% tiene perfil en Facebook, el 12% en Google+ y el 3% en Myspace.

Nuestros niños y jóvenes no son conscientes de que ya cuentan con un historial completo, con una biografía detallada, que incluye sus gustos, sus actividades, sus amigos, sus opiniones, sus recuerdos, etc. accesible en la red. Existen métodos para conseguir, por trazabilidad de datos, un perfil muy concreto de millones de usuarios de redes sociales menores de edad en el mundo y no existe una conciencia en los mismos de proteger esa privacidad para que esta información no pueda ser utilizada a la larga de manera maliciosa. Pensemos que aproximadamente el 30% de los contactos que tienen los adolescentes en las redes sociales son desconocidos o "amigos virtuales" según un reciente informe de la OCU.

Entre los menores de 10 a 13 años, el 44% tiene un perfil en Facebook. Se dan de alta simplemente simulando una edad que no tienen, ya que las más populares redes sociales están restringidas para menores de 16 años (14 en las redes sociales específicas para adolescentes). Estamos ante una tendencia imparable en la que, por supuesto, debemos formar desde muy pequeños a los niños para que vigilen su privacidad y su seguridad, pero en el que no debemos descuidar las exigencias a las empresas que operan estas grandes plataformas.

En nuestro país hasta la más pequeña de las PYMES debe cumplir con la Ley Orgánica de Protección de Datos. ¿Se exige ese cumplimiento estricto a Facebook y otras plataformas, que han revelado recientemente las solicitudes de acceso a datos de sus usuarios por parte de los diversos gobiernos del mundo? ¿A quién y de qué manera debe reclamar un usuario al que le han suplantado su identidad en una red social?¿Puede un usuario solicitar su "portabilidad" de una a otra red social, como se exige a las compañías telefonía móvil, sin perder toda su información personal?¿Se le ofrecen garantías de borrado de sus contenidos al darse de baja? El cierre del servicio de Megaupload, independientemente de las causas, provocó que muchos usuarios perdiesen archivos personales que habían depositado en ese servicio. ¿Qué pasaría si el día de mañana

Facebook o Twitter, que constituyen para muchas personas su diario personal cierran o cambian las condiciones del servicio? Es un escenario improbable pero técnicamente posible. Pensemos que a nivel técnico, estas plataformas son aplicaciones hospedadas en servidores alojados en centros de datos. Probablemente con máximas garantías de seguridad en cuanto a redundancia y disponibilidad, porque de ello depende el negocio. Pero en definitiva, aplicaciones que pueden desactivarse o modificarse de forma muy rápida sin el consentimiento de los usuarios.

El modelo de Internet que hemos construido, está basado en la gratuidad, que ya es entendida por los propios internautas como un derecho. Este modelo tiene obvias virtudes, porque permite que las bondades de la Sociedad de la Información se extiendan rápidamente, pero también importantes inconvenientes, ya que en muchos casos el prestador de servicios se escuda en que los ofrece de forma gratuita para no garantizar que los ofrece con unos parámetros de calidad adecuada. Y además, plantea importantes interrogantes sobre la adecuada retribución de los generadores de contenidos y sobre la sostenibilidad del ecosistema de Internet.

En este contexto ¿Quién va a garantizar nuestro derecho al secreto constitucional de las comunicaciones? Hasta ahora teníamos una compañía operadora registrada en la CMT (Ahora CNMC) y con unas obligaciones concretas y estrictas en este campo, pero ¿Cómo podemos garantizar la seguridad de la información si ni siquiera tenemos opción de exigir responsabilidades a estas empresas cuando este derecho es vulnerado o cuando los datos quedan al descubierto por algún agujero de seguridad? Estas empresas, en muchos casos, no tienen oficinas ni personal en nuestro país, pero sin embargo cuentan con millones de usuarios españoles (un 93% de los internautas españoles tiene al menos una cuenta activa en redes sociales)

En definitiva, hay múltiples aspectos que deberían ser abordados urgentemente relativos a los derechos fundamentales de los usuarios a los que debemos garantizar su intimidad, su reputación e incluso aspectos tan

sensibles como el derecho al olvido digital, o cómo operar con toda la información volcada por un usuario en las redes sociales una vez que éste haya fallecido.

Además, debemos categorizar las "infracciones" que se cometan en el entorno digital porque, si bien hay algunas que son un mero reflejo de las ya reguladas en el mundo físico, como obviamente, muchas de las abiertamente delictivas (pensemos por ejemplo en el acoso a menores o en la apología del terrorismo) existen otras que nacen de la utilización de estas nuevas herramientas y no están previstas en el ordenamiento (por ejemplo la suplantación de identidad virtual, o la publicación en abierto de información etiquetada como privada por el usuario) y ante las que, hoy por hoy, el internauta se encuentra desprotegido.

Derivar algunas de estas infracciones al ámbito policial o judicial, además de ser una medida posiblemente desproporcionada, podría colapsar el sistema. Por ello, parece lógico contemplar también la resolución de estos conflictos desde el ámbito administrativo, como ya ocurre con otras actividades relacionadas con las propias telecomunicaciones. Pensemos en un caso de ciberbullyng sobre un menor, ¿a qué instancias debe dirigirse un padre para solicitar a una red social la desactivación de una imagen o video que denigra al menor? Hoy por hoy esos cauces no están debidamente articulados y debemos poder exigir que se articulen para una correcta y sobre todo rápida respuesta por parte de los prestadores de los servicios.

Ofrecer a los internautas la posibilidad de denunciar ante el órgano administrativo competente aquellas acciones que vulneren los derechos citados en esta intervención obligaría a los responsables de estas plataformas a atenerse a unas exigencias concretas de calidad del servicio, lo que, sin duda, redundaría en la puesta en marcha mecanismos ágiles para la resolución de estos problemas.

Por supuesto, los telecos y técnicos que trabajan día a día en la puesta en marcha de estos servicios trataremos de aportar en soluciones a los

problemas de seguridad pero entendemos que para conseguir una efectiva protección de los menores y de todos los usuarios de Internet es preciso acometer medidas valientes que sitúen a estos agentes que operan y que, no lo olvidemos, basan sus potentísimos negocios en la red, a cumplir con unos baremos básicos de calidad del servicio, que incluyen la rápida respuesta a estos conflictos.

Como ya se ha expuesto, consideramos que al igual que las telecomunicaciones están coordinadas internacionalmente, parece razonable que las aplicaciones, y en concreto las redes sociales, en la medida en que utilizan datos y contenidos personales de los usuarios, también lo estén. Y estas iniciativas deben cobrar fuerza en el marco europeo, desde donde debe darse un impulso para que todo ciudadano usuario de redes sociales esté puntualmente informado de si la compañía a la que confía sus datos y a través de la que se comunica, cumple unos determinados requisitos de seguridad y garantiza sus derechos fundamentales. Máxime cuando estos usuarios son menores y es obligación de todos que estén especialmente protegidos.

Desde el Colegio Oficial de Ingenieros de Telecomunicación, a través de nuestros grupos de trabajo, que implican a expertos en todas las temáticas ligadas a nuestra ingeniería, estamos trabajando ya en propuestas concretas en el entorno de las redes sociales, que esperamos sean de utilidad para la reflexión en profundidad sobre este asunto que afecta a la práctica totalidad de nuestros jóvenes y a un amplísimo porcentaje de población española.

Quedo a su disposición para cualquier cuestión que quieran formularme. Muchas gracias.